

Legislative Brief

HIPAA Privacy Regulations *What are Plan Sponsors Required to Do?*



While employers are not directly regulated by the new federal regulations governing the privacy of medical records, the HIPAA Privacy Rules indirectly affect employers that sponsor group health plans. The compliance requirements imposed on the plan sponsor will vary, depending upon whether or not it has access to personally identifiable health information. This issue of the The Rollins Agency, Inc. Legislative Brief is intended to provide plan sponsors with an overview of what is required of them by the HIPAA Privacy Rules.

What are the HIPAA Privacy Rules?

As required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the U.S. Department of Health and Human Services (HHS) released final federal regulations that govern use and disclosure of personally identifiable health information in December 2000 (HIPAA Privacy Rules). Final changes to the regulations were published on August 14, 2002. In most cases, the deadline for compliance with the HIPAA Privacy Rules is April 14, 2003.

What do the HIPAA Privacy Rules accomplish?

The HIPAA Privacy Rules place restrictions on how patients' personally identifiable health information may be used and disclosed by certain organizations. While some states have laws that protect patients' privacy, this federal regulation establishes a minimum level of privacy protections that must be afforded to all patients' medical records. In summary, the regulation:

- Requires that patients be told how their medical records will be used and disclosed,
- Sets limits on how patients' medical records may be used and disclosed, and
- Imposes fines where the requirements contained within the regulations are not followed.

In short, the regulations allow protected health information to be used or disclosed by a covered entity for the purposes of treatment, payment, and health care operations, subject to the minimum necessary standard. An individual's prior written authorization must be received before protected health information may be used in any other manner.

What entities are regulated by the HIPAA Privacy Rules?

The HIPAA Privacy Rules directly regulate the following Covered Entities:

- Health plans,
- Health care clearinghouses, and
- Health care providers that conduct certain transactions electronically.

The HIPAA Privacy Rules indirectly regulate plan sponsors and other third parties by requiring that a Covered Entity require an otherwise non-regulated entity to agree to comply with the restrictions contained within the HIPAA Privacy Rules.

Legislative Brief

HIPAA Privacy Regulations

What are Plan Sponsors Required to Do?

What information is governed by the HIPAA Privacy Rules?

The HIPAA Privacy Rules govern Protected Health Information (PHI), which is defined as:

- Oral, written, or electronic,
- Individually identifiable health information,
- Created or received by a covered entity, and
- Relates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

What are plan sponsors required to do?

The compliance requirements indirectly imposed upon a plan sponsor by the HIPAA Privacy Rules vary based on whether or not the plan sponsor has access to PHI.

Plan Sponsors Offering a Fully-Insured Group Health Plan — No Access to PHI

A plan sponsor that offers a fully-insured group health plan will be minimally impacted by the HIPAA Privacy Rules if its access to health information is limited to the following plan sponsor functions:

- Assisting employees with claim disputes as permitted by the employees' written authorization,
- Receiving Summary Health Information (SHI)¹ for purposes of obtaining premium bids or modifying, amending or terminating the plan, and
- Conducting enrollment and disenrollment activities.

While insurance carriers are required to comply with the majority of requirements contained within the HIPAA Privacy Rules on behalf of the group health plan, plan sponsors within this category may not:

- Require an individual to waive the rights afforded to him or her by the HIPAA Privacy Rules as a condition on the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits;
- Intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual for exercising his or her rights provided by the HIPAA Privacy Rules; or
- Use PHI received in connection with an employee benefit plan when making employment related decisions.²

Plan Sponsors Offering a Fully-Insured or Self-Funded Group Health Plan — With Access to PHI³

Where a plan sponsor has access to PHI in order to perform plan administration functions⁴, the plan sponsor must do all of the following:

- Amend the plan documents to include a description of permitted uses and disclosures of PHI by the plan sponsor;

¹ SHI summarizes claims history, claims experience, or type of claims experienced by individuals from whom a plan sponsor has provided health benefits under a group health plan. The HIPAA Privacy Rules require that certain identifiers such as name, social security number, and date of birth be excluded from SHI.

² The regulations provide an exception to the plan amendment requirement for plan sponsors within this category, however, some benefit experts disagree.

³ Self-funded, self-administered plans with fewer than 50 participants are not required to comply.

⁴ Plan administration functions include claims processing, quality improvement, and fraud detection activities.

Legislative Brief

HIPAA Privacy Regulations

What are Plan Sponsors Required to Do?

- Certify to the group health plan that the plan documents have been amended; and
- Comply with all of the administrative requirements contained within the HIPAA Privacy Rules.

What are the administrative requirements of the HIPAA Privacy Rules?

In general, the HIPAA Privacy Rules require plan sponsors with access to PHI, together with the group health plan, to comply with all of the following administrative requirements contained within the HIPAA Privacy Rules.

