Think You're Ready? Don't Forget the Self-insured Health Plan (HIPAA on the Job)

by Margret Amatayakul, RHIA, FHIMSS

Many providers are putting the finishing touches on their HIPAA privacy compliance activities—but may have overlooked their self-insured health plan or assumed that their third-party administrator (TPA) was taking care of HIPAA compliance. Now is the time to take a closer look at your self-insured health plan.

What Is a Self-insured Health Plan?

Many large employers (including hospitals, long-term care facilities, large physician practices, automotive and other manufacturers, and airline carriers) have found they can save money by self-insuring their employee health plans rather than purchasing coverage from private insurers. This self-insured health plan program is permitted under the Employee Retirement Income Security Act (ERISA), and may be known as an "ERISA plan." Self-insured health plans are considered group health plans (GHPs) and are subject to HIPAA regulations.

A group health plan, as defined by HIPAA (p. 82,799), is:

> an employee welfare benefit plan (as defined in...ERISA), including insured and self-insured plans, to the extent that the plan provides medical care..., including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise that:
>
> 1. Has 50 or more participants (as defined in...ERISA); or
> 2. Is administered by an entity other than the employer that established and maintains the plan.

As a practical matter, virtually all self-insured health plans are subject to HIPAA. Actuarial and cost considerations preclude employers with fewer than 50 participants (that is, employees or former employees eligible for benefits) from self-insuring. The Department of Health and Human Services (HHS) has stated that a health plan that uses a TPA is administered by another entity.

Note, however, that the privacy compliance date for a "small health plan" with receipts of $5 million or less has been extended by one year. HHS says that ERISA health plans should use proxy measures such as premiums or claims paid to calculate "receipts."

Employer versus GHP Responsibilities

Employers must grasp several crucial concepts and definitions to understand their HIPAA obligations. First, many GHPs are really only a piece of paper and most have no staff. The operations of the GHP are either contracted to a TPA, carried out by the employer's staff, or performed by the insurance issuer or health maintenance organization (HMO) from which the employer—through its GHP on paper—purchases benefits.

HHS, like ERISA, recognizes a distinction between the employer as plan sponsor and the insured or self-insured GHP maintained by the plan sponsor. The regulations do not directly regulate the employer. However, unless the employer complies with requirements outlined in the regulations, HIPAA restricts the GHP from disclosing protected health information (PHI) except for summary health information (SHI) to the employer or plan sponsor.

HIPAA appears to impose different obligations on insured and self-insured group health plans. An employer may provide health benefits through a GHP, health insurance issuer, or HMO. The preamble to the August 14, 2002 (p. 53,207), modification to the privacy regulations clarified that "an employer is not a hybrid entity simply because it is the plan sponsor of a group health plan.

The employer/plan sponsor and group health plan are separate legal entities and, therefore, do not qualify as a hybrid entity." The GHP, however, will have plan documents with the plan sponsor that establishes how the plan will be administered.

A self-insured health plan may—and usually does—delegate claims processing and other plan administration functions to a TPA or administrative services only (ASO) vendor. However, the TPA is not a covered entity; rather, it is a business associate of the GHP.

What Are GHPs' Responsibilities?

A GHP is subject to all HIPAA regulations (that is, transactions and code sets, identifiers, privacy, and security), although sometimes in unique ways. With respect to privacy, there are several specific requirements and exceptions for GHPs. For the transactions, the GHP must be able to accept and send standard transactions if any entity requests that the plan conduct standard transactions.

What Are the Specific Privacy Requirements?

"Compliance Responsibilities" summarizes the various scenarios in which insured and self-insured plans may operate and how their privacy rule compliance requirements vary.

Key to understanding the privacy requirements is first understanding who administers the plan and whether the plan receives PHI or only SHI. A GHP that is fully insured and receives only SHI and enrollment/disenrollment information avoids most of the responsibility for HIPAA compliance. However, if the insurer, HMO, or GHP provides PHI to the sponsor, the sponsor is required to certify that plan documents have been amended to incorporate privacy provisions. These certification requirements are summarized in "Amending Plan Administration Documents". In some respects, they are similar to provisions of a business associate agreement and include organizational separation requirements.

If the plan sponsor is self-insured and administers the plan in-house or retains final adjudication responsibility for claims, it is obviously handling claims and, therefore, PHI. It is critical that the plan be identified and separated organizationally from all other employment-related functions. These GHPs must amend their plan documents to make the necessary organizational separation. They must also ensure compliance with the other privacy requirements, including providing a notice of privacy practices, and with all administrative requirements, such as having an information privacy official, employing safeguards, having privacy policies and procedures, and more (see "Notice of Privacy Practices Requirements,").

If the self-insured plan uses a TPA, the type of information the plan receives must be established. If the TPA does not supply PHI to the plan sponsor, there is no need for plan documents to be amended to require organizational separation and certification.

