KnowHIPAA.com
HIPAA Privacy Training and Consulting for Group Health Plans

Employer Sponsored Group Health Plans
and the
HIPAA Privacy Rules

Employers must be prepared for their obligations under the HIPAA Privacy Rules

January 2003

Bob Radecki
KnowHIPAA.com
HIPAA-COBRA-FMLA Consulting
bradecki@KnowHIPAA.com
www.KnowHIPAA.com
612-581-6281

© 2002 KnowHIPAA.com

Introduction

The HIPAA regulations make it clear that employers themselves are not HIPAA Covered Entities (CEs). However, an employer sponsored health plan is a CE under HIPAA. Because the employer is involved in the operation of a health plan, and has access to PHI, it becomes responsible for a number of HIPAA privacy requirements. The HIPAA regulations are not always consistent in the use of certain terms. In this overview the following terms are used to distinguish between employer and insurer responsibilities.

Health Insurance Issuer - An HMO or Insurance Company that issues a fully insured health plan to an employer (the plan sponsor).

Plan Sponsor – An Employer, or other entity which sponsors a health plan for their employees or members.

The Health Plan – This term is used in different ways in the HIPAA regulations. In the case of a self-funded plan, the health plan is a legal entity, set up by the "plan sponsor", to provide benefits to its employees or members. The "health plan" in this case typically has no employees or operations. The employer, as the plan administrator and fiduciary, is responsible for the compliance of the health plan. In the case of a fully insured plan, the HIPAA regulations often use this same term when referring to the HMO or Insurance Company that issues the policy to the employer. In this document, the health plan refers to employer sponsored plan offered to their employees, not to the HMO or insurance company.

The effect HIPAA has on the relationship between a health insurance issuer, employers and brokers is different depending to some extent on whether the plan is fully insured or self-funded.

Fully Insured Plans

Fully insured employer sponsored health plans are HIPAA Covered Entities. The insurance company or HMO that provides to benefits is also a HIPAA covered entity. The HIPAA Privacy Rules apply to both in different ways. HIPAA contains an exception that allows employers to avoid most of the privacy requirements if they receive nothing more than summary health information (see below). If an employer with a fully insured plan wants to receive more than summary information, they will need to take some compliance steps soon.

Beginning April 14, 2003, a health insurance issuer may no longer share Protected Health Information (PHI) with an employer unless:
1.) Group plan documents are amended to include a number of elements defined in the rules and,
2.) A health insurance issuer has received a written certification from the plan sponsor/employer that it will meet the requirements of the rule.[1]

Two exceptions exist which allow a health insurance issuer and the employer to share some information while avoiding the plan document and certification rules. In this case the employer would also avoid most of the requirements HIPAA imposes on the plan sponsor.

[1] HHS Final Reg. 45 C.F.R. §164.504(f)(1)(i) *…in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO…, (a group health plan) must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart*

© 2002 KnowHIPAA.com

1. HIPAA allows a health insurance issuer to share "Summary Health Information" with the employer for rating, renewal and plan amendment purposes.[1]
2. HIPAA allows a health insurance issuer to share information with the employer for enrollment and disenrollment purposes.[2]

Important Note! Fully Insured Employers need to make a decision.

If an employer wishes to receive anything more than summary health information, or information for enrollment purposes, it must meet a number of requirements. Employers need to choose if they want to limit the information they receive from a health insurance issuer and avoid the HIPAA requirements, or if they want to certify that they have met the requirements and thus can receive more detailes PHI from the health insurance issuer.

Fully Insured Employer Choice #1

If an employer agrees to receive only "Summary Health Information" and enrollment information from the health plan or health insurance issuer, they avoid most of the HIPAA Privacy requirements. In this case the employer's obligations are limited to:

- The employer is prohibited from retaliatory acts and asking an employee to waive HIPAA rights.
- The employer must keep a copy of the Privacy Notice on file and provide to employees on request.

Summary Health Information is claims data with the following specific identifiers removed:

- Names
- All geographic subdivisions smaller 3 digit zip codes
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

[1] HHS Final Reg. 45 C.F.R. §164.504(f)(1)(ii) *(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of :*

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan

[2] HHS Final Reg. 45 C.F.R. §164.504(f)(1)(iii) *(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan*

© 2002 KnowHIPAA.com

Fully Insured Employer Choice #2

If an employer wishes to receive PHI (including detailed high claims reports which contain individual identifiers) from a health insurance issuer they must take most of the steps to comply with HIPAA that are required of most Covered Entities. Plan documents must be amended and the employer must give written certification that it will abide by a series of requirements defined in section 164.504(f), including that it will:

(ii)(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524 (which gives individuals certain defined rights to access their own PHI);

(F) Make available protected health information for amendment (at the request of the individual) and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph[1]

A fully insured employer sponsored health plan must enter into a Business Associate Agreement with its broker and any other entity with which it shares PHI.[2] The deadline for this agreement is either April 14, 2003 or 2004 depending on the size of the employer's health plan (see box below). Fully insured health plans are not required to enter in to business associate agreements with their carrier or HMO.

