# AMERICAN RECOVERY & REINVESTMENT ACT OF 2009
# TITLE XIII-HEALTH INFORMATION TECHNOLOGY
# ANALYSIS OF PRIVACY AND SECURITY REQUIREMENTS (SUBPART D)

## October 27, 2009

Introduction:

The purpose of this addendum to the HIPAA Training Manual is to provide a detailed analysis of the new requirements relating to health care privacy and security enacted February 17, 2009 as part of the American Recovery and Reinvestment Act of 2009 (ARRA). Provisions are included in Division A, Title XIII, Subpart D. Title XIII is also known as the HITECH Act. Title XIII includes new requirements for health information technology (HIT) standards development and adoption, HIT funding and the establishment of an oversight body to provide direction as HIT use expands. Significant changes to existing privacy and security requirements that impact health care (and in some cases non-health care) entities were included in Subpart D.

All provisions of the Act do not take effect immediately and a number of the provisions require the promulgation of rule by the US Department of Health and Human Services (HHS) and, in one instance the Federal Trade Commission (FTC). Also, especially as it relates HIT standards adoption, the requirement to adhere to new standards is delayed. On the other hand, many of the expanded security and privacy provisions take effect much sooner and some impact the healthcare industry outside the formal rule making process. Congress included provisions along with listed requirements that allow HHS to promulgate interim final rules that do not require public comment but will need to go through the public comment process before being finalized.

It is important for all health care entities and vendors with access to individually identifiable health information pay attention to these new provisions. Given language regarding increased enforcement, it would be advisable to review the new requirements and implement those requirements as soon as practicable rather than reacting after the fact as has been the case with a number of healthcare entities.

Also, earlier provisions in Title XIII include a requirement to implement appropriate privacy and security controls to be eligible to take advantage of stimulus dollars associated with Title XIII. This is covered in certification requirements, standards development, electronic health record

funding, etc. These are not specific on-going legal requirements but are tied to the ability to take advantage of funds made available through ARRA.

The following analysis is structured to follow the language of the Act. Sections of Title XIII, Subpart D are identified as points of reference to assist the reader. When and how new requirements will be effective and enforced is also included where such language is available.

## Title XIII Subpart D Provision Summary

1. Business Associates:
    a. Must comply with all provisions of the HIPAA security rule (45 CFR 164.302 through 164.318)
    b. Must comply with certain provisions of the HIPAA privacy rule (45 CFR 164.502, 164.504)
        i. Use and disclosure of protected health information (PHI), general requirements
        ii. Use and disclosure of PHI, organizational requirements
    c. Subject to civil and criminal penalties for violation of the HIPAA security rule and certain provisions of the HIPAA privacy rule
    d. Creation of new categories of business associates including:
        i. Health Information Exchange Organizations
        ii. Regional Health Information Organizations
        iii. E-prescribing Gateways
        iv. Vendors who contract with covered entities to provide a PHR to the covered entities' patients or health plan members

2. Covered Entities:
    a. Covered entities are required to amend existing business associate contracts/agreements to reflect the change requiring business associates to comply with the HIPAA security rule and certain provisions of the HIPAA privacy rule
    b. Covered entities are required to enter into business associate relationships with the new categories of business associates

3. New Privacy Rule Requirements:
    a. Covered entities are required to honor individual restriction requests if the restriction requests cover PHI disclosed to health plans for healthcare operations or it applies to devices or services that are directly paid for by the individual (versus payments made by health plans).

 

b. Covered entity disclosures must be limited to a limited data set or, if not feasible, disclosures meet the minimum necessary requirement (exception still exists for disclosure for treatment). This provision sunsets following HHS publication of the definition and requirements related to minimum necessary.
c. Covered entity accounting of disclosures from an electronic health record (EHR) must include disclosures made for treatment, payment and healthcare operations in addition to other disclosure accounting already required by the HIPAA privacy rule. The EHR accounting covers the three year period preceding the request for an accounting of disclosures by the individual.
d. Covered entities and business associates are prohibited from receiving payment for the release of PHI with certain exceptions.
e. If a covered entity uses, discloses or stores individual PHI electronically, the covered entity must make PHI available electronically upon request to the individual. The individual may be charged for providing an electronic copy of the PHI but the cost cannot exceed the cost to the covered entity to prepare and send the electronic copy to the individual.
f. Marketing is not considered healthcare operations unless it falls under the limited exceptions included in the HIPAA privacy rule that allow for certain types of marketing. Also, when marketing can occur is more clearly spelled out in the language of Title XIII, Subpart D.
g. Any written fund raising communication must be clear and directly identify the communication as related to fund raising, inform the recipient that he or she has the right to request no further fund raising communication. When an individual elects not to receive any further fund raising communication it shall be treated in the same matter as the revocation of authorization (minor change from current HIPAA privacy rule requirements).

