

Medical Privacy BULLETIN

An Overview of HIPAA Privacy Requirements

Small Health Plans Must Comply with HIPAA Privacy Requirements by April 14, 2004



The HIPAA Privacy requirements apply to “small” plans (under \$5 million in annual receipts) as of April 14, 2004. Many small plans already may be aware of these requirements, since they have applied since April 14, 2003, to large plans and other “covered entities” (CEs), such as health insurance companies. In fact, many small plans already may have been forced to comply with some of the privacy requirements as a result of the earlier date for health insurance companies. This Marsh Privacy Bulletin details the HIPAA privacy requirements and what they will require of:

- Small fully insured plans that receive only summary health information and enrollment/disenrollment information, but not “protected health information” (PHI)
- Small plans—both insured and self-funded—that do receive PHI.

HIPAA Privacy Compliance Checklist

The following items must be completed before April 14, 2004

Note: The Plan sponsor is almost always the plan administrator and acts on behalf of the Plan.

INSURED PLAN

Whether or not you will get PHI, you must:

- Appoint a PRIVACY SPECIALIST to coordinate privacy issues and to determine if the Plan wants access to PHI.
- Have a policy not to retaliate or discriminate against, or intimidate any participant who exercises his/her privacy rights.
- Have a policy not to require anyone to waive his/her privacy rights as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits.
- Verify that each carrier distributes a PRIVACY NOTICE to all enrollees in that coverage.
- Contact carrier to determine what reports and information you will get if you want PHI and what reports and information you will get if you elect not to get PHI.

If you WILL get PHI, you must
do all of the above, and also:

- AMEND your plan document (your carrier probably has a sample) to specify those employees or categories of employees whose job responsibilities include managing and administering the plan (who are “behind the firewall”).
- Execute a CERTIFICATION that you have amended your plan document and implemented the required provisions.
NOTE: Most carriers will require that you file a copy of the Certification with the carrier, but they do not want copies of plan amendments.
- Establish POLICIES and PROCEDURES to govern how you will handle the PHI you receive.
- TRAIN those EMPLOYEES who are “behind the firewall”—and those employees who work in close proximity to them—regarding the Plan’s privacy policies and procedures.
- Execute a BUSINESS ASSOCIATE AGREEMENT with your broker and with other BAs to whom the plan will disclose PHI.
- Have and apply SANCTIONS against workforce members who violate the Plan’s privacy policies and procedures.
- Appoint a PRIVACY OFFICIAL for the Plan.
- Have a PRIVACY NOTICE, but you need not distribute it except upon request

SELF-FUNDED PLAN

Whether or not plan (sponsor) wants PHI,
a self-funded plan must:

- Appoint a PRIVACY OFFICIAL for the Plan, to ensure the plan complies with the Privacy Rule.
- Have a policy not to retaliate or discriminate against, or intimidate any participant who exercises his/her privacy rights.
- Have a policy not to require anyone to waive his/her privacy rights as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits.
- Distribute a PRIVACY NOTICE to all employees enrolled in the Plan. Many TPAs will provide sample Privacy Notices, and some will also mail out the Notices.

The plan sponsor, on behalf of the Plan, must:

- AMEND your plan document (your TPA or broker probably have a sample) to specify those employees or categories of employees whose job responsibilities include managing and administering the plan (who are “behind the firewall”).
NOTE: Most TPAs will want copies of plan amendments.
- Execute a CERTIFICATION that you have amended your plan document and implemented the required provisions.
NOTE: Some TPAs & stop-loss carriers will want a copy of the Certification.
- Establish POLICIES and PROCEDURES to govern how employees “behind the firewall” will handle PHI.
- TRAIN those EMPLOYEES who are “behind the firewall”—and those employees who work in close proximity to them—regarding the Plan’s privacy policies and procedures.
- Execute a BUSINESS ASSOCIATE AGREEMENT with your TPA, broker and with other BAs to whom the plan will disclose PHI.
- Have and apply SANCTIONS against workforce members who violate the Plan’s privacy policies and procedures.
- HEALTH FSAs are self-funded plans and must comply with all these requirements. Arguably, however, a plan does not need policies and procedures for those functions it has contracted out to an FSA administrator. (e.g., The FSA administrator must have policies & procedures to protect PHI disclosed to it for claims processing purposes.)

Overview of HIPAA Privacy Requirements

The Privacy Rule prohibits “covered entities” (CEs), such as group health plans, from using or disclosing PHI except:

- pursuant to an Authorization;
- for treatment, payment or health care operations (TPO);
- to the individual to whom the PHI pertains; or
- for other specified purposes, including but not limited to public health and safety, to law enforcement officials, pursuant to a judicial order, or as required by another law.

