

American Recovery and Reinvestment Act (ARRA) Privacy Provisions

The Health Information Technology for Economic and Clinical Health (HITECH) Act

- Privacy provisions are at Subtitle D
of Title XIII

Health Insurance Portability and Accountability Act (HIPAA) Security Rule

- HITECH Act applies the HIPAA Security Rule's provisions on administrative, physical, and technical safeguards directly to business associates

HIPAA Security Rule

- HITECH Act extends HIPAA's civil and criminal penalties to business associates for violations of the Security Rule.

Breach Notification

- HITECH Act imposes notification requirements for covered entities and business associates when “unsecured Protected Health Information (PHI)” is compromised.
- Similar requirement also imposed on vendors of Personal Health Records (PHR).

Education on Health Information Privacy

- A privacy officer for each regional office of the Department of Health and Human Services (HHS) will offer guidance and education to covered entities, business associates, and individuals on their rights and obligations regarding PHI.

HIPAA Privacy Rule

- HIPAA privacy provisions and penalties applied to business associates
- Extends HIPAA's civil and criminal penalties to business associates for violations of these provisions

Individual Rights Regarding PHI

- HITECH Act contains several provisions giving individuals more direct control and oversight over their PHI.

Restrictions on Disclosures

- Requires a covered entity to comply with an individual's request that the covered entity restrict the disclosure of PHI if (except as otherwise required by law) the disclosure: (1) is to a health plan for payment or healthcare operations and (2) pertains to items or services paid in full out-of-pocket.

Minimum Necessary

- HITECH Act requires covered entities and business associates to restrict the uses, disclosures, or requests of PHI to a *limited data set* to the extent practicable.
- If not practicable, the *minimum necessary* may be used or disclosed.

Requesting an Accounting

- HITECH Act expands the rights to an accounting of PHI disclosure to include disclosures made for treatment, payment, or healthcare ops
- Covers previous three years for disclosures for these purposes

Sales of PHI

- Prohibits a covered entity or business associate from directly or indirectly receiving any remuneration for an individual's PHI unless the individual provides a valid authorization.

Access to Electronic Health Records (EHRs)

- HITECH Act requires covered entities that maintain EHRs to provide individuals an electronic copy of their health records

Restrictions on Commercial Uses of PHI

- Marketing
- Fundraising

BA Contracts Required for Certain Entities

- Applies to “organizations that provide data transmission of PHI and that need routine access to PHI”
- Examples: Health Information Exchanges, Regional Health Information Organizations, E-prescribing gateways, and vendors that contract with a covered entity to provide PHRs to patients

Criminal Penalties

- HITECH Act clarifies that any person (including employees of covered entities) may be subject to criminal penalties for disclosing PHI.

Improved Enforcement

- HITECH Act increases the civil and criminal penalties.
- HITECH Act gives State Attorney Generals the authority to bring enforcement suits for HIPAA violations.