4. New Security Related Education Responsibilities – HHS:
   a. The Center for Medicare and Medicaid Services (CMS) is required to work with stakeholders and issue guidance on the most effective and appropriate technical safeguards to implement or follow to meet the requirements of the HIPAA security rule.
   b. HHS is required to publish guidance that defines technologies and methodologies that can be used to make PHI unusable, unreadable, or indecipherable to unauthorized individuals (relates to breach notification provisions and how to avoid inappropriate disclosure of "unsecured PHI").

5. New Privacy Related Education Responsibilities – HHS:

a. HHS (likely the Office for Civil Rights (OCR)) is required to designate an individual in each regional office who is responsible for providing guidance/education to covered entities, business associates, and individuals regarding the HIPAA privacy and security rules.
b. OCR is required to develop and maintain a national education initiative intended to increase transparency regarding the uses of PHI which includes individual education.

6. Breach Notification Requirements:
   a. National identity theft protection requirements (specifically breach notification) is established by this Act and applies to covered entities, business associates, personal health record (PHR) vendors and PHR vendor third party contractors.
   b. Covered entities are required to notify individuals of any breach of PHI (see detailed analysis section for specific notification requirements) within 60 days, to notify HHS if any breach includes 500 individuals or more and maintain a breach log for breaches involving less than 500 individuals.
   c. Business associates are required to notify covered entities of any breaches. This includes providing the covered entity with specific information about the breach and the individuals involved. It is the responsibility of the covered entity to notify affected individuals (see b. above).
   d. PHR vendors and third party service providers supporting PHR vendors are required to notify individuals of any breach of individually identifiable health information and report breaches to the Federal Trade Commission (FTC). The FTC is responsible for publishing rules defining notification requirements and is responsible for notifying HHS of any reported breaches.
   e. Covered entities and business associates are required to adhere to the interim final Breach Notification rule effective September 23, 2009.

7. New Categories of HIPAA Criminal Violations:
   a. Any disclosure of PHI by a workforce member for purposes other than allowed by the HIPAA Privacy Rule, other federal law, other state law or as authorized by an individual is considered a criminal act.
   b. If a covered entity is found non-compliant with HIPAA rules due to willful neglect such violations are now considered a criminal act. If during a preliminary investigation HHS believes a violation is due to willful neglect, HHS must investigate.

8. Increased Enforcement and Increase in Civil Penalties:
   a. Categories of civil penalties have been expanded and the associated penalties have increased and in a number of cases significantly (see detailed analysis).

b. HHS in conjunction with guidance from the General Accounting Office (GAO) shall define a percentage of fines or monetary settlements that will be paid to individuals harmed by covered entity or business associate violations.
c. State Attorney General Offices now have the authority to file suit in federal court if the attorney general considers a violations to have harmed individuals in that state (does not prevent further or concurrent action on the part of HHS).
d. HHS is required to conduct regular compliance audits of covered entities and business associates.

9. New Federal Reporting/Study Requirements:
   a. HHS is required to report to Congress complaints of alleged HIPAA privacy and security violations received by OCR and CMS. The report will include detailed information about informal and formal action taken against a covered entity or business associate, reported breaches, etc. Also, the report must be posted on the HHS public web site.
   b. HHS is required to issue guidance on best practices for de-identification of PHI.
   c. HHS is required to study and report on the privacy and security requirements non-covered entities should adhere to (specifically PHR vendors and supporting third party service providers) and indicate the federal agency best suited to enforcing any new privacy and security rules imposed on these non-covered entities.
   d. HHS is required to study the definition of "psychotherapy notes" to determine if the definition found in the HIPAA privacy rule needs to be updated or amended.
   e. GAO is required to develop a report on the best practices related to disclosure of PHI between health care providers for the purpose of treatment.
   f. GAO is required to report to Congress and HHS the impact of this Act on health insurance premiums, overall health care costs, adoption of EHRs by providers and reduction in medical errors and other quality improvements.

