



February 19, 2009

To: State Unit on Aging Directors
From: Martha Roherty, Cathy Rudd
RE: Economic Stimulus Package – HIPAA Privacy and Security Provisions

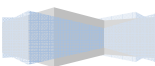
This document summarizes provisions contained in the American Recovery and Reinvestment Act (ARRA) affecting the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These provisions are found in Title XIII – Health Information Technology (beginning at Section 13001 of the ARRA). This new law will be cited as the “Health Information Technology for Economic and Clinical Health Act” or the “HITECH Act”. Information about the effective dates of the various provisions is in bold. References to “the Secretary” are to the Secretary of the Department of Health and Human Services. Please feel free to contact NASUA with any questions.

Section 13400 Definitions

Adopts existing regulatory definitions of “business associate,” “covered entity,” “disclose,” “health care operation,” “health care provider,” “health plan,” “payment” “protected health information,” “security,” “treatment,” and “use”

Defines “breach,” “electronic health record,” (EHR) and “personal health record” (PHR). A personal health record is a type of electronic health record (EHR); an EHR is created, gathered, managed, and consulted by authorized health care clinicians and staff; a PHR is managed, shared, and controlled by or primarily for the individual.

Part 1 Improved Privacy and Security Provisions



Section 13401 Application of Security Provisions and Penalties to Business Associates of Covered Entities; Annual Guidance on Security Provisions

Makes certain security provisions (administrative, physical, technical safeguards as well as policies, procedures and documentation requirements) applicable to business associates in the same way as they apply to a covered entity. Also makes business associates subject to civil and criminal penalties for security breaches in the same manner as covered entities. Additional requirements added by this title that are applicable to covered entities are also applicable to business associates and must be incorporated into the business associate agreement between the business associate and the covered entity.

Section 13402 Notification in Cases of Breach

Covered entities must notify each individual whose unsecured protected health information (PHI) has been accessed, acquired, or disclosed, of the breach. Business associates are required to notify covered entities of breaches. Notifications are to be made without unreasonable delay and no later than 60 days after discovery. Individual notice is required (written notification by first-class mail, or email if email has been specified as a preference for contact). In cases of insufficient contact information, a substitute notice must be provided (for 10 or more individuals, web site posting, print or broadcast media for a period of time determined by the Secretary). If imminent misuse of PHI is suspected, telephone notice may be provided.

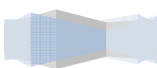
If more than 500 people are affected by the disclosure, notice shall be provided to prominent media outlets.

Notice to Secretary of HHS – If 500 or more people are affected, notice must be provided immediately. If less than 500 people, the covered entity may maintain a log and submit it annually to the Secretary. The Secretary will post information about breaches involving 500 or more people on the HHS website. Statute provides for the content of the notice to individuals and on the HHS website.

Unsecured protected health information is defined as PHI that is not secured through the use of technology or methodology specified by the secretary. The Secretary is to issue guidance within 60 days of enactment, with input from stakeholders, identifying technologies and methodologies that secure PH). Secretary must report breaches to congress annually.

The Secretary is to promulgate interim final regulations no later than 180 days after enactment. These provisions apply to breaches discovered on and after 30 days after publication of the interim final regulations.

The state pre-emption requirement contained in the existing HIPAA law also applies to all of these new provisions. This means that HIPAA is the floor. Thus, if a state has existing laws concerning notification in the case of breaches (many do) those will likely still apply.



Section 13404 Application of Privacy Provisions and Penalties to Business Associates of Covered Entities

Makes business associates subject to the privacy rule concerning uses and disclosures of PHI (45 CFR 164.504(e)) and civil and criminal penalties.

Section 13405 Restrictions on Certain Disclosures and Sales of Health Information; Accounting of Certain Protected Health Information Disclosures; Access to Information in Electronic Format

Requires a covered entity to restrict disclosure requested by an individual if the disclosure is to a health plan for purposes of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which the provider involved has been paid out of pocket in full. This is a change from current law, which permits a covered entity to decline the request for restriction.

Covered entities are required to limit the use, disclosure, or request of PHI, to the extent practicable, to a limited data set, or the minimum necessary to achieve the intended purpose of the disclosure. No later than 18 months following enactment, the Secretary shall issue guidance on what constitutes “minimum necessary.”

