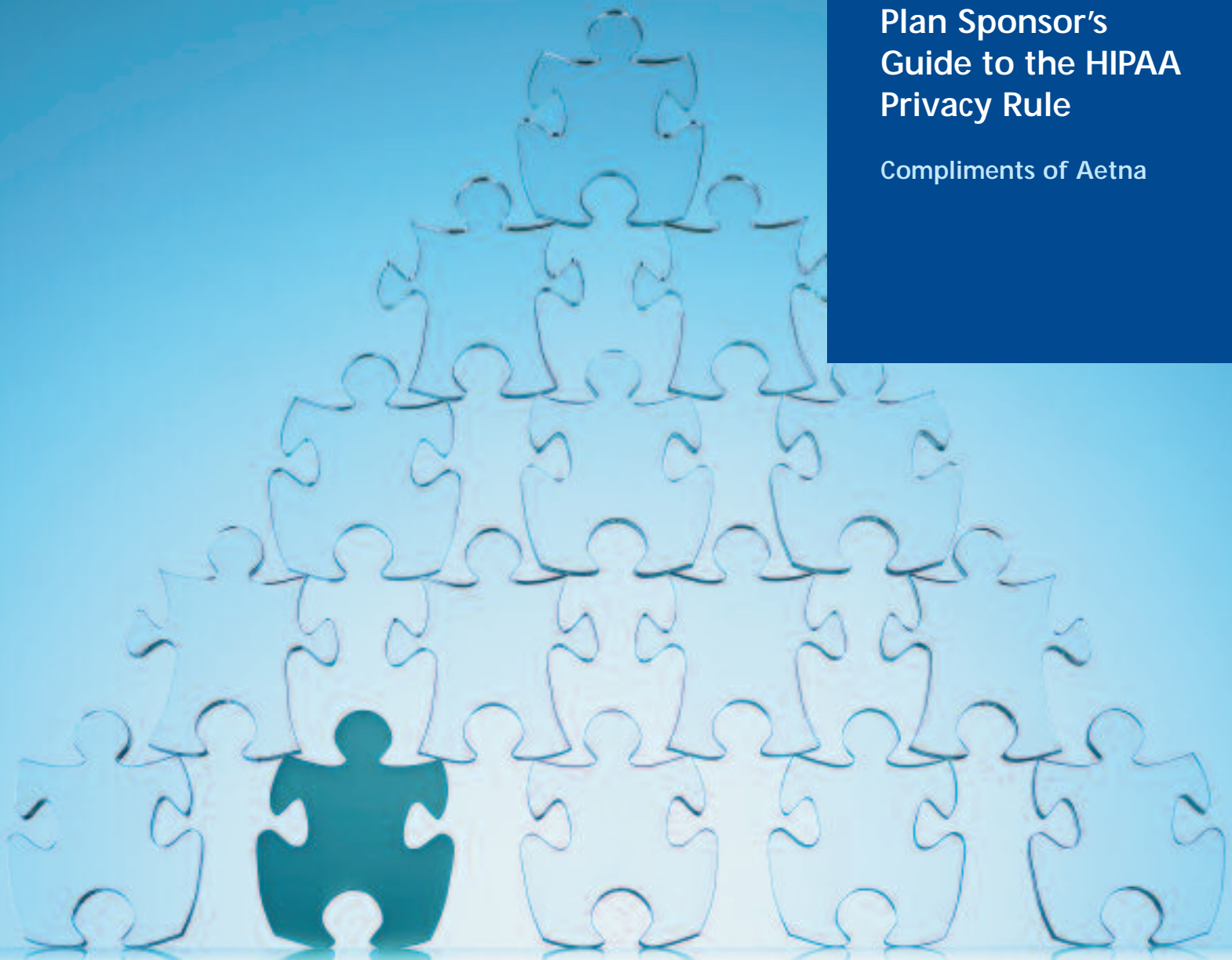


Plan Sponsor Guide

HIPAA Privacy Rule

Plan Sponsor's
Guide to the HIPAA
Privacy Rule

Compliments of Aetna



We want you to knowSM



Compliments of Aetna

You have likely heard a great deal about the HIPAA Privacy Rule and how it has had a sweeping effect on the health care industry. Although the Privacy Rule primarily impacts health care providers and insurers, it also affects employers that sponsor group health plans. If you have not done so already, Aetna urges you to consult your professional/legal advisors for guidance on how the Privacy Rule impacts you and what, if anything, you need to do to comply. Although Aetna can't substitute for your professional advisor's advice, this Guide highlights some of the issues that you will need to consider in regard to the HIPAA Privacy Rule.

