The Health Information Privacy and Security Act of 2007
Section by Section Summary

The Health Information Privacy and Security Act creates new privacy safeguards to better protect Americans' health information in the Information Age, by ensuring the right of all Americans to privacy, confidentiality and security with respect to their health information and imposing criminal and civil sanctions for the unauthorized disclosure of sensitive health information.

TITLE I – INDIVIDUALS' RIGHTS

Section 101. Right to Privacy and Security.
- Ensures an individual's control over, and right to privacy and security with respect to, the use and disclosure of their protected health information.

Section 102. Inspection and Copying of Protected Health Information.
- Allows an individual to inspect and copy any protected health information concerning them held by an entity.
- Allows an entity to charge a fee to cover the costs of copying health services, unless the fee prevents an individual from accessing his or her own health records.

Section 103. Modifications to Protected Health Information.
- Guarantees an individual's right to supplement, amend, correct, or destroy any of that individual's protected health information that is maintained or stored by an entity.
- Requires an entity to notify an individual when data corruption or loss of health information is discovered.
- Provides a procedure for an entity to refuse a modification request and properly inform the requester.

Section 104. Notice of Privacy Practices.
- Requires entities maintaining, accessing, using, or storing an individual's protected health information to provide the individual with a notice of privacy rights and practices, including:
  - The right of the individual to the privacy, security, and confidentially of all of his protected health information stored in electronic systems;
  - Procedures for authorizing disclosures of information to third parties, and for revoking such authorizations;
  - The right of the individual to inspect, copy, or modify the information and to obtain records of disclosures and authorizations;
  - The right to employment, continued maintenance of information, or receipt of services not conditioned on an individual's decision to authorize or not;
  - The right to opt out of any entity's electronic system;
  - A description of how the individual's information will be used, and by whom;
  - The right to be notified in the case of a security breach; and
  - The right to segregate information and limit access to this information to only a subset of authorized recipients.

Section 105. Health Literacy Demonstration Grant.

- Creates a demonstration grant program to help people with low health literacy and low English language proficiency access and exercise their privacy rights in a culturally and linguistically appropriate way.

Section 111. Establishment of Safeguards.

- Requires an entity to establish technological, administrative, organizational, technical, and physical safeguards to secure protected health information that they create, access, use, or maintain.
- Requires that safeguards be reviewed and updated as technology changes.

Section 112. Transparency.

- Requires an entity to publish a list of all data brokers that provide the entity with services involving protected health information.
- Requires entities contracting with service providers that are not subject to this bill to ensure that such providers maintain appropriate privacy and security measures.

Section 113. Risk Management.

- Mandates that an entity undertake annual risk assessment, management, and control exercises to prevent, limit, and detect security threats or breaches.

Section 114. Accounting for Disclosures and Uses.

- Requires entities with access to protected health information to create an electronic record of all disclosures and uses, to the extent practicable, including which information was disclosed, to whom, and for what purposes.
- Guarantees individuals who are the subjects of protected health information access to the record of disclosures and uses of that health information.

## TITLE II – RESTRICTIONS ON USE AND DISCLOSURE

Section 201. General Rules Regarding Use and Disclosure.

- Prohibits individuals or entities from disclosing, accessing, or using protected health information without authorization.
- Excepts de-identified health information from the rules in this section.
- Requires that no person's protected health information be disclosed until that person has the option to opt out of any health information networks in which the receiving agent participates.
- Requires that an authorized disclosure of information be the minimum amount of necessary data and be used only for the purposes for which it was authorized.
- Bars unauthorized recipients of protected health information from using, accessing, or disclosing such information for any purposes. Unauthorized disclosures or use are subject to penalties established under this Act.

Section 202. Authorizations for Disclosure of Protected Health Information for Treatment and Payment.

- Requires employers, health plans, health insurers, health care providers, and others seeking to disclose protected health information to obtain a signed, written authorization from an individual in connection with any treatment, payment, or other purpose.
- Directs the Secretary to provide model authorization forms to assist health care providers and other persons involved in the provision of health care.
- Provides that an individual may revoke or amend an authorization for protected health information concerning him at any time.
- Mandates that the authorization form include:
  - Which information will be authorized for disclosure, who may disclose it, to whom it will be disclosed, and for what purposes;
  - A description of any information the individual would like segregated, generally or from a particular group;
  - The extent to which information will be disclosed to external systems, databases, or networks or to overseas entities; and
  - How authorization can be revoked.

Section 203. Authorizations for Disclosure of Protected Health Information Other than for Treatment and Payment.
- Requires employers, health plans, health insurers, health care providers, and others seeking to disclose protected health information for reasons other than treatment or payment to obtain a signed, written authorization from an individual that is separate from the authorization described in § 202 of this Act, and must meet only a subset of the requirements under § 202.
- Directs the Secretary to provide model authorization forms to assist health care providers and other persons involved in the provision of health care.
- Authorizes the release of protected health information to coroners and medical examiners for the purpose of inquiry into an individual's death.

Section 204. Notification in the Case of Breach.
- An individual must be provided with notification in the case of an actual or attempted security breach if there is at least a "reasonable belief" that protected health information concerning him was accessed or acquired during the breach.
- Notification must be provided within 15 business days of discovery of the breach and must include the categories of protected health information breached.
- Notification may be delayed by law enforcement if it would impact an ongoing criminal investigation or national security.