## Title XIII, Subpart D Requirement Summary and Time Lines

| Requirement | Applies To | Compliance Date | HHS Responsibility | Enforcement Agency |
|---|---|---|---|---|
| **Expanded security rule compliance** | Business associate | February 17, 2010 | Promulgate rule | CMS |
| **Expanded privacy rule compliance** | Business associate | February 17, 2010 | Promulgate rule | OCR |
| **New categories of business associates** | Business associate | February 17, 2010 | Amend business associate definition | HHS |

 

| | | | | |
|---|---|---|---|---|
| | | | (HIPAA Administrative Simplification Provision Rules) | |
| **Expansion of civil and criminal penalties** | Business associate | February 17, 2009 | Promulgate rule | CMS, OCR, Dept. of Justice |
| **New privacy rule requirements – restriction requests** | Covered entity | February 19, 2010 | Promulgate rule | OCR |

| **Requirement** | Applies To | Compliance Date | HHS Responsibility | Enforcement Agency |
|---|---|---|---|---|
| **New privacy rule requirements – minimum necessary & limited data sets** | Covered entity | • Effective data of act<br>• 18 months from the effective date of ARRA | • New minimum necessary/ limited data set use requirements<br>• Publication of minimum necessary definition | • OCR<br>• HHS |
| **New privacy rule requirements – EHR accounting of disclosures** | Covered entity<br>Business associate | • Promulgate rule defining elements to include in accounting of disclosures with six months of a definition defined by the HIT Policy Committee<br>• If EHR implemented by 1/1/2009 – | • Define elements included in EHR accounting of disclosures<br>• Promulgate rule regarding effective date (may be later than dates included in ARRA but no later than 2016 and 2013 respectively) | OCR |

 

| | | | | |
|---|---|---|---|---|
| | | effective 1/1/2014<br>• If EHR implemented after 1/1/2009 – effective 1/1/2011 or when implement EHR | | |

 

| Requirement | Applies To | Compliance Date | HHS Responsibility | Enforcement Agency |
|---|---|---|---|---|
| **New privacy rule requirements – Payment for exchange of PHI** | Covered entity<br>Business associate | • 18 months from the effective date of ARRA promulgate rules<br>• Industry compliance 6 months from the date rules defining payment restrictions are finalized | Develop and publish rules regarding restriction on payment for the exchange of PHI | HHS |
| **New privacy rule requirements – Provide electronic copy of PHI** | Covered entity | February 17, 2010 | Amend HIPAA privacy rule | OCR |
| **New privacy rule requirements – Marketing** | Covered entity<br>Business associate | February 17, 2010 | Amend HIPAA privacy rule | OCR |
| **New privacy rule requirements – Fund raising** | Covered entity | February 17, 2010 | Amend HIPAA privacy rule | OCR |
| **Publish technical assistance/guidance related to security rule technical safeguards** | Center for Medicare and Medicaid Services | February 17, 2010 | Collaborate with stakeholders and publish annually technical guidance related to the security rule | CMS |

 

| Requirement | Applies To | Compliance Date | HHS Responsibility | Enforcement Agency |
|---|---|---|---|---|
| **Publish technical assistance/guidance regarding "securing" PHI (e.g., encryption, etc.)** | Dept. of Health & Human Services | Final guidance published August 24, 2009 | Collaborate with stakeholders and publish technical guidance regarding "securing" PHI and updating guidance annually | HHS |
| **Privacy education/ guidance** | HHS (likely OCR) | August 18, 2009 | Appoint one individual per HHS region responsible for providing education/guidance to covered entities, business associates and individuals regarding privacy and security rights and responsibilities | HHS |
| **Health information education initiatives** | OCR | February 17, 2010 | Create an educational program for individuals explaining privacy rights, use of PHI, etc. | HHS |
| **Breach notification** | Covered entity | August 24, 2009/Effective September 30, 2009 | • Promulgate rule defining notification requirements, terms and timing<br>• Maintain list of covered entities and associated breaches<br>• Post notice on HHS web site of all covered entities with breaches of | HHS |