Background on HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress and signed into law in 1996. Until recently, most of the focus on HIPAA has been confined to certain health insurance-related issues. For example, HIPAA addresses limitations on exclusions for pre-existing conditions, availability of health insurance coverage for small employers, and rights of individuals to apply for health coverage when they lose their existing coverage. HIPAA also strengthens federal health care fraud and abuse laws.

Recently, more attention has shifted to Title II, Subtitle F of HIPAA, which deals with Administrative Simplification. Privacy is just one of the five components of Administrative Simplification — the other components are: Electronic Transactions; Code Sets; Security; and Unique Identifiers. Each of the Administrative Simplification components has its own compliance date. The compliance date for the HIPAA Privacy Rule was April 14, 2003.

Covered Entities

The HIPAA Privacy Rule governs the use and disclosure of Protected Health Information (PHI) by “covered entities.” Covered entities are defined as health plans, health care clearinghouses and health care providers who transmit health information electronically. While the Privacy Rule does not directly regulate employers, the requirements apply to “group health plans” that are sponsored by many employers.

Covered plans include those providing medical, dental, vision, pharmacy and other medical benefits. Flexible spending accounts also fall within the definition. The Privacy Rule specifically excludes from coverage disability plans, workers compensation plans and life insurance — despite potential coverage of medical services.

Protected Health Information

Under HIPAA, Protected Health Information (PHI) is information that:

- Relates to an individual's physical or mental health, the provision of health care to the individual, or the payment for the individual's health care;
- Identifies, or could reasonably be used to identify, the individual; and
- Is created or received by a covered entity.

The Privacy Rule covers PHI that is transmitted or maintained in any form or medium (e.g., electronic, paper and oral communications).

Uses and Disclosures

Health plans may use or disclose PHI for purposes of treatment, payment or health care operations without a participant's consent or authorization. "Payment" is defined as any activity undertaken by a health plan to obtain premiums or fulfill its coverage responsibilities. "Treatment" means the provision, coordination or management of health care and related services. "Health care operations" means administration of health benefits policies or contracts, quality assessment and

improvement activities, customer service, disease management, etc. Any allowable use or disclosure must be limited to the "minimum amount necessary" to achieve the stated purpose. Health plans should conduct a survey of their uses and disclosures of PHI to ensure that they comply with the Privacy Rules and adopt appropriate policies.

Participants' Rights

Group health plan participants and beneficiaries have a right to:

- Receive a notice explaining their health plan's privacy policies and practices (the notice must be sent each time the practices change materially);
- Access their PHI;
- Request amendments to their PHI;
- Request an accounting of certain types of disclosures (i.e., those outside the scope of treatment, payment and health care operations); and
- Request, in certain instances, that PHI be communicated through alternative confidential means or to alternative locations.

Business Associates

Health plans must have a written contract with each "Business Associate" that contains certain prescribed provisions (in essence, the business associate must be required to abide by the use and disclosure limitations in the Privacy Rule). "Business Associates" are persons or entities who perform functions on behalf of a covered entity and either have access to or are reasonably likely to have access to PHI. Health plans have to take action if they become aware of a Business Associate breach (i.e., require the Business Associate to cure the breach, and, failing that, the health plan may have to terminate the contract).

Administrative Requirements

The following tasks must be implemented by "covered entities" in order to be in compliance with the HIPAA Privacy Rule:

- Appoint a privacy officer;
- Develop HIPAA-compliant privacy policies and procedures;
- Implement privacy safeguards;
- Conduct employee training; and
- Establish a complaint process.



Impact on Self-Insured Plan Sponsors

There are a variety of HIPAA Privacy Rule issues that must be addressed by self-insured plan sponsors. Summarized below are some of the key issues that deserve special attention because they require coordination between the plan sponsor and their health plan.

1. *Business Associate Agreements.*

Self-insured plan sponsors will need to enter into “business associate” agreements with all of their service providers who have access to protected health information (“PHI”). The plan sponsor’s claims administrator will be one of the principal business associates. The business associate agreement must contain a number of very specific provisions.

