

# THE HIPAA PRIVACY RULE: How it Affects Sponsors of Group Health Plans

**DISCLAIMER:** This information is provided “as is” without any express or implied warranty. It is provided for educational purposes only and does not constitute legal advice. If you require legal advice, you should consult with an attorney.

An employer who sponsors a group health plan (“GHP” or “plan”) will most likely be impacted by the health privacy regulations implemented pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The HIPAA Privacy Rule (“the Rule”) imposes restrictions on the use and disclosure of protected health information (“PHI”) by certain “covered entities,” which include group health plans sponsored by employers. Thus, while the Privacy Rule does not apply directly to employers, most employers will nonetheless be affected because the Rule applies to the group health plans they sponsor.

**Compliance Deadline.** The deadline for compliance with the Privacy Rule is April 14, 2003 for most covered entities, while small health plans (those with annual gross receipts of less than \$5 million) will have an additional year to comply.

**Definition of PHI.** Under the Privacy Rule, PHI is defined as “individually identifiable health information,” whether maintained or transmitted on paper, in electronic format or orally. “Individually identifiable health information” is any information that permits the identification of an individual or could be used, alone or in combination with other available information, to identify the individual and that: (1) was created or received by a health care provider, health plan, health care clearinghouse or employer; and (2) relates to the individual’s past, present or future physical or mental health or condition, or the provision of or payment for the individual’s health care.

**State Law Preemption.** The Privacy Rule provides a national privacy “floor.” Generally, to the extent that a state law is contrary to the Rule, then the state law is preempted by the Privacy Rule. However, if a state law is “more stringent” than the Rule regarding the privacy of health information, then the state law is not preempted. (For example, if a state law prohibits or restricts a use or disclosure of PHI that would be permitted under the Rule, or if it gives individuals greater rights of access or amendment to their PHI, then the state law would not be preempted.)

**Business Associates.** Under the Rule, a business associate is an entity or individual who uses or discloses PHI to perform a function or service on behalf of a covered entity such as a GHP. Plans are required to have written contracts with their business associates before PHI can be disclosed to them. Among other things, this business associate contract must:

- Include the permitted and required uses and disclosures of PHI by the business associate, and to whom further disclosures can be made;
- Prohibit the business associate from using or disclosing the PHI other than as permitted under the contract or by law;
- State that the business associate will use appropriate safeguards to prevent the improper use or disclosure of PHI;

- State that the business associate will report to the plan any unauthorized use or disclosure of PHI of which it becomes aware;
- Require the business associate to contractually impose all of these same PHI requirements on all of the business associate’s subcontractors;
- Require the business associate to abide by an individual’s new rights regarding their PHI;
- Require the business associate to return or destroy the plan’s PHI, if feasible, at the termination of the relationship; if not feasible, then the business associate must extend its protections of the PHI for as long as it retains it; and
- Allow the plan to terminate the contract if the business associate has materially violated it.

## 1. Disclosing Health Information to Plan Sponsors

As mentioned above, an employer will generally not be considered a covered entity under HIPAA. However, the privacy requirements of HIPAA will impact plan sponsors by controlling a group health plan’s ability to share PHI with its plan sponsor, so employers/plan sponsors will indirectly be affected by the Rule, often to a significant extent.

The Rule generally prohibits a GHP from sharing PHI with a plan sponsor, except for the following:

- Disclosing “summary health information” for purposes of insurance placement, and for modifying, amending, or terminating the plan [see section A. below];
- Disclosing GHP enrollment and disenrollment information [see section B. below];
- Disclosing PHI to plan sponsor personnel that are involved in plan administration when the sponsor complies with the Rule’s administrative requirements [see section C. below]; and
- Disclosures made pursuant to a valid authorization [see section D. below].

With the exception of disclosures made pursuant to a valid authorization, the above disclosures are subject to the “minimum necessary” provisions of the Rule, which basically state that a covered entity must reasonably ensure that the amount of PHI that is used, disclosed, or received is the minimum amount necessary to accomplish the intended use, disclosure, or request.