Even if a group health plan uses PHI for the allowable purposes of payment or health care operations, it cannot disclose PHI to the health plan sponsor unless the sponsor has executed a plan amendment and certification and established safeguards to protect the privacy of PHI. A plan sponsor that will not receive PHI is not required to execute a plan amendment or certification nor to establish safeguards. Additionally, a group health plan cannot disclose PHI to a “business associate” (BA) except pursuant to a business associate agreement (BAA). A BA is an entity that performs a covered function on behalf of, or a service for, a CE and that uses PHI in doing so. Examples of BAs include brokers, TPAs, attorneys, and consultants.

Another basic provision under the Privacy Rule is that individuals have specified rights to access and control how their PHI is used

and disclosed. Additionally, CEs must respond to and act upon individuals’ requests regarding their PHI. For group health plans, this means:

- Plans must provide Notices of Privacy Practices to plan participants that clearly explain how the CE can use and disclose their PHI;
- Plans must allow participants to access and copy their PHI upon request;
- Participants may request amendments to their PHI;
- Participants may request restrictions on the uses and disclosures of their PHI and may request confidential communication of their PHI;
- Plans must log many of their uses and disclosures of participants’ PHI, because patients/participants may request an accounting of such uses and disclosures; and
- Participants can file complaints with Health and Human Services (HHS) if they believe their privacy rights have been violated.

Obligations of Health Plan Sponsors

The Privacy Rule itself imposes obligations only on CEs; group health plans are one category of CEs. Since most single-employer group health plans are merely written documents and have no employees, they can act only through those employees of the plan sponsor whose job

responsibilities include managing the plan. It is these people who must ensure the plan’s compliance with the Privacy Rule. Those employees of the plan sponsor who are responsible for managing and administering the health plan are often said to be “behind the fire-wall.” These individuals use and disclose PHI in managing and administering the plan. They act as “plan employees” when they ensure the plan is compliant with the Privacy Rule, although they are actually on the plan sponsor’s payroll. These individuals must be familiar with the Privacy Rule, and they must receive training on the plan’s privacy policies and procedures. A plan sponsor who has employees “behind the firewall” must execute a plan amendment and certification, establish safeguards, have a Privacy Notice and implement policies and procedures regarding PHI.

In order to determine whether its group health plan does or will want to have access to PHI, each plan sponsor should appoint or hire a “privacy specialist” at the very least, and those who will have PHI are required by the Privacy Rule to have a “Privacy Official.” For a self-funded plan, the employer must appoint a Privacy Official for the plan. In a fully insured plan, the (or each) carrier must appoint a Privacy Official, because each carrier is also a CE. If the plan sponsor of a fully insured plan will have PHI, it also must appoint a Privacy Official for the plan. Even if a plan sponsor of a fully insured plan elects that it and the plan will not have PHI, it should appoint or hire a “privacy specialist” who can:

- determine what, if any, PHI the plan and sponsor have in the past had access to;
- determine what, if any, PHI the plan and sponsor want to have going forward;
- monitor the information received and ensure the plan and sponsor do not inadvertently obtain or disclose PHI;
- set up privacy-related policies, procedures and files, such as use and retention of Authorizations (if the plan sponsor does assist employees with claims issues), and procedures to mitigate the effects of improper disclosures (should they occur);
- monitor legal changes and ensure policies and procedures change if required by legal changes; and
- coordinate with the carrier's contact person and ensure the plan sponsor has copies of the carrier's Privacy Notice.

Privacy Requirements on Fully Insured Health Plans with No PHI

Fully insured plans with no PHI are exempt from most—but not all—of the HIPAA privacy requirements. Specifically, the HIPAA regulations (at 164.530(k)) significantly limit the compliance requirements for group health plans that:

- Provide health benefits solely through an insurance contract with a health insurance issuer or an HMO, and

- do not create or receive PHI, except for summary health information (SHI), or information on whether an individual is participating in the group health plan or is enrolled or disenrolled from an insurance contract or HMO offered by the plan (summary health information summarizes claims history, claims expenses, or types of claims generally).