For covered entities using an electronic health record, the provisions concerning accounting for disclosures has been revised. Disclosures to carry out treatment, payment and healthcare operations (“TPO”) must be included in the accounting and the individual’s right to receive an accounting of disclosures for TPO applies only for the three years prior to the date of the request. **This provision applies to disclosures made by the covered entity on and after January 1, 2014 (for current users of EHRs) and January 1, 2011 or the date that the covered entity acquires EHRs. The Secretary may set a later date.**

The Secretary shall promulgate regulations on what information shall be collected about each disclosure concerning TPO no later than 6 months after the date on which the secretary adopts standards on technologies used for accounting for such disclosures as recommended by the HIT Policy Committee established under the ARRA.

Prohibits covered entities and business associates from selling PHI without authorization from the individual. There are exceptions including: public health activities, research (as long as the price reflects the costs of preparation and transmittal of data for such purpose), charge to the individual for a copy of the individual’s information pursuant to existing regulation, any other purpose determined appropriate by the Secretary in regulations. The Secretary is required to promulgate regulations no later than 18 months after enactment and they shall apply to exchanges occurring on and after 6 months after the date of promulgation of final regulations.

An individual has a right to obtain an electronic copy of PHI if the covered entity uses or maintains an EHR. The individual may choose to have the copy transmitted to someone else. The charge for an electronic copy cannot be greater than the covered entity’s labor costs.

Section 13406 Conditions on Certain Contacts as Part of Health Care Operations

Imposes some stricter provisions on marketing communications by clarifying that a communication by a covered entity or business associate about a product or service that encourages the recipient to purchase or use the product or service may not be considered health care operations, unless the communication relates to a health care-related product or service. Written communications concerning fundraising must provide the individual with an opportunity to opt out of future communications.

Applies to written communications issued one year after enactment.

Section 13407 Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities

Vendors of personal health records are entities other than a covered entity that offer or maintain a personal health record. A breach of security of an unsecured PHR discovered by vendors of PHR and other entities not covered by HIPAA requires notification of the individual and the Federal Trade Commission. Failure to provide the required notification will be treated as an unfair and deceptive act or practice in violation of existing law. The FTC is responsible for notifying the Secretary of breaches for which it receives notice. **The FTC is responsible for promulgating interim final regulations within 180 days of enactment to implement this provision. These provisions shall apply to breaches of security discovered on or after the date that is 30 days after publication of the interim final rule.**

Section 13408 Business Associate Contracts Required for Certain Entities

Requires business associate contracts for health information exchanges, regional health information organizations and PHR vendors.

Section 13409 Clarification of Applications of Wrongful Disclosures Criminal Penalties

Under current law, only covered entities can be criminally liable for unauthorized disclosures. This provision clarifies that criminal penalties for wrongful disclosure of PHI apply to individuals who without authorization obtain or disclose such information maintained by a covered entity, whether they are employees or not.

Section 13410 Improved Enforcement

Amends HIPAA to permit OCR to pursue investigation and possible civil penalties for an alleged criminal violation if the Department of Justice has not prosecuted the individual. Requires formal investigation and imposition of penalties for violations due to willful neglect. The Secretary is required to promulgate regulations within 18 months to implement these new requirements.

Increases and sets tiers for penalties for violations of HIPAA.

Permits State Attorneys General to bring civil actions for injunctive relief and damages in federal court against individuals who violate security and privacy standards.

Section 13411 Audits

Requires Secretary to audit covered entities and business associates to ensure compliance with security and privacy requirements.

Part 2 – Relationship to Other Laws, Regulatory References; Effective Date Reports

Section 13421 Relationship to Other Laws

HIPAA pre-emption applies to new provisions.

The privacy and security regulations already promulgated by the Secretary remain in effect to the extent they are consistent with these amendments. The Secretary must amend any rules necessary to make them conform with these amendments.

Section 13423 Effective Date

Everything in Part 1 is effective 12 months from the date of enactment, unless otherwise specified.

Section 13424 Studies, Reports, Guidance

Secretary must submit annual report to certain congressional committees concerning complaints of alleged violations (statute specifies the contents of the report).

The Secretary, in consultation with the FTC, must conduct a study and submit a report to certain congressional committees within one year of enactment on privacy and security requirements for non-covered entities or business associates (statute specifies the content of the report).

Not later than 12 months after enactment, the Secretary must issue guidance, with input from stakeholders, on how best to implement requirements for de-identification of PHI.

Not later than one year after enactment, GAO must submit a report to certain congressional committees on best practices related to disclosure of PHI for the purpose of treatment.

Not later than 5 years after enactment, GAO must submit a report to Congress and HHS on the impact of the provisions in the Act on health insurance premiums, overall health care costs, adoption of EHR by providers and reduction in medical errors and other quality improvements.

The Secretary shall study the definition of “psychotherapy notes” in regulation with regard to including test data that are part of a mental health evaluation and may, based on the study, issue regulations to revise the definition.