Under the Rule, GHP’s are specifically prohibited from disclosing PHI to a plan sponsor for employment-related actions or decisions or in connection with any other benefit, unless an authorization is received from the individual.

### A. Summary Health Information: Limited Disclosure to Plan Sponsor Allowed

“Summary health information” is information that summarizes the claims history, expenses, or types of claims by individuals for whom the plan sponsor has provided benefits under a GHP.

Summary health information may contain certain individual identifiers, but it must be at least partially de-identified. The entity disclosing this information must remove the following 18 specific identifiers:

- Names;
- All geographic subdivisions smaller than a state, *except for aggregated five-digit ZIP codes*;
- All elements of dates (except year) for dates directly related to an individual, and all ages over 89;
- Telephone numbers;
- Fax numbers;

- Email 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 URL's;
- Internet Protocol (IP) addresses;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

A GHP, or its health insurer, HMO, or TPA, is allowed to disclose “summary health information” to the plan sponsor, if requested, for only two purposes: a) obtaining premium bids for providing health insurance coverage under the GHP; or b) modifying, amending, or terminating the GHP. Summary health information may be disclosed for these two reasons without the plan having to satisfy the plan document amendment and firewall requirements described in section C. below, and may be disclosed even if the information is not completely “de-identified.”

## **B. GHP Enrollment Information: Disclosure to Plan Sponsor Allowed**

The preamble to the Rule states that GHP's and insurers will be able to disclose enrollment/ disenrollment information to a plan sponsor without the plan having to satisfy the plan document amendment and firewall requirements described in section C. below. The newly finalized modifications to the Rule clarify that a GHP, or its health insurer or HMO (or TPA), may disclose information regarding whether an individual is participating in the plan, or is enrolled in or has disenrolled from a health insurer or HMO offered by the plan, to a plan sponsor. Such information may be disclosed to the plan sponsor without the plan having to satisfy the plan document amendment and firewall requirements.

## **C. Plan Document Amendment and Firewall Requirements: Disclosures to Plan Sponsor of PHI Beyond Summary Health Information and Enrollment Information**

As described in sections A. and B. above, a group health plan (or its health insurer, HMO, or TPA) may disclose summary health information and enrollment/disenrollment information to the plan sponsor. Additionally, a plan (or its health insurer, HMO, or TPA) may disclose PHI to a plan sponsor for “plan administration functions,” but only after the plan sponsor jumps through certain hoops and agrees to amend the plan documents to limit the uses and disclosures of the PHI. The plan documents must be amended to:

1. Describe the permitted and required uses and disclosures of PHI by the plan sponsor.
2. Specify that disclosure of PHI by the plan to the plan sponsor is only permitted upon receipt of the plan sponsor's written certification that the plan documents have been amended to include the following provisions, and that the plan sponsor agrees to:
  - Not use or further disclose PHI other than as permitted or required by the plan documents or as required by law;

- Ensure that any agents or subcontractors to whom it provides PHI received from the plan agree to the same restrictions and conditions regarding such PHI that apply to the plan sponsor;
  - Not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan;
  - Report to the plan any use or disclosure of the PHI that is inconsistent with the uses or disclosures provided for of which it becomes aware;
  - Make PHI available to allow individuals to access and request changes to their PHI, and upon request, provide them with an accounting of disclosures of their PHI;
  - Make its internal practices, books, and records relating to the use and disclosure of PHI received from the plan available to the Secretary of DHHS to determine the plan’s compliance with the Rule; and
  - If feasible, return or destroy all PHI received from the 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 the 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 PHI infeasible.
3. Provide adequate firewalls to: identify the employees or classes of employees who will have access to PHI; restrict access solely to such employees and only for the “plan administration functions” performed on behalf of the plan; and provide a mechanism for resolving issues of noncompliance.

“Plan administration functions” are those activities that would meet the definition of “payment” or “health care operations” under the Rule, including functions such as quality assurance, claims processing, auditing, and monitoring. “Plan administration functions” do not include employment-related functions or functions in connection with other benefits, however. Disclosures for those types of purposes would require an authorization from the individual.

