

HIPAA Privacy Rules for Employer Health Plans

May 2003

As the first deadline for compliance with the HIPAA Privacy Rules approaches, employers are finally beginning to think about their compliance responsibilities. The HIPAA regulations make it clear that an employer sponsored health plan, not the employer itself, is a HIPAA Covered Entity. In its role of plan sponsor and plan administrator, employers must deal with a variety of HIPAA privacy requirements.

The HIPAA regulations are not always clear in describing the various responsibilities of different entities affected by the law. In this article, health plan refers to the employer sponsored plan offered to employees, not to the HMO or insurance company. The employer is usually the plan administrator and fiduciary, and is responsible for the compliance of the health plan. The extent of an employer's responsibility depends in part on whether their health plan is self-funded or fully insured.

Many employers offer a combination of plans and will be faced with different requirements for different plans. An employer may, for example, offer a fully insured health plan underwritten by an insurance carrier or HMO, a self-funded dental plan administered by a TPA and a self administered Section 125 medical reimbursement account. Depending on a number of factors, the Privacy Rules could apply differently to each plan.

Fully Insured Plans

Fully insured employer sponsored health plans are HIPAA Covered Entities. The insurance company or HMO that provides the coverage is also a HIPAA Covered Entity. The HIPAA Privacy Rules apply to both in different ways.

Beginning April 14, 2003, a health insurance issuer may no longer share Protected Health Information (PHI) with an employer, unless it meets a number of requirements:

1. Group plan documents must be amended to include a number of elements defined in the rules
2. The employer must create what the rule calls "firewalls", designed to restrict the use of PHI
3. The employer must give the health insurance issuer a written certification that it has met the requirements of the rule.¹

¹45 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

HIPAA contains an important provision that allows an employer with a fully insured plan to avoid most of the privacy requirements. Two categories of limited data may be shared without an employer meeting the requirements described above.

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.

Employers need to choose if they want to limit the information they receive from a health insurance issuer, and avoid most HIPAA Privacy requirements, or if they want to certify that they have met specific requirements which will allow the employer to receive individually identifiable information.

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, it avoids most of the HIPAA Privacy requirements.

Summary Health Information

Summary Health Information is claims data with specific individual identifiers removed. In the preamble to the Privacy Rules, the Department of Health and Human Services recognizes that it may be possible for an employer to “figure out” who summary information refers to, especially in smaller groups. However, as long as specified individual identifiers are removed, the data still qualifies as Summary Health Information.

Individual Identifiers:

- Names
- All geographic subdivisions smaller 5 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, etc.
- Telephone, fax numbers, and e-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers

¹ 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 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*

- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs), and 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

Fully Insured Employer Choice #2

If an employer wishes to receive PHI which contains individual identifiers (for example, a detailed high claims report which includes names), it must take a series of steps to comply with HIPAA. Plan documents must be amended and the employer must give written certification to the health insurance issuer that it will abide by a series of requirements defined in the Privacy Rule.

Section 164.504(f) of the Privacy Rule spells out in detail the plan document amendments that must be made, and the compliance steps that must be taken. According to this section the employer must:

(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 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 paragraph¹

Self-Funded Plans

An employer with a self-funded plan is typically the plan administrator and is responsible for the health plans compliance with HIPAA privacy rules. An employer with a self-insured plan almost always has access to individually identifiable information. As with fully insured plans, the employer's health plan, not the employer itself, is a HIPAA Covered Entity.

Employers who sponsor self-funded plans (including Section 125 medical reimbursement account face a long list of compliance responsibilities. Over 30 specific requirements are included in the Privacy Rules. Examples include:

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. Fully insured plan receipts are the plans premiums. Small Health Plans must comply with the privacy rules by 4-14-2004, large plans must comply by 4-14-2003.

- Formally designate a Privacy Officer
- Send a Notice of Privacy Practices to covered individuals
- Amend plan documents
- Identify uses and disclosures that require an individuals authorization
- Implement procedures to administer authorizations when required
- Develop policies to respond to individual's rights required by the rules
 - Right to an accounting of certain uses and disclosures
 - Right to request limits on uses of PHI and confidential communications
 - Right to access to PHI
- Develop a number of required policies and procedures to protect the privacy of individuals PHI
- Train employees involved in the administration of the health plan
- Develop sanctions for privacy violations
- Enter into business associate agreements

Business Associate Agreements

An employer sponsored health plan must enter into a Business Associate Agreement with its broker; TPA and any other person or organizations which provide a service to the plan involving the use of PHI.² The deadline for this agreement is April 14, 2003 for large

¹ 45 C.F.R. §164.504(f)(2)(ii)

² 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...

health plans (or at contract renewal date under certain circumstances) or April 14, 2004 for small health plans. Fully insured health plans are not required to enter in to Business Associate Agreements with their insurance carrier or HMO.

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, its responsibilities are very limited.

If, however, an employer offers self-funded benefits (including Section 125 medical reimbursement 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.

Employers with large health plans have very little time and should take steps to get in compliance immediately. Employers who offer plans that qualify as Small Health Plans need to begin their compliance efforts now. April 14, 2004 is not as far away as it sounds!

Bob Radecki is a HR and benefits compliance consultant in Minneapolis, MN. Bob founded and for 10 years served as President of A.E. Roberts Company. He now spends his time helping employers, agents and brokers deal with a variety of compliance issues including HIPAA, COBRA and the FMLA (and looking for excuses to go skiing in the mountains!). Currently Bob is engaged as the principal HIPAA consultant for a number of major managed health care companies and runs a website which focuses on HIPAA and employer sponsored health plans at www.KnowHIPAA.com. Bob is also co-editor of the HIPAANow! Compliance Kit for Group Health Plans. For more information contact Bob at bradecki@knowhipaa.com or 612-581-6281.