2. *Privacy Notice.* Self-insured plan sponsors are required to send a privacy notice to all of their plan participants. Because this notice will, in large measure, be addressing the privacy practices of the claims administrator, self-insured plan sponsors will need to work closely with the administrator in developing the notice.

3. *Participants’ Rights.* In addition to the right to receive a privacy notice, plan participants have a series of other rights highlighted previously, including the right of access, amendment, accounting and the right, in certain instances, to have PHI communicated through alternative confidential means. Plan sponsors should coordinate with all parties administering any portion of the designated record set to avoid confusion and ensure that all parties honor all requests in a consistent fashion.

4. *Disclosure of PHI by or for the “Group Health Plan” to the “Plan Sponsor.”* The HIPAA Privacy Rule contains detailed and complex requirements for disclosures of PHI by or for the group health plan to the plan sponsor in conjunction with its plan administrative role. These requirements are identified in the Epstein Becker & Green, P.C., Frequently Asked Questions and Answers included in this Guide. There are four aspects to note in particular:

- *“Group Health Plan” vs. “Plan Sponsor.”* The regulations force us all to draw a line of demarcation between the “plan sponsor” and the “group health plan.” The outline provides more information on this

subject, including why you need to draw the line and why it can be difficult to do.

- *“Certification Requirement and Plan Document Amendments.”* One of the requirements for the disclosure of PHI (other than Summary Health Information for limited purposes and enrollment information) is for the plan sponsor to provide a certification to the group health plan that the plan documents have been amended in a number of respects. It will often be incumbent upon the plan sponsor, as the administrator of its group health plan, to put the necessary compliance measures in place. The employer is also certifying to its group health plan that it will not use the PHI it has access to in its health plan administration role in the context of other benefit plans or in employment-related decisions.

The plan documents will need to be amended to contain certain disclosures relating to the data sharing practices with the plan sponsor and the plan sponsor’s use of the PHI. It is important that the plan sponsor coordinate any such amendments to ensure that they correctly describe data sharing.



- **Summary Health Information and Enrollment Information.** The foregoing “plan sponsor disclosure” rules contain a limited exemption for certain PHI that qualifies as “Summary Health Information.” This term is defined in the Epstein Becker & Green, P.C., Frequently Asked Questions and Answers included in this Guide. To the extent your organization is relying on this exemption, please note that it is incumbent upon you to verify that the information meets the requirements of the definition and that the information is only being used for purposes of obtaining premium bids or for modifying, amending or terminating the group health plan. There is also an exemption for enrollment information.

Impact on Fully-Insured Plan Sponsors

For plans providing benefits solely through insurers and HMOs the impact of the Privacy Rule is fairly minimal, provided the plan and the plan sponsor do not create or receive any PHI other than “Summary Health Information” received for the purposes described above (e.g., the new standard experience report is considered “Summary Health Information”) or enrollment information. Among other things, plans meeting this definition avoid the need to name a privacy officer, deliver a privacy notice (the insurer will do it for them), create special privacy policies and procedures and train their employees on them. However, plans are urged to consult their professional advisors about how the Privacy Rule might impact them. Note that the burden is substantially greater for insured customers who create or receive PHI, so insurers will generally shield insured customers from any information that is not “Summary Health Information.” You should know that we also do this for state law reasons.

5. **Administrative Requirements.**

Sponsors of self-funded plans will need to comply with some or all of the administrative requirements highlighted above and as set out in Section 530 of the HIPAA Privacy Rule.

How Employers Can Comply with the HIPAA Privacy Rule¹



Frequently Asked Questions and Answers

By Mark E. Lutes, mlutes@ebglaw.com

The following set of Frequently Asked Questions and Answers, relating to the issues plan sponsors must deal with, is provided as a courtesy by the Law Firm of Epstein Becker & Green, P.C., in Washington, D.C.

What is the HIPAA Privacy Rule?

The Rule governs the privacy of individually identifiable health information (including information related to the payment for health services). It was promulgated pursuant to the administrative simplification provisions of the Health Insurance Portability and Accountability Act (“HIPAA”) — legislation which sought to reduce health care costs by standardizing the format for health claims and other data. Another HIPAA rule will govern the security of health information.