Once a plan sponsor certifies to the GHP that the plan documents have been appropriately amended to include the above items, the GHP is permitted to rely upon that certification.

#### **D. Disclosures Made Pursuant to an Authorization**

Group health plans may use and disclose PHI with an individual’s valid, HIPAA-compliant authorization for any purpose specified in the authorization. However, plans may not condition treatment, payment, enrollment, or eligibility on the provision of an authorization, except:

- A health plan may condition enrollment or eligibility on provision of an authorization, as long as the authorization is requested prior to enrollment in the health plan, and only if the authorization sought is for the health plan’s eligibility or enrollment determinations, or for the purposes of underwriting or risk determinations; and
- A health plan may condition payment of a specific claim on provision of an authorization if the disclosure is necessary to determine payment of the claim, and is not for a use or disclosure of psychotherapy notes.

*A plan sponsor’s responsibilities under the Privacy Rule will vary, depending on whether the plan is fully-insured or self-funded, and if fully-insured, on how much health information the plan sponsor wishes to receive. Self-funded plans are generally subject to the most requirements under the Rule:*

## 2. Self-Funded Group Health Plans

A group health plan that is not fully-insured will be subject to the full requirements of the HIPAA Privacy Rule. The core requirements of the Rule can be grouped into three main categories: use and disclosure rules; individual rights and privacy notice; and administrative requirements.

### A. Use and Disclosure Rules:

**Uses and Disclosures of PHI** – PHI may not be used or disclosed by a group health plan except as follows (the Rule contains detailed information on each of these):

- To the individual (in accordance with the right to access and inspect PHI);
- For “payment” or “health care operations;”
- To family members or close personal friends for care or payment for care, after the individual has an opportunity to agree or object;
- In accordance with an authorization from the individual; and
- As required or permitted under the Privacy Rule for public policy or legal reasons.

**Payment and Health Care Operations** – These two broad categories are intended to encompass most of the reasons for which a plan would need to use or disclose PHI:

“Payment” is an activity undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for provision of benefits under the health plan, or to obtain or provide reimbursement for health care.

“Health care Operations” means activities such as internal quality oversight review, credentialing and health provider evaluation, underwriting, insurance rating and other activities relating to creation, renewal, or replacement of a contract of health insurance or health benefits (including stop-loss insurance and excess of loss insurance), medical review, legal services, and auditing functions (including fraud and abuse detection), business planning, management and general administration and fundraising.

**Minimum Necessary** – Most of these permitted uses and disclosures of PHI are subject to the Rule’s “Minimum Necessary” standard, whereby a group health plan must reasonably ensure that PHI that is used, disclosed or received is the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request. Disclosures to the individual who is the subject of the PHI are not required to comply with the minimum necessary standard.

### B. Individual Rights and Privacy Notice:

**Individual Rights** – Several new rights are granted under the Rule to individuals regarding their own PHI, including the right to:

- Access, inspect and copy their own PHI, with limited exceptions; plans may charge a reasonable fee for copying, mailing, or summarizing the information;
- Amend or correct inaccurate or incomplete PHI ;
- Request restrictions on the use and disclosure of PHI; plans are not required to agree to such a request, however;
- Request and receive (if the request is reasonable) confidential communications of PHI by alternative means or at alternative locations;

- Obtain a paper copy of the plan’s privacy notice upon request; and
- Receive an accounting of disclosures of PHI made within the past six years, with certain exceptions (though this right largely disappears under the Final Modifications to the Privacy Rule, published 8/14/02).

**Privacy Notice** – Group health plans will be required to create a notice of the plan’s privacy practices regarding PHI, and to distribute it to enrollees by the Rule’s compliance date (April 14, 2003 for most plans). After that, the privacy notice must be provided to new enrollees at the time of enrollment in the plan, and to all enrollees within 60 days after a material change to the privacy notice. Also, plans must notify enrollees at least once every three years that they have a right to receive a copy of the plan’s privacy notice.