 

| | | | | |
|---|---|---|---|---|
| | | | more than 500 individuals | |

| Requirement | Applies To | Compliance Date | HHS Responsibility | Enforcement Agency |
|---|---|---|---|---|
| **Breach notification** | Business associate | August 24, 2009/Effective September 30, 2009 | • Promulgate rule defining notification requirements, terms and timing | HHS |
| **Breach notification** | PHR vendors Supporting third party providers | 60 days following promulgation of interim final rules by the FTC | **FTC Responsibility -** Promulgate interim final rules within 180 days of the effective date of ARRA | FTC |
| **Breach notification** | HHS | February 17, 2010 | Report to Congress breaches that have occurred and related actions taken by HHS (to be repeated annually) | HHS |
| **Criminal activities – Release of PHI without authorization** | Covered entity Business associate | February 17, 2010 | Amend HIPAA privacy rule | OCR, Dept. of Justice |
| **Criminal activities – Willful neglect** | Covered entity | 24 months from the effective date of ARRA | Promulgate rule within 18 months of the effective date of ARRA | OCR, Dept. of Justice |
| **Increased civil penalty amounts** | Covered entity Business Associate | February 17, 2009 | Enforce HIPAA privacy and security rules and assess new penalties (OCR enforcement funded by penalties assessed) | OCR, CMS |

| Requirement | Applies To | Compliance Date | HHS Responsibility | Enforcement Agency |
|---|---|---|---|---|
| **Increased civil penalties – Percentage distribution to harmed individuals** | Covered entity<br>Business associate | 3 years from the effective date of ARRA | • GAO methodology report due to HHS within 18 months of the effective date of ARRA<br>• HHS promulgate rule defining percentage payments to harmed individuals | OCR, CMS |
| **State attorney general enforcement** | Covered entity<br>Business associate | February 17, 2010 | Review report of intent to pursue legal action and intervene as considered appropriate | OCR |
| **Privacy & security compliance audits** | Covered entity<br>Business associate | February 17, 2010 (will not be published until 2Q 2010) | Conduce periodic privacy and security compliance audits | OCR, CMS |
| **Enforcement report to Congress – General** | OCR, CMS | February 17, 2010 and annually thereafter | Annually report to Congress violations reported and investigated, actions taken and audits conducted | HHS |
| **Enforcement report to Congress – Public availability** | HHS | February 17, 2010 and annually thereafter | Post a copy of the Congressional report on the HHS public web site | HHS |
| **Guidance on de-identified information** | HHS | February 17, 2010 | Issue guidance on best practices for de-identifying PHI | HHS |

 

| Requirement | Applies To | Compliance Date | HHS Responsibility | Enforcement Agency |
|---|---|---|---|---|
| **Study – application of privacy & security practices on non-covered entities** | HHS (in conjunction with the FTC) | February 17, 2010 | Study and issue a report defining appropriate privacy and security practices for non-covered entities, recommended regulations and recommended federal enforcement agency | HHS |
| **Psychotherapy notes study** | HHS | February 17, 2010 | Study what constitutes psychotherapy notes and tools used to treat and evaluate individuals by mental health professionals with the intent of potentially revising the definition of psychotherapy notes | HHS |
| **Report – Disclosure for treatment purposes** | GAO | February 17, 2010 | Report analyzing disclosure of PHI for treatment purposes by health care providers and what is considered appropriate disclosure | GAO |
| **Report – Impact of ARRA provisions on the healthcare industry** | GAO | 5 years from the effective date of ARRA | Report analyzing the impact of the provisions of ARRA on the healthcare industry | GAO |

 

## Detailed Analysis – ARRA, Title XIII Privacy and Security Provisions

1. Business Associates – New Requirements:
    a. **HIPAA Security Rule Compliance –** Business associates are now subject to the requirements of the HIPAA security rule. This means what was previously required by contract between a business associate and a covered entity is now required by statute. In addition, business associates will now be subject to the same civil and criminal penalties as covered entities for non-compliance. Covered entities are required to modify their existing business associate contracts to reflect this new language (Section 13401(a) and (b)).

    b. **HIPAA Privacy Rule Compliance –** Business associates are now required to adhere to certain provisions of the HIPAA privacy rule. Business associates who create, use or disclose PHI on behalf of the covered entities they contract with may use and disclose the covered entity's PHI only if use and disclosure is compliant with the HIPAA privacy rule requirements in Section 164.504(e) of the privacy rule. Also, the additional requirements related to privacy and use and disclosure of PHI are applicable to business associates. The covered entity is required to include the new privacy rule requirements in the business associate contract between the covered entity and business associate.

    Business associates are also required to comply with Section 164.504(e)(1)(ii} of the HIPAA Privacy Rule and comply with the standards included in Sections 164.502(e) and 164.504(e), except pursuant to Section 164.504(e)(1)(ii) references to the business associate (regarding the business associate contract) will be treated as a reference to the