HIPAA Privacy Rules

The provisions of HIPAA are the first national standards for protecting health information. They are a result of increased public concern over the use and disclosure of health and other personal information as technology makes access to all types of records much easier. The rules are intended to protect and enhance the rights of consumers regarding their health information, control the inappropriate use of medical records and improve the quality of health care in the United States by restoring trust in the health care system.

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.

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 also must comply with the Privacy Rule.

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.

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).
- 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.

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.
- 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.

The following benefits are not subject to the HIPAA Privacy Rule:

- Accident-only
- Disability Insurance
- Liability Insurance
- Life Insurance
- Worker's Compensation