[1] HHS Final Reg. 45 C.F.R. §164.504(f)(2)(ii)

[2] HHS Final Reg. 45 C.F.R. §164.502(e)

A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information…A covered entity must document the satisfactory assurances required…through a written contract or other written agreement or arrangement with the business associate…

© 2002 KnowHIPAA.com

Self-Funded Plans

An employer with a self-funded plan is typically the "plan administrator" under ERISA rules, even if they hire a TPA to pay claims for them. An employer with a self-insured plan almost always has access to PHI. In this case, the employer's health plan, not the employer itself, is considered a HIPAA Covered Entity. However the employer, acting as the plan administrator, is responsible for the health plans compliance with HIPAA privacy rules.

Important Note! Small Health Plan Definition

A "Small Health Plan" is a plan with less than $5,000,000 in plan receipts the previous fiscal year. "Receipts" for self-funded plans include the cost of the medical claims, but not the cost of stop loss insurance. Small Health Plans must comply with the privacy rules by 4-14-2004, large plans must comply by 4-14-2003.

Employers with a variety of plans may have different HIPAA responsibilities relative to different benefits provided. For example, an employer who offers a fully insured health plan with no access to PHI and a self-administered Section 125 Health Spending Account will be subject to most HIPAA rules related to the Flex plan, but very few for the fully insured health plan.

A self-funded health plan must enter into a Business Associate Agreement with its TPA, administrator, broker and any other entity with which it shares PHI.[1] The deadline for this agreement is either April 14, 2003 or 2004 depending on the size of the employer's health plan (see box above).

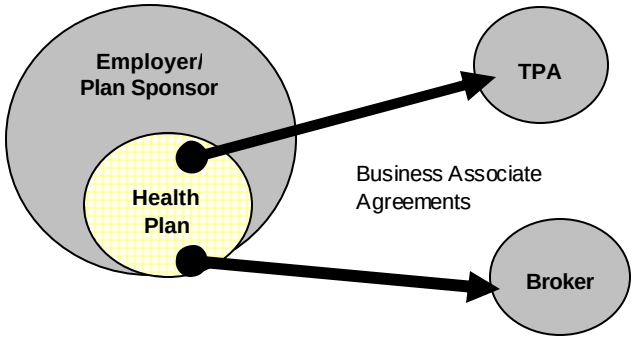
Brokers and Agents

Fully Insured Plans

Brokers and Agents are Business Associates of; the employer health plan, the health insurance issuer, or both. Before a health insurance issuer is allowed to release PHI to a broker/agent, a Business Associate Agreement must be in place between the broker/agent, and either the employers health plan or the insurance issuer. The regulations allow a health insurance issuer to enter directly into a BAA with an agent. However, since it is information about the employees of a group that will be shared, typically a health insurance issuer will require permission from the employer before releasing PHI to a broker/agent.

Self Funded Plans

For self-funded health plans, brokers/agents and TPAs are Business Associates of the employer sponsored health plan. As soon as a plan is subject to the privacy rules, the employer group health plan must enter into Business Associate Agreements with brokers and TPAs to allow the sharing of PHI.[1]



[1] HHS Final Reg. 45 C.F.R. §164.502(e)
A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information…A covered entity must document the satisfactory assurances required…through a written contract or other written agreement or arrangement with the business associate…

© 2002 KnowHIPAA.com

Summary

All employer sponsored group health plans are affected by the HIPAA privacy rules to some extent. If an employer only shares and receives enrollment and disenrollment information and receives no more than summary health information their responsibilities are very limited.

If, however, an employer offers self-funded benefits (including Section 125 flex accounts), or offers a fully insured plan and receives PHI which include individual identifiers, the employer must take a series of steps to protect the privacy of their employees confidential information.

Brokers and agents should identify group clients with more than $5,000,000 in annual receipts and enter in BA agreements prior to 4-14-03. Smaller groups should consider BA agreements prior to 4-14-04 depending on the level of information shared with a broker or agent.

If an employer offers self-funded benefits, or offers a fully insured plan and receives PHI which includes individual identifiers, they must begin their HIPAA compliance efforts soon!

For more information on HIPAA and employer sponsored health plans visit www.KnowHIPAA.com or call 612-581-6281.

© 2002 KnowHIPAA.com