Such group health plans are not subject to the standards or implementation specifications in paragraphs (a) – (f) or (i) of section 164.530. The insurance carrier or HMO is required to meet these requirements, but the employer's group health plan is not separately required to meet them. Specifically, **fully insured plans with no PHI are NOT required to:**

- a) Designate a privacy official.
- b) Train workforce members as appropriate.
- c) Have administrative, physical, and technical safeguards to protect PHI.
- d) Have a complaint process.
- e) Have and apply sanctions to workforce members who do not comply.
- f) Mitigate any harmful effects of disclosure of PHI (because they do not have PHI).
- i) Have policies and procedures with respect to PHI.

Privacy Notices: The regulations (at 164.520(a)(iii)) also provide that, for a fully-insured plan, the carrier or HMO is required to provide the Privacy Notice to enrollees. If the plan sponsor does not receive or

create PHI (other than SHI), the plan sponsor is not required to create or distribute a Privacy Notice. However, if a fully insured plan also creates or receives PHI, the plan must have a separate Privacy Notice but is required to distribute it only to those participants who request a copy.

Practical Note: *Some carriers have sent letters to plan sponsors asking them to distribute the Privacy Notice to participants and to sign a form agreeing to take this responsibility. You are not required to sign such a form or to distribute the carrier's Privacy Notice if your plan does not receive PHI, unless you have obligated yourself in the contract with the carrier to distribute notices on the carrier's behalf.*

Business Associate Agreements:

A plan sponsor of a fully-insured plan that does not intend to use or disclose PHI will not need to execute business associate agreements (BAAs) on behalf of the plan, because the plan will have no business associates (BAs). This is because a BA is an entity or individual that performs covered services for or on behalf of a CE and uses PHI in performing such services. If a vendor (such as a broker) does not have access to PHI, the vendor is not a BA under HIPAA, and no BAA is required.

Plan Amendment and Certification:

A plan sponsor who will not receive PHI, except for SHI or enrollment and dis-enrollment information, is not required to amend its plan document, and obviously is not required to certify to the plan that it has amended the document.

Although relieved of most Privacy obligations, an insured plan with no PHI does have to comply with the following HIPAA requirements:

- Refrain from intimidation or retaliatory acts against individuals who exercise their privacy rights or file complaints with HHS (164.530(g)); and
- Not require individuals to waive their privacy rights as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits (164,530(h)).

It is not clear if a separate statement of compliance with the above two requirements must be issued; however, it is advisable that a plan sponsor state its compliance in its SPD or in a separately-issued one-page summary of material modifications (SMM).

The regulations rather cryptically require that insured plans with no PHI also must maintain policies and procedures and copies of documentation (as required in 164.530(j)), but only with respect to plan documents amended in accordance with 164.504(f). Since 504(f) only requires that plans be amended if they will disclose PHI to the plan sponsor or permit the carrier or HMO to disclose PHI to the plan sponsor, this reference seems contradictory since an insured plan with no PHI will not have to be amended in accordance with 504(f).

It is unclear what HHS intended by this reference.

Additionally, a plan sponsor of a fully insured plan should obtain the name and contact information of each carrier's Privacy Official and complaint contact persons, and should verify with the carrier(s) that they will provide Privacy Notices to participants.

Privacy Requirements on Fully Insured Health Plans With PHI or Self-Funded Plans

Fully insured and self-funded plans that use or disclose PHI are required to comply with all the privacy requirements. Note that because most single-employer health plans have no employees, they can only "act" through the plan sponsor's employees who are "behind the firewall" (and also through third-party administrators that contract to administer claims, for self-funded plans). Thus, requirements listed below that are imposed on the plan are actually implemented by those plan sponsor employees who are "behind the firewall" and are responsible for plan administration and management.

Execute a plan amendment and certification: A plan sponsor who wants to have access to PHI must amend its plan document to specify the employees or categories of employees who are "behind the firewall" and will have access to PHI and the purpose for which they will have access, and to include several other provisions required by the Privacy Rule. The plan sponsor also must establish safeguards to make sure the PHI will be used only as allowed by the

Privacy Rule or as required by law, and that only those employees whose job responsibilities require them to have access to PHI will have such access. Additionally, the plan sponsor must certify to the plan that these actions have been taken. This rule applies to both insured and self-funded plans, if the plan sponsor wants to have access to PHI.

Fully insured plan. Sponsors should check with their carriers to find out what information or reports the carrier(s) will provide if the sponsor amends its plan document and if it does not amend it. Additionally, many carriers provide sample plan amendments and certifications that plan sponsors can customize.

Self-funded plan. Many TPAs and brokers provide sample plan amendments and certifications that sponsors can customize.