How does the Privacy Rule apply to my company’s health benefit plans?

The Rule treats each welfare benefit plan (within the meaning of ERISA) as a distinct covered entity. The employer or employee organizations that have developed the ERISA plan are referred to in the Rule as the “plan sponsors.” Plan sponsors are not directly regulated by the Rule but will be affected by the Rule in a number of ways.

Are all welfare benefit plans covered by the Privacy Rule?

The vast majority of ERISA plans furnishing health benefits are. The only exempt plans of this type are those with fewer than 50 participants when they are self-administered. Additionally, while for convenience we have focused on the effects of the Rule on ERISA welfare benefit plans, the Privacy Rule also applies to any other individual or group plan, or combination of group plans, that provides or pays for the cost of medical care as defined in the Rule. This will include, for instance, medical, dental, vision, pharmaceutical and behavioral health plans. It even includes some employee assistance plans and all flexible-spending accounts. The rule specifically excludes workers compensation, disability and life benefits.

When does the Privacy Rule take effect?

The Office of Civil Rights, of the Department of Health and Human Services, began enforcement of the Rule (through criminal or civil penalties) on April 14, 2003. So-called “small health plans” have an additional year to comply. The Rule defines small health insurance issuers as those with annual receipts of less than \$5 million. You should review with counsel the application of this size threshold to each of your health plans.

Generally, how does the Privacy Rule affect my company and the health benefits it offers to employees?

The Privacy Rule requires that your company’s health benefit plan:

1. absent special authorization, use and disclose protected health information (PHI) only for activities permitted under the Rule — chiefly activities related to treatment, payment and health care operations;
2. describe in a written notice published to plan beneficiaries uses and disclosures it makes of PHI unless the plan is fully insured² and the plan and its sponsor create or receive only summary health and enrollment information as defined by the Rule and use that information only for limited purposes;
3. enter into contracts with entities that create or receive PHI in the course of providing services to the plan that require that entity (a *business associate*) to use and disclose the PHI consistent with the Rule and, among other things, make the data available to beneficiaries for copying and amendment;³

4. name a privacy officer, set up a complaint mechanism, begin a privacy training program unless the plan is fully insured and creates or receives only summary health and enrollment information and limits the use of that information to the purposes defined by the Rule;
5. implement policies and procedures allowing beneficiaries 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
6. 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.

What are “business associates”?

The Privacy Rule applies the label of business associate to any entity with a work force that is distinct from the work force of a covered entity when it provides services to a covered entity and, in doing so, receives or creates PHI. Covered entities must contract with their business associates to put in place protections for the PHI using contractual terms and conditions prescribed by the Rule.

Thus, where the ERISA plan contracts with one or more third parties other than the plan sponsor for claims administration, network management, utilization management, disease management or any other service which involves the use of PHI, the ERISA plan will need to include in that contract the business associate covenants prescribed by the Rule. Business associate agreements are not required with insurers or HMOs when they are providing insurance coverage to a group health plan because those entities are, in their insured capacity, already subject to the Rule.

Under what circumstances can ERISA plan personnel transmit PHI to other employer personnel?

The Privacy Rule generally allows covered entities to transmit PHI for treatment, payment or health care operations and other exempt purposes. However, health plans are subject to special rules (the “Section 504(f) rules”) where the recipient of the PHI is the plan sponsor.

Unless it is summary health information⁴ transmitted solely for the purpose of obtaining bids or amending or terminating the plan (so-called “settlor functions”), PHI can be transmitted to the plan sponsor only if the plan sponsor has either obtained an authorization from each plan participant whose PHI is received or has amended

the plan documents for the group health plan to inform the plan participants as to the manner in which the plan will be sharing PHI with the sponsor and how the sponsor will be using the PHI. Additionally, the sponsor must make a series of certifications to the plan which state, among other things, that the PHI will not be utilized to make employment related decisions about the ERISA plan’s participants. The Rule also charges plans with describing in the plan documents those plan sponsor employees or classes of employees which will have access to PHI in the course of the plan’s operations. The plan documents are to restrict those persons’ use of the PHI to what is necessary for plan administration.

What changes must therefore be made to the plan documents?

