COMPLIANCE OVERVIEW

Provided by Clarke & Company Benefits, LLC

HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information. The Privacy Rule applies to covered entities—health plans, health care clearinghouses and most health care providers—and their business associates.

The HIPAA Privacy Rule:

- ✓ Sets limits and conditions on the uses and disclosures of protected health information (PHI) that can be made without an individual's authorization;
- ✓ Gives individuals rights over their PHI, including the right to receive a notice from covered entities regarding their privacy practices; and
- ✓ Requires appropriate safeguards to protect the privacy of PHI.

Although the Privacy Rule applies to both self-funded and fully insured plans, special rules apply to fully insured plans that do not have access to PHI for plan administration purposes.

LINKS AND RESOURCES

The Department of Health and Human Services' (HHS) website includes a brief summary of the HIPAA Privacy Rule and links to the official regulation text.

HIGHLIGHTS

AFFECTED ENTITIES

- The HIPAA Privacy Rule applies to covered entities and business associates.
- A covered entity is a health plan, a health care clearinghouse or a health care provider that conducts certain transactions electronically.
- In general, a business associate is an entity that performs a function, activity or specific service for a covered entity that involves PHI.

IMPACT ON EMPLOYERS

- The extent of a plan sponsor's obligations under the Privacy Rule depends on whether the employer has access to PHI for plan administration.
- Sponsors of fully insured plans that do not have access to PHI have minimal obligations under the Privacy Rule.

CLARKE & COMPANY
BENEFITS LLC

AFFECTED ENTITIES

The HIPAA Privacy Rule directly regulates these covered entities:

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

Business Associates

Business associates also must comply with the Privacy Rule. For additional protection, covered entities and business associates must enter into agreements requiring them to comply with the HIPAA Privacy and Security Rules.

Who is a business associate?

In general, a business associate is an entity that performs a function, activity or specific service for a covered entity that involves creating, receiving, maintaining or transmitting PHI.

If a business associate delegates any of its functions to a subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate, the business associate must enter into a written contract with the subcontractor to ensure that the subcontractor will agree to comply with the HIPAA Privacy and Security Rules.

Plan Sponsors

The Privacy Rule indirectly regulates employers as plan sponsors. If an employer performs administrative functions for its group health plan (for example, reviewing health FSA claims), the employer will usually need to access PHI from the plan. When an employer receives PHI from its group health plan for plan administrative purposes, the employer must agree to comply with certain requirements of the HIPAA Privacy and Security Rules.

PROTECTED INFORMATION

The HIPAA Privacy Rule governs PHI.

What is PHI?

PHI is individually identifiable health information (in oral, written or electronic form) that is created or received for a covered entity and relates to the 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.

PRIVACY PROTECTIONS

While some states have laws that protect patients' privacy, the HIPAA Privacy Rule establishes a minimum level of privacy protections that must be given to all personal health information covered by the Privacy Rule. In summary, the Privacy Rule includes three main protections for PHI:

Use and Disclosure Rules	Covered entities may use and disclose PHI for purposes of treatment, payment and health care operations, subject to a minimum necessary standard. Unless an exception applies, a covered entity must first obtain an individual's written authorization before using or disclosing PHI for any other purpose.
Individual Rights	Providers and health plans must provide individuals (for example, health plan participants) with detailed written information that explains their privacy rights and how their information will be used (a Notice of Privacy Practices). Individuals also have the right to: • Access their own health records and request corrections; • Request restrictions on the uses and disclosures of their PHI, including that communications containing PHI be sent to an alternate location; and • Obtain documentation of certain disclosures made of their health care records.
Administrative Safeguards	Covered entities must develop written privacy procedures and implement appropriate safeguards. For example, covered entities must designate a privacy official, train employees and establish a system for receiving complaints. Covered entities must refrain from intimidating or retaliatory acts, and they cannot require a waiver of HIPAA privacy rights.

REQUIREMENTS FOR HEALTH PLAN SPONSORS

The compliance requirements indirectly imposed upon a plan sponsor by the HIPAA Privacy Rule 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 Rule 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) for purposes of obtaining premium bids or modifying, amending or terminating the plan; and

- ✓ Conducting enrollment and disenrollment activities.

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 Rule requires that certain identifiers such as name, Social Security number and date of birth be excluded from SHI.

While insurance carriers are required to comply with the majority of requirements contained within the HIPAA Privacy Rule 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 Rule 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 Rule; or
- Use PHI received in connection with an employee benefit plan when making employment related decisions.

Plan Sponsors Offering a Fully Insured or Self-funded Group Health Plan—With Access to PHI

Sponsors of fully insured group health plans that have access to PHI for plan administration functions will be required to comply with the Privacy Rule's requirements. These requirements also apply to sponsors of self-funded group health plans.

Where a plan sponsor has access to PHI in order to perform plan administration functions, 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;

- ✓ 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 Rule.

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

WHAT ARE THE ADMINISTRATIVE REQUIREMENTS OF THE HIPAA PRIVACY RULE?

In general, the HIPAA Privacy Rule requires 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 Rule.

- 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 Rule, including providing plan participants with a right to:
    - Access and copy records containing their PHI;
    - Amend records which contain their PHI;
    - An accounting of disclosures made containing their PHI during the last six years (an accounting is not required for disclosures made for treatment, payment or health care operations or pursuant to an authorization); and
    - 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 (Privacy Notice) to all new plan participants at enrollment;
- 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 HHS alleging a violation of the HIPAA Privacy Rule;
- 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 Rule;
- 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 about 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;
- Refrain from using PHI received in connection with an employee benefit plan when making employment related decisions; and
- If feasible, return or destroy all PHI when no longer needed.

In addition, all plan participants must also 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 Privacy Notice upon request.

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 Rule requires that the insurance carrier or third-party administrator be provided with the plan participant's written authorization.

ENFORCEMENT

HHS' Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy Rule. OCR has increased its enforcement of the HIPAA Privacy and Security Rules in recent years, with some costly outcomes for covered entities. OCR enforces HIPAA's Privacy and Security Rules by investigating complaints that are filed with it, conducting compliance reviews of covered entities and business associates and performing education and outreach to promote compliance with the Rules' requirements. OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA.

An OCR investigation may trigger **civil penalties** for a covered entity or business associate. The penalty amounts vary based on the type of violation. Also, penalties may not apply if the violation is corrected within 30 days of when the person know, or should have known, of the violation.

Type of violation	Each violation	All violations of identical provision in a calendar year
Did not know about violation	$100 – $50,000	$1.5 million
Violation due to reasonable cause	$1,000 – $50,000	
Corrected violation caused by willful neglect	$10,000 – $50,000	
Violation caused by willful neglect, not corrected	$50,000 – no maximum	

The possible **criminal penalties** that may be assessed for violations of the HIPAA Privacy and Security Rules are $50,000 and one year in prison for knowing violations, $100,000 and five years in prison for violations committed under false pretenses, and $250,000 and 10 years in prison for offenses committed for commercial or personal gain.