Execute Business Associate Agreements (BAAs): The Privacy Rule allows CEs to disclose PHI to BAs only pursuant to a written BAA, even if the purpose of the disclosure is treatment, payment or healthcare operations (TPO). As noted above, a BA is an entity that uses PHI in providing a service or acting on behalf of a CE and helping the CE perform a covered function (such as payment or health care operations). Examples of BAs to group health plans include brokers, TPAs, attorneys and accountants.

Fully insured plan. The plan sponsor should sign a BAA on behalf of the plan with the broker

or consultant. A BAA is not appropriate between the carrier and the plan or the plan sponsor.

Self-funded plan. The plan sponsor should sign a BAA on behalf of the plan with the TPA, the broker or consultant, and with other entities that qualify as BAs. HHS has said that a stop-loss carrier is not a BA merely because it provides stop-loss; however, it may be a BA if it provides other services on behalf of or to the plan. Some stop-loss carriers want to sign BAAs if they provide case management or transplant centers of excellence; other stop-loss carriers refuse to sign BAAs. Either way is acceptable.

Designate a Privacy Official:

Fully insured plan. If the plan or sponsor will receive PHI, the plan sponsor must designate a Privacy Officer for the plan. Additionally, the (or each) carrier will designate a Privacy Official for its benefits, because a carrier or HMO is also a CE and is subject to the requirement to designate a Privacy Official.

Self-funded plan. The plan sponsor must designate a Privacy Official for the plan. This should be a position with the plan sponsor that is sufficiently senior to implement required policies and procedures to protect PHI, to require compliance with privacy requirements, and to apprise senior management of privacy requirements.

Plan with both insured and self-funded components. The plan sponsor must designate a Privacy Official for the plan overall, and each carrier should designate a

privacy official regarding the benefits it provides. An example of such a plan would be one that offers insured health coverages plus a health FSA in a consolidated plan (i.e., one plan number for Form 5500 filing purposes).

Have a complaint process and a contact person:

Fully insured plan. The (or each) carrier will have a complaint process and a contact person for complaints about how that carrier has handled PHI, and this will be noted in the carrier's Privacy Notice. Additionally, the plan must have a complaint process and a contact person, since the plan also will have PHI. The plan's complaint process may be to forward privacy complaints about a particular carrier to that carrier's contact person; however, many plan sponsors will want to get involved to help ensure that complaints are resolved before the individual files a complaint with HHS.

Self-funded plan. The plan must have a complaint process and a contact person for complaints, and this will be noted in the plan's Privacy Notice. To the extent a self-funded plan contracts with a TPA to handle all or most PHI (i.e., making benefit determinations), the plan can contract with the TPA to also provide a complaint process and contact person for complaints regarding the TPA's handling of PHI. The plan must have its own complaint process and contact person for functions the plan performs rather than contracts out to a BA. As noted above, many plan sponsors

will want to get involved to ensure complaints are resolved before the individual files a complaint with HHS.

Send Privacy Notices to

Participants: **Fully insured plan.**

The (or each) carrier or HMO must send a Privacy Notice to participants enrolled for coverage from that carrier or HMO. Additionally, a plan sponsor that uses or discloses PHI also must have a Privacy Notice available, but is only required to send it to participants who request it.

Self-funded plan. The plan sponsor of a self-funded plan must ensure that Privacy Notices are sent to plan participants. Many TPAs will provide sample Notices, and some even customize them and send them to participants.

Have policies and procedures

with respect to PHI: **Fully insured plan.** Both the carrier or HMO and the plan sponsor must have policies and procedures with respect to the PHI they each use or disclose.

Self-funded plan. Both the TPA and the plan sponsor must have policies and procedures with respect to the PHI they each use or disclose. Many attorneys believe a plan that contracts out covered functions to a business associate (BA) (e.g., hires a TPA to administer the plan) is not required to have separate or duplicative policies and procedures covering those functions the plan has contracted out to the BA. There is disagreement as to whether the

plan simply is not responsible for compliance for those functions it contracts out, or whether a plan can comply by stating in the plan's policies and procedures that the (or each) BA is responsible for implementing HIPAA-compliant policies and procedures for those functions it has contracted to perform. For example, if a self-funded group health plan contracts with a TPA to administer claims, send Privacy Notices, respond to individuals' privacy rights, and have safeguards to protect PHI handled by the TPA, the plan does not need separate policies and procedures in addition to those of the TPA.

Train workforce members

as appropriate: Fully insured plan. Both the carrier or HMO and the plan sponsor must train employees who will be using and disclosing PHI on the applicable privacy policies and procedures.