The Rule describes the specific elements required of a plan’s privacy notice. The notice must:

- Be written in plain language;
- Contain specific language found in the Rule as a header or prominently displayed;
- Provide a sufficiently detailed general description of the plan’s uses and disclosures of PHI;
- Separately describe certain types of uses and disclosures, if the plan intends to engage in any such uses or disclosures (for example, that the plan may disclose PHI to the plan sponsor);
- Contain a statement of the individual’s rights with respect to their PHI and a brief description of how the individual may exercise these rights;
- Contain certain statements regarding the plan’s duties under the Rule with respect to PHI;
- State that individuals may complain to the plan or to DHHS if they believe their privacy rights have been violated, describe how to file a complaint, and state that the plan will not retaliate against an individual for filing a complaint;
- Provide the name (or title) and telephone number of a person or office to contact for further information; and
- Contain the date on which the privacy notice is first in effect.

### **C. Administrative Requirements:**

**Privacy Official and Contact Person** – Group health plans must designate a privacy official responsible for the development and implementation of privacy policies and procedures. Plans must also designate a contact person (who may or may not be the same as the privacy officer) or office for receiving complaints and providing additional information regarding the plan’s privacy notice.

**Training** – Group health plans must train all workforce members on the plan’s privacy policies and procedures. If such policies and procedures are materially changed, then retraining must occur. Plans must maintain documentation of the training.

**Safeguards** – Plans must have in place, or develop, appropriate administrative, technical, and physical safeguards to protect PHI from being used or disclosed in violation of the Privacy Rule. This section of the Privacy Rule overlaps with the Proposed Security Rule, which is expected to be finalized in the near future.

**Complaints** – Group health plans must provide a process for individuals to make complaints concerning the plan’s privacy policies and procedures, and must document all complaints received and their disposition, if any.

**Sanctions** – Plans must have and apply appropriate sanctions against workforce members who fail to comply with the plan’s privacy policies and procedures. Plans must document the sanctions that are applied, if any.

**Mitigation** – Plans must mitigate, to the extent possible, any harmful effect known to the plan of a use or disclosure of PHI, by the plan or its business associate, that violated the plan’s privacy policies and procedures.

**No Intimidation** – Plans may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals or others for exercising their rights under the Rule, filing a complaint, participating in an investigation, or opposing any improper practice under the Rule. This requirement even applies to all fully-insured group health plans.

**No Waivers** – Plans cannot require individuals to waive their rights under the Rule as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits. This requirement even applies to all fully-insured group health plans.

**Documentation of Policies and Procedures** – Plans must create and implement policies and procedures with respect to PHI that are designed to comply with the Privacy Rule. These policies and procedures must be reasonably designed to ensure compliance, taking into account the size of the group health plan and the types of activities relating to PHI that the plan undertakes.

Plans must document their privacy policies and procedures and maintain such documentation for at least six years. This requirement even applies to all fully-insured group health plans

### 3. Fully-Insured Group Health Plans

As mentioned earlier, the impact of the HIPAA Privacy Rule on a fully-insured group health plan will depend upon how much health information the plan wishes to receive.

**Plan Sponsor Has NO Access to PHI.** If a plan provides health benefits solely through an insurance contract and does not create, maintain, or receive PHI (other than summary health information or plan enrollment/disenrollment information), then the plan will not need to comply with most of the Administrative Requirements of the Rule [see II. C. above]. The exceptions are for the No Intimidation, No Waivers, and Documentation provisions – these apply to all group health plans regardless of what health information the plan receives.

Also, the plan will not need to send out a notice of its privacy practices [see II. B. above], because the health insurer will be responsible for this. In addition, since the plan will not have access to PHI, the requirements regarding individual rights [also see II. B. above] will not apply to the plan.