In order for the plan sponsor to receive PHI from the plan which does not meet the Privacy Rule’s definition for summary health information or which would be used for purposes other than the settlor functions, the plan documents must be amended to warn the plan’s participants that such information sharing may occur and to describe the uses and disclosures of PHI by the plan sponsor. The plan documents must also limit the sponsor’s further



disclosure of PHI, require the sponsor to require its subcontractors to protect PHI, prohibit the use of the PHI for employment-related decisions, and explain the participant rights established by the Rule.

What are the participant rights established by the Privacy Rule?

The Rule requires the ERISA health plan to give participants a right to:

- inspect and obtain a copy of the PHI held by the plan in the relevant “designated record set”;
- request amendment of the PHI held by the plan in a designated record set;
- receive an accounting of disclosures made by the plan outside the context of treatment, payment and health care operations and other defined circumstances; and
- request restrictions on the uses and disclosures of PHI the ERISA health plan is otherwise permitted to make within the scope of “treatment, payment and health care operations” (although such requests need not be honored by the plan).

You will want to work with counsel to include all regulatorily mandated aspects of these rights in the plan documents. You will want to work with your providers of administrative services to understand what restrictions they could accommodate if agreed to by the ERISA

health plan. You will also want to work with these providers of administrative services to determine who the contact point or points will be for plan participants seeking to exercise these rights. Finally, prior to receiving PHI which is not in summary form and for settlor or premium bid purposes, the plan sponsor must certify to the ERISA health plan that it will assist participants with the exercise of several of these rights with respect to the PHI it receives.

How should these changes to the plan documents be made?

Employers will want to work with counsel, benefits consultants and others who advise them on health plan issues to make HIPAA conforming changes to their plan documents and to give appropriate notice of such changes or to create plan documents if none currently exist. Self-funded plans will want to coordinate these efforts with any third parties which perform their administration so that the content of the plan document disclosure can accurately reflect the use of PHI by the plan and the administrator as well as the types of disclosures which plan sponsors might require the plan, through the administrator otherwise, to make to the sponsor. These requirements are complex and the changes should be made by someone very familiar with the HIPAA Privacy Rule.

What other contracts may need changes?

Insurers and HMOs might seek changes in their contracts with employers and plans to set out the terms under which the plan sponsor could receive PHI in other than summary form or for purposes other than bid placement or settlor functions. For instance, the plan sponsor might be required to warrant in the group agreement or a side agreement that the plan document changes required by the Privacy Rule have been made and that any PHI it receives will not be used to make employment decisions.

Entities performing administrative services may amend their service agreements to include their covenants as business associates of the plan. Moreover, those service agreements may also be amended to set forth the parties’ expectations with respect to the conditions under which the administrative services vendor will disclose PHI to the plan sponsor.

Is there any alternative to amending the plan documents?

Yes. Plans could elect not to disclose PHI to plan sponsors except for summary health information for purposes of premium bidding or plan settlor activities.

Are there other laws or developments to be considered?

Yes. The so-called “Patients Bill of Rights” (PBR) legislation will have an impact on the designated decision makers of plans. Employers may find it appropriate to coordinate their approach to isolating the handling of PHI with their management of the PBR risk. Also relevant are the Americans with Disabilities Act (ADA) regulations governing the maintenance of separate files for the results of medical examinations conducted in the context of employment or other medical records received by the employer.

ERISA welfare plans should also be aware that the HIPAA Privacy Rule provides a federal “floor” but not a ceiling on health information privacy requirements. Thus, state laws’ health information privacy rules which are stronger than the HIPAA Privacy Rule must also be monitored and complied with.

What organizational and other changes will our health plans need to make?

A. *Self-funded plans*

Whether or not it chooses to disclose PHI to plan sponsors, a self-funded health plan must implement a number of organizational changes to accommodate the Privacy Rule. First, it must designate a privacy official as well as a privacy contact point. Second, it

must train its work force on the policies and procedures it develops as to the use and disclosure of PHI. Third, it must put into place “appropriate” administrative, physical and technical safeguards to protect PHI. Fourth, it needs to adopt complaint policies and procedures. Fifth, it must adopt sanctions against its workforce’s inappropriate use of PHI and document their application. Finally, the plan must mitigate any harmful effects of inappropriate PHI disclosures.

Although these requirements apply to each plan covered by the Privacy Rule, those plans that have a common plan sponsor will generally adopt a common compliance program. Those plans can consult their professional advisors as to the merits of operating as an “organized health care arrangement” for compliance purposes.