Self-funded plan. Both the TPA and the plan sponsor must train those employees who will be using and disclosing PHI on the applicable privacy policies and procedures.

Have and apply sanctions to workforce members who do not comply:

Fully insured plan. Both the carrier or HMO and the plan sponsor must have and apply sanctions to workforce members who do not comply with their privacy policies and procedures.

Self-funded plan. Both the TPA and the plan sponsor must have and apply sanctions to workforce members who do not comply

with their privacy policies and procedures.

Implement administrative, physical, and technical safeguards to protect PHI:

Fully insured plans and self-funded plans. Carriers, HMOs, plan sponsors and TPAs that handle PHI all must implement administrative, physical and technical safeguards to protect the PHI they handle. An example of an administrative safeguard is a policy regarding who has access to PHI. An example of a physical safeguard is locks on filing cabinets containing PHI. Examples of technical safeguards include passwords, and encryption of electronic data at rest and data sent over the internet.

Obtain authorization forms

before disclosing PHI: A CE can only disclose PHI to a plan sponsor or other third party pursuant to an authorization form, except for specified purposes (such as payment or health care operations). For a group health plan, the need for an authorization form usually arises when a plan sponsor assists employees with claims resolution issues. This function can be handled in one of two ways:

- 1) In the plan amendment, the plan sponsor can specify that one of the payment or health care operations functions the employees "behind the firewall" perform is assisting plan participants with claims resolutions issues. Under this method, it should not be necessary to secure an authorization each time the employer assists with

claims resolution. If a broker is also involved in this function, the broker must sign a BAA with the plan before the plan can share PHI with the broker.

- 2) If there is no plan amendment, if the plan amendment does not include this as one of the purposes for which PHI may be disclosed to the plan sponsor, or if the carrier or a provider refuse to disclose PHI pursuant to a plan amendment, the plan sponsor can obtain an authorization from the affected participant each time the plan sponsor assists with a claims issue.

Fully insured plan. Most carriers have implemented procedures under which they will not require an authorization to disclose PHI regarding claim status (i.e., received, pending, paid) to those plan sponsor employees who are designated in the plan amendment as being "behind the firewall" and who have certain information about the claim at issue (i.e., name, date of birth, date of services). However, they will require an authorization to disclose any additional PHI.

Self-funded plan. Policies vary as to what various TPAs will require before disclosing PHI to plan sponsor employees who are "behind the firewall."

Mitigate any harmful effects

of disclosure: Fully insured plans and self-funded plans. Carriers, HMOs, plan sponsors and TPAs that handle PHI all must mitigate any harmful effects of a known unauthorized disclosure of PHI. Examples

of mitigation include strengthening policies to protect PHI, requiring additional training of workforce members to prevent future unauthorized disclosure, and implementing additional physical and technical safeguards to prevent future unauthorized disclosure.

Application of Privacy Requirements to Health Flexible Spending Accounts (FSAs)

Health FSAs are self-funded plans and must comply with the requirements noted above. This may pose a challenge for an employer who offers a health FSA in addition to fully insured benefits and who has elected not to receive PHI. Such an employer may wish to specify in the plan's BAA with the FSA administrator that the administrator will handle all PHI on behalf of the plan and will fulfill many of the privacy requirements listed above on behalf of the plan. Specifically, the above requirements apply as follows:

The plan/sponsor is responsible to:

- Sign a BAA on behalf of the FSA plan with the FSA administrator;
- Designate a Privacy Official;
- Ensure Privacy Notices are sent to FSA plan participants (sponsor can send on behalf of plan or can contract with FSA administrator to send the Notices);
- Train workforce members as appropriate (should train HR employees whose responsibilities include the FSA plan, even if the intent is that they will not have PHI).

The FSA administrator (the BA) is responsible to:

- Have a complaint process and a contact person;
- Have policies and procedures relating to PHI;
- Train workforce members as appropriate;

- Have and apply sanctions to workforce members who violate the BA's policies and procedures;
- Implement administrative, physical, and technical safeguards to protect PHI;
- Mitigate any harmful effects of disclosure.

If the FSA plan will not disclose PHI to the plan sponsor, it is not necessary that the sponsor execute a plan amendment or certification, nor that the plan or sponsor mitigate any harmful effects of a known disclosure of PHI (as long as the plan and sponsor will not have PHI). Additionally, as noted previously, many attorneys believe that a plan must have policies and procedures only with respect to functions it performs but not with respect to those it contracts out to a BA to perform. Additional guidance from HHS would be helpful.

Copyright 2004 Marsh Inc.

All rights reserved.