Exercise caution here, however, because while the TPA may not directly supply PHI, some TPAs have made PHI available to the sponsor in the past. For example, a plan sponsor may have had access to claim information to assist employees with managing their claims. Many of these plan sponsors are now requesting that this access be discontinued and are referring their employees directly to the TPA for such assistance. When an employee voluntarily brings claim information to an employer or plan sponsor, the employee's authorization is implied. However, if the TPA supplies the plan sponsor with the information for the employee, the TPA should obtain an employee authorization.

For self-insured plans, because there is no insurance issuer or HMO, the plan sponsor is the GHP and must supply a notice of privacy practices and adhere to the administrative requirements. The TPA could draw up the notice, make the provision, provide the policies and procedures, and receive complaints, but it is the plan sponsor's responsibility to ensure the notice is accurate and has been provided and other requirements are met.

What Are the Transactions Requirements?

A GHP, as a covered health plan, must be able to accept ASC X12N and NCPDP (National Council on Prescription Drug Programs) standard transactions (for example, 837 claims or 270 eligibility inquiries) and return standard transactions (835 remittance advice or 271 eligibility response) if any entity requests the plan to conduct standard transactions.

Self-insured plans, whether self-administered or administered through a TPA, need to assess their capabilities to conduct the HIPAA transactions, and may need to analyze the costs and benefits of obtaining in-house translator software or using a clearinghouse. If a clearinghouse is chosen as the means to accept or return standard transactions, the plan may not pass the cost of the clearinghouse on to the provider. Plans also may not enter into any unilateral agreements with providers where they agree to use non-standard electronic transactions.

What Is the Bottom Line?

The regulations are complicated with respect to self-insured plans and careful consideration of exact relationships is needed. It is essential that providers and other employers understand their relationship to their GHP and determine what their TPA is doing on their behalf, that plan documents are amended appropriately, and that they will be compliant by the respective deadlines.

Glossary of Health Plan Terms

Compliance Responsibilities

	Plan Sponsor of Insured Plan		Fully Insured GHP (Insurance Issuer or HMO)		Self-insured GHP, Adminis-tered by Self	Self-insured GHP, Administered by TPA	
Sponsor receives	SHI	PHI	SHI	PHI	PHI	SHI	PHI
Plan amendment	No	Yes	No	Yes	Yes	No	Yes
Certification	No	Yes	No	Yes	Yes	No	Yes
Organizational separation	No	Yes	No	Yes	Yes	No	Yes
Notice of privacy practices	No	No	No	See "Notice of Privacy Practices Requirements"	See "Notice"	See "Notice"	See "Notice"
Administrative requirements	No	No	Some*	All	All	All	All

* The GHP that is fully insured and has only SHI is subject only to the administrative requirements of privacy that it must not retaliate against any individual for participating in any privacy process, must not require individuals to waive their privacy rights, and must maintain plan administration documents.

Amending Plan Administration Documents

For a GHP to disclose PHI to the plan sponsor or to permit the disclosure of such information to the plan sponsor by a health insurance issuer or HMO, the plan documents of the GHP must be amended to:

- Establish permitted and required uses of PHI by the plan sponsor
- Require a certification by the plan sponsor to:
  - not use or further disclose information other than as permitted or required
  - ensure that any agents or subcontractors agree to the same conditions
  - not use or disclose the information for employment-related actions
  - report to the GHP any use or disclosure of which it is aware that is inconsistent with the permitted and required uses and disclosures
  - make available PHI to individuals who request access
  - make available PHI for amendment
  - make available the information required to provide an accounting of disclosures

- make its internal practices, books, and records relating to the use and disclosure of PHI received from the GHP available to the secretary of HHS for determining compliance
- when no longer needed, return or destroy PHI
- ensure adequate separation between the GHP and the plan sponsor, including:

  - describing persons who may be given access to PHI
  - restricting access to plan administration functions
  - providing a mechanism for resolving issues of noncompliance

Notice of Privacy Practices Requirements

A notice of privacy practices describes the uses and disclosures of PHI that may be made by the covered entity and the individual's rights and covered entity's legal duties with respect to PHI. The content of the notice is specified in the HIPAA privacy regulations. Different requirements exist for provision of the notice with respect to the type of health plan and what information is created or received by the health plan:

- Health insurance issuers, HMOs, or government healthcare programs that provide or pay the cost of medical care must provide a notice of privacy practices to individuals covered by the plan no later than the privacy rule compliance date for the plan, at the time of enrollment for new enrollees, or within 60 days of a material revision to all individuals covered by the plan. Also, the health plan must notify individuals covered by the plan of the availability of the notice at least once every three years.
- GHPs that provide benefits solely through an insurance contract or HMO and create or receive PHI must maintain a notice and provide it to persons upon written request.

  If the GHP provides benefits solely through an insurance contract with a health insurance issuer or HMO and does not create or receive PHI other than SHI or only provides information on whether an individual is participating in the plan, it is not required to maintain or provide a notice of privacy practices.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "Think You're Ready? Don't Forget the Self-insured Health Plan." *Journal of AHIMA* 74, no.3 (2003): 16A-D.