- Limit its use and disclosure of PHI to activities related to treatment, payment, and health care operations (unless specific patient authorization permits otherwise), including the creation of internal firewalls.
- Designate a privacy official.
- Train members of its workforce on its policies and procedures with respect to PHI.
- Create policies and procedures designed to ensure compliance with the HIPAA Privacy Rules, including providing plan participants with a right to:
 1. Access and copy records containing their PHI,
 2. Amend records which contain their PHI,
 3. An accounting of disclosures made containing their PHI during the last 6 years⁵, and
 4. Request reasonable restrictions on the use and disclosure of PHI, including that communications containing PHI be sent to an alternate location.
- Provide a notice of privacy practices to all existing plan participants no later than April 2003 and to all new plan participants at enrollment.⁶
- Provide a process for individuals to make complaints concerning its policies and procedures related to use and disclosure of PHI.
- Refrain from taking retaliatory action against an individual that makes a complaint with the plan sponsor, group health plan, or U.S. Department of Health and Human Services alleging a violation of the HIPAA Privacy Rules.
- Require that any business associate that is provided access to PHI agrees to limit its use and disclosure of PHI as set forth in the HIPAA Privacy Rules.
- Establish and apply appropriate sanctions against business associates and members of its workforce that fail to comply with its privacy policies and procedures.
- Report to the group health plan any violations of its privacy policy and procedures.
- Mitigate, to the extent possible, the harmful effect of any violation of its privacy policies.
- Not require individuals to waive their privacy rights as a condition of enrollment in the plan, eligibility for benefits, treatment, or payment.

⁵The accounting is not required to include those made for treatment, payment, or health care operations or pursuant to authorization.

⁶Thereafter, all plan participants must be notified every three years that a Privacy Notice is available and how they may obtain a copy. Plan sponsors of fully-insured plans with access to PHI must provide a HIPAA Notice of Privacy Practices upon request.

Legislative Brief

HIPAA Privacy Regulations

What are Plan Sponsors Required to Do?

-
- Refrain from using PHI received in connection with an employee benefit plan when making employment related decisions.
 - If feasible, return or destroy all PHI when no longer needed.
-

Legislative Brief

HIPAA Privacy Regulations

What are Plan Sponsors Required to Do?

When are plan sponsors required to have their contracts with business associates amended?

The final rules released in December 2000, required that all covered entities must amend their written agreements with business associates that are provided access to PHI no later than April 2003. The final rules as modified in August 2002, allow covered entities an additional year to amend *existing* written contracts to comply with the HIPAA Privacy Rules. However, if a contract is amended, renewed, or modified sooner, the Covered Entity is required to incorporate HIPAA's mandatory provisions at that time. Although the rules allow the covered entity more time to amend its written contracts, the business associate's obligations to allow plan participant access to and amend PHI, maintain an accounting of disclosures made, and allow access by the Department of Health and Human Services as needed to determine compliance is not postponed.

Does a plan sponsor need to obtain a signed authorization in order to assist a plan participant with a claim?

Yes. In order for a plan sponsor or other third party to discuss a pending claim on behalf of the plan participant with an insurance carrier or third party administrator, the HIPAA Privacy Rules require the insurance carrier or third party administrator be provided with the plan participant's written authorization.

What happens if our organization doesn't comply with the HIPAA Privacy Rules?

Failure to comply with the HIPAA Privacy Rules may result in assessment of the following penalties:

- \$100 per violation, up to \$25,000 per year, per standard, for disclosures made in error;
- \$50,000 and/or one year in prison for knowingly obtaining or disclosing PHI;
- \$100,000 and/or up to five years in prison for obtaining information under false pretenses; and
- \$250,000 and up to ten years in prison for obtaining PHI with an intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

How will The Rollins Agency, Inc. assist its clients in complying with the HIPAA Privacy Rules?

Rollins Insurance will assist our clients with their HIPAA Privacy compliance efforts by:

- Providing them with a HIPAA Privacy Legislative Guide located on our Web site designed especially for our clients — MyWave™⁷;
- Continuing to keep our clients informed of the latest legal developments impacting employee benefit plans, including any future guidance from the Department of Health and Human Services related to the HIPAA Privacy Rules;
- Reviewing the services provided by third party administrators in response to the HIPAA Privacy Rules⁸; and

⁷ The HIPAA Privacy Legislative Guide contains answers to commonly asked questions, legislative news, and sample forms.

Legislative Brief

HIPAA Privacy Regulations

What are Plan Sponsors Required to Do?

- Evaluating the need for and assisting with the creation of formal business associate relationships, including Rollins Insurance, third party administrators, and pharmacy benefit management organizations.

How will The Rollins Agency, Inc. comply with the HIPAA Privacy Rules?

Like plan sponsors with access to PHI, insurance brokers are also indirectly regulated by the HIPAA Privacy Rules. In cases where Rollins Insurance needs access to PHI in order to a) assist the plan sponsor with plan administration functions, b) obtain bids from insurance carriers, or c) recommend plan design modifications, we will ask that the plan sponsor enter into a business associate contract with us. In short, the business associate contract requires the insurance broker to limit its use and disclosure of PHI to the permissible uses defined by the plan sponsor.

Rollins Insurance takes the obligations imposed upon it by the HIPAA Privacy Rules seriously. More importantly, we continue to follow policies and procedures designed to ensure that *all* confidential information entrusted to us by our clients is held in strictest confidence. In light of the new HIPAA Privacy Rules, we are in the process of re-evaluating our existing policies and procedures for handling confidential information. Upon completion of our review, all employees with access to PHI will be re-trained on our privacy policies and procedures.

We look forward to continuing to be of service to you. Please contact your Rollins Insurance representative with any questions.

⁸ The services offered by third party administrators in response to the HIPAA Privacy Rules vary. For example, some third party administrators will create and distribute a notice of privacy practices for their clients, while others will not.