HIPAA REQUIREMENTS UNDER THE HITECH ACT

The American Recovery and Reinvestment Act, signed by President Barack Obama, imposes updated HIPAA privacy and security requirements. The HIPAA requirements fall under the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Below are the new requirements of the HIPAA privacy and security rules (45 CFR, Parts 160-164). These requirements take effect February 17, 2010.

Right to Restrict Disclosures

Previously, HIPAA allowed an individual the right to request that a covered entity not disclose their PHI, even for purposes of routine treatment, payment or health care operations. However, the covered entity was not required to agree to the restriction.

HIPAA now requires the covered entity to agree to the restriction where services for treatment have been paid out-of-pocket in full. This means if an individual has paid out-of-pocket for a certain treatment, the provider or another plan would not be permitted to disclose this information to another health plan if the individual does not want that information to be disclosed.

Accounting for Disclosures

Previously, HIPAA allowed an individual to request an accounting of disclosures of their PHI for the previous 6 years, with the exception of routine disclosures for treatment, payment and health care operations (TPO).

HIPAA now requires a covered entity that maintains PHI electronically to include routine disclosures for treatment, payment, and health care operations (TPO) in its accounting list. The TPO accounting will be limited to 3 years. Other disclosures will remain at 6 years.

Access to Electronic PHI

Where the covered entity holds an electronic health record (EHR), an individual must be able to request their information in electronic form. The covered entity may only charge labor costs. In addition, an individual may direct the covered entity to transmit a copy of their electronic health records directly to an entity or person designated by the individual.

Extension of HIPAA Rules to Business Associates

HIPAA privacy and security requirements will now apply to business associates in the same manner as they apply to covered entities. A business associate is subject to the same penalties as the covered entity. Business associate agreements must be revised to include any new privacy or security requirements. Any entity that provides data transmission services to a covered entity is considered a business associate.

Duty to Notify in Case of Breach

If protected health information (PHI) is breached, the covered entity is required to notify each individual. The notification must be made within 60 days of discovery or the date the breach reasonably should have been discovered, and must describe the circumstances of the breach, including:

- The date of the breach
- The date of discovery
- The type of PHI involved
- Steps individuals should take to protect themselves
- Steps the covered entity is taking to mitigate harm and protect against future breaches

If the breach is by a business associate, the business associate must notify the covered entity, including the identity of each individual involved.

The notice must be made by first class mail or electronic mail (if specified as a preference by the individual). If more than 500 individuals in a state or jurisdiction are involved, the covered entity must provide notice to prominent media outlets serving the state or jurisdiction. The covered entity must also notify the secretary of health and human services immediately of breaches involving 500 or more individuals and on an annual basis for other breaches. The secretary will list breaches involving more than 500 individuals on its website.

Prohibition on Sale of Electronic Health Records or Protected Health Information

A covered entity or business associate shall not directly or indirectly receive payment in exchange for any PHI of an individual unless the covered entity obtained a valid authorization that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that individual except for the purpose of:

- Public health activities
- Research (the price charged must reflect the costs of preparation and transmittal of the data for such purpose)
- Treatment of the individual
- Health care operation
- Remuneration that is provided by a covered entity to a business associate for activities involving the exchange of protected health information that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement
- Providing an individual with a copy of the individual's protected health information

Enforcement & Penalties

The new law has improved enforcement of the HIPAA requirements and has increased the penalty amounts for HIPAA violations:

CIVIL PENALTIES

These civil penalties may not apply if the violation is corrected within 30 days of the date the person knew of the violation or should have known of the violation.

	Minimum Penalty	Maximum Penalty
Due Diligence: The person does not know of a violation, unintentional	$100 per violation A cap of $25,000 per calendar year for violations of an identical requirement	$50,000 per violation A cap of $1.5 million per calendar year for violations of an identical requirement
Reasonable Cause	$1000 per violation A cap of $100,000 per calendar year for violations of an identical requirement	$50,000 per violation A cap of $1.5 million per calendar year for violations of an identical requirement
Willful Neglect	$10,000 per violation A cap of $250,000 per calendar year for violations of an identical requirement	$50,000 per violation A cap of $1.5 million per calendar year for violations of an identical requirement

CRIMINAL PENALTIES

Criminal penalties remain the same, but the new law states that criminal action may be brought against <u>any individual</u> who wrongfully discloses PHI, not just the covered entity. This means if you wrongfully disclose PHI knowingly, you will be fined and possibly be imprisoned.

	Fine	Imprisonment
Knowingly and in violation	$50,000	1 year
Under false pretenses	$100,000	5 years
With intent to sell, transfer, or use for personal gain/commercial advantage, or malicious harm	$250,000	10 years

Civil and criminal penalty provisions apply to business associates in the same manner as a covered entity.

Also, if the State's Attorney General has reason to believe that an interest of one or more of the residents of the State has been or is threatened or adversely affected by any person(s) in violation, the State's Attorney General has the authority to bring civil actions against a covered entity to enjoin violations and obtain damages on behalf of the residents of that state, up to $100 per violation with a cap of $25,000 for violations of an identical requirement during a calendar year.