**Plan Sponsor Has Access to PHI for “Plan Administration Functions.”** If the plan sponsor of a fully-insured plan wishes to have access to PHI, beyond summary health information and enrollment/disenrollment information, in order to perform the so-called “plan administration functions” [see I. C. above], then the plan will need to provide individuals with the new individual rights granted under the Rule [see II. B. above], as well as prepare a notice of the plan’s privacy practices [also see II. B. above], though this notice only needs to be provided upon request since the health insurer will still have

the primary obligation to provide the notice. In addition, the plan must comply with the Administrative Requirements of the Rule [see II. C. above].

In addition, before disclosing the PHI to the plan sponsor, the plan must obtain a certification from the plan sponsor stating that the plan documents have been amended and the appropriate firewalls have been put in place to protect the PHI [see I. C. above]. And, the plan sponsor must comply with those same plan document and firewall requirements, and must provide the plan with certification that these requirements have been satisfied.

In essence, then, if a fully-insured plan's plan sponsor wishes to have access to PHI (other than summary health information or enrollment information) for "plan administration functions," then the plan will be treated very similarly to how a self-funded plan would be treated if its plan sponsor wished to have access to such PHI.

***Plan Sponsor Has Access to PHI for Other Purposes.*** No plan, whether fully-insured or self-funded, will be permitted to disclose PHI (other than summary health information or enrollment information) to the plan sponsor for any purposes other than "plan administration functions," without first getting a valid authorization from the individual(s) who is the subject of the PHI.

## **HIPAA Privacy Checklist** for Employers

The following checklist is to help employers that sponsor group health plans understand their obligations as plan sponsors under the HIPAA Privacy Rule.

1. Determine whether your employer-sponsored group health plan(s) meet the Privacy Rule definition of a health plan. Only plans with less than 50 participants that are self-funded and self-administered are exempt from all of the Privacy Rule's requirements.
2. Obtain approval of upper management to develop HIPAA plan.
3. Appoint a privacy officer and contact person or office.
4. Create a HIPAA privacy compliance team, with members from all departments affected by the Privacy Rule.
5. Establish a privacy budget.
6. Establish HIPAA privacy compliance timeline by working back from the April 2003 (or 2004) deadline.
7. Conduct state law preemption analysis, and analyze applicability of other federal laws.
8. Determine which part(s) of company would be a covered entity (health plan) under the Privacy Rule, and which might be a business associate.
9. Determine how protected health information ("PHI") is created, received, maintained, or disclosed by each part of the company.
10. Map the flow of PHI within the company and conduct a gap analysis to understand where actual corporate practices may fall short of HIPAA's requirements.
11. Identify which disclosures would qualify as payment or health care operations (these can continue without an authorization under the Rule), which disclosures would require an authorization, and which disclosures would fit an exception to the authorization requirement.

12. Minimum Necessary: Identify which employees need PHI to carry out health plan functions, and identify the type of PHI needed.
13. Create privacy policies and procedures that comply with the Rule's requirements.
14. Identify all business associates and revise contracts with business associates to comply with requirements of the Privacy Rule.
15. If fully-insured plan with no plan sponsor access to PHI, then plan's health insurer will be solely responsible for meeting the Rule's requirements. Summary health information may be shared with plan sponsor.
16. If fully-insured plan with plan sponsor access to PHI, then plan must comply with Rule:
  - Plan amendments must restrict use and disclosure of PHI.
  - Employees with access to PHI must be designated.
  - Firewalls must be put in place to protect PHI.
  - Notice of privacy practices must be provided by plan upon request, though health insurer will have primary obligation to provide the notice.
  - Plan must abide by the new individual rights regarding PHI.
  - Plan must comply with administrative requirements of the Rule.
17. If self-funded plan, then plan must comply with the Rule:
  - Plan amendments must restrict use and disclosure of PHI.
  - Employees with access to PHI must be designated.
  - Firewalls must be put in place to protect PHI.
  - Notice of privacy practices must be provided by plan.
  - Plan must abide by the new individual rights regarding PHI.
  - Plan must comply with administrative requirements of the Rule.

WPS Health Insurance  
1717 W. Broadway—P.O. Box 8190  
Madison, WI 53708-8190  
[www.wpsic.com](http://www.wpsic.com)