The self-funded plan also needs to provide its participants with a notice of privacy practices that describes the plan’s uses and disclosures of PHI. It also informs participants as to their rights to access and amend the PHI in their “designated record set” and to receive an accounting of certain disclosures of PHI made by the plan or its service providers. Plans with a common sponsor may wish to utilize a joint notice.

B. *Insured plans*

A plan that provides benefits solely through insurers and HMOs does not need to adopt these organizational changes or furnish the notice of privacy practices so long as its sponsor does not receive PHI except in summary form and in the context of the settlor functions described above or when needed to understand what coverage an individual has elected. Again, the plan should review with counsel whether it meets the conditions for being deemed fully insured. Issues most commonly arise when benefits personnel in companies with insured plans seek, without written authorization, to receive PHI in the context of resolving questions raised by plan participants and beneficiaries.

Where should my company/plan start?

1. If PHI other than summary health information is reviewed or if its uses exceed plan settlor functions, delineate the classes of employees performing plan administration functions and develop policies limiting those employees’ use of the PHI and prohibiting PHI disclosures to other employees.

2. If PHI other than summary health information is reviewed or if its uses exceed plan settlor functions, amend plan documents to describe the classes of employees with access to the PHI and the company's commitment not to use the PHI for employment purposes.
3. Coordinate with your insurers and administrative service vendors on the development of a Notice of Information Practices that addresses the use and disclosure of PHI and the participants' rights of access, amendment and accounting.
4. Address any disclosure of PHI which is not summary health information disclosure to the plan sponsor by incorporating the necessary certifications in agreements with administrative services vendors, insurers and HMOs.
5. If your company's health plan is not fully insured, you will want to appoint a privacy officer, set up a complaint mechanism, develop a privacy training program for the employees administering the health plan, and develop appropriate physical, technical and administrative safeguards for the plan's PHI.
6. Add the mandated business associate covenants into agreements with all service providers to the plan that are not acting in the capacity of a HIPAA covered entity (e.g., insurer).



We at Aetna hope you find this information helpful. This information summarizes selected elements of the HIPAA Privacy Rule, but does not include a full statement of these or related regulations. Please remember that this information is not intended as legal advice and that plan sponsors should consult their own professional/legal advisors regarding compliance with the Rule.

If you would like further details or have questions about Aetna's compliance with the HIPAA Privacy Rule, please contact your Aetna Account Executive or Account Manager. For more information about Aetna, please visit our website at www.aetna.com.

¹ The information furnished herein is of a general educational nature and does not constitute legal advice. Each plan sponsor should consult with counsel as to the particulars of its situation.

² Plan sponsors should consult with counsel as to the conditions under which a plan will be deemed to be "fully insured" for Privacy Rule purposes including the effect of a flexible spending account on this determination.

³ If the group health plan is insured, no business associate contract is required with the insurer — an "issuer" in Privacy Rule terms.

⁴ For purposes of the Rule, "summary health information" is information that summarizes the claims history, claims expenses, or types of claims experienced by beneficiaries of the group health plan from which identifiers have been deleted.

This set of Frequently Asked Questions is provided by Epstein Becker & Green, P.C., for general information purposes; it is not and should not be used as a substitute for legal advice. Copyright 2000, 2001, 2002, 2003, 2004, 2005© Epstein Becker & Green, P.C. All Rights Reserved.

Aetna is the brand name used for products and services provided by one or more of the Aetna group of subsidiary companies. The Aetna companies that offer, underwrite or administer benefit coverage include Aetna Health, Inc., Aetna Health of California Inc., Aetna Health of the Carolinas Inc., Aetna Health of Illinois Inc., Aetna Dental Inc., Aetna Dental of California Inc., Aetna Life Insurance Company, Aetna Health Insurance Company of New York, Corporate Health Insurance Company and Aetna Health Administrators, LLC. Aetna Pharmacy Management refers to an internal business unit of Aetna Health Management., LLC.

This material is for informational purposes only and contains only a partial, general description of plan benefits or programs. While this material is believed to be accurate as of the print date, it is subject to change.

00.02.108.1A (5/05)

©2005 Aetna Inc.

We want you to knowSM



www.aetna.com