Section 211. Emergency Circumstances.
- Allows for emergency disclosure of protected health information, without an individual's authorization, in the case of an emergency threatening harm to an individual or an individual's threat of harm to another person.

Section 212. Public Health.
- Allows for unauthorized disclosure of protected health information to a public health authority for the purposes of protecting public health.

Section 213. Protection and Advocacy Agencies.

- Allows for unauthorized disclosure of protected health information to report neglect or abuse of an individual to an authority.

Section 214. Oversight.
- Allows for unauthorized disclosure of protected health information for the purposes of oversight and judicial investigation of matters relating to health, provided that disclosure is limited to information required for judicial, administrative, or court proceedings.

Section 215. Disclosure for Law Enforcement, National Security, and Intelligence Purposes.
- Allows for unauthorized disclosure of protected health information to law enforcement officials, provided that a court order or warrant is obtained. Notice must still be provided to individual.
- Allows for unauthorized disclosure of protected health information to federal officials authorized to carry out lawful intelligence or other national security investigations and activities. Notice to the individual may not be necessary.

Section 216. Next of Kin and Directory Information.
- Allows for unauthorized disclosure of protected health information about health services to next of kin, provided that an individual has been notified of their right to object to such disclosure.
- Authorizes disclosure of certain protected health information by an individual's next of kin, or another entity that the individual has identified, for the purposes of maintaining a health care facilities directory.

Section 217. Health Research
- Requires the Secretary to develop recommendations on the extent to which health researchers must receive authorization before accessing or using protected health information.
- Identifies which health research and health researchers might qualify for receipt of protected health information without prior authorization for disclosure.
- Identifies the obligations of recipients of protected health information for the purposes of health research (among them, the immediate de-identification of all health data).

Section 218. Judicial and Administrative Purposes
- Allows for unauthorized disclosure of protected health information for use in judicial proceedings, provided that a court order is obtained.

Section 219. Individual Representatives.
- Outlines rights of minors to access their protected health information.
- Authorizes disclosure of an individual's protected health information to entities designated to have health care power of attorney or otherwise designated as representatives of an individual.

TITLE III - OFFICE OF HEALTH INFORMATION PRIVACY OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

Section 301. Designation.
- Establishes an office to investigate complaints and alleged violations, conduct audits and establish guidelines for compliance under this Act.
- Establishes and implements Federal standards and product certifications for health information technology products that handle protected health information.

Section 311. Wrongful Disclosure of Protected Health Information.
- Establishes criminal penalties for wrongful (unauthorized) disclosure or use of protected health information.

Section 312. Debarment for Crimes.
- Directs the Attorney General to produce regulations and procedures that
  - Debar Health Industry entities from receiving Federal funds if they are found guilty of wrongful disclosure of protected health information (18 USC § 2801).
  - Assess civil penalties against Health Industry entities for illegal disclosure of health information or attempts to conceal such a disclosure.

Section 321. Civil Penalty.
- Authorizes the Secretary (in consultation with the Attorney General) to seek a range of penalties against entities for violating various provisions of this Act.
  - A violation of an individual's rights in their health information (Title I of this Act) may result in a civil penalty of not more than $500 for each violation, not exceeding $5000 in the aggregate.
  - An improper use or disclosure of protected health information (Title II of this Act) may result in a civil penalty of not more than $10,000 for each violation, not exceeding $50,000 in the aggregate.
  - If violations of either type have occurred so frequently as to constitute a general business practice, a civil penalty of not more than $100,000 may be sought.

Section 322. Procedures for Imposition of Penalties.
- Provides that the Attorney General may bring suit to impose the civil penalties outlined in § 321 within a 6 year statute of limitations.

Section 323. Civil Action by Individuals.
- Allows an individual whose rights under the Act have been knowingly or negligently violated to bring a civil action against the violating entity within a 3 year statute of limitations, seeking
  - Preliminary and equitable relief;
  - The greater of compensatory damages or liquidated damages of $5,000;
  - Punitive damages (if warranted); and
  - Attorneys' fees.

Section 324. Enforcement by State Attorneys General.
- Authorizes a State Attorney General to bring a civil action against an entity for such violations of this Act as threaten or adversely affect an interest of the residents of that State. The State Attorney General may
  - enjoin the violations;
  - to force compliance with the Act; or

o assess a daily civil penalty of not more than $1,000 for each infringement, up to a maximum of $50,000 per day.

- The Federal Attorney General, upon receiving notice of an action by a State Attorney General, may move to stay or to intervene in the action.

Section 325. Protection for Whistleblower.

- Protects an employee from retaliation, demotion, suspension, discharge, or other discrimination by an employer as a result of exercising a right under this Act or reporting a suspected or actual violation of this Act to a State or Federal official.
- Provides protection to an individual who provides information to a State or Federal official relating to any actual or suspected violation of this Act.

TITLE IV - RELATIONSHIP TO OTHER LAWS

Section 401. Relationship to Other Laws.

- Does not supplant HIPAA but requires the Secretary to revise HIPAA as necessary to make it consistent with this Act.

Section 402. Efffective Date.

- Establishes that the Act takes effect no later than 30 months after enactment and requires that the Secretary promulgate regulations implementing the Act within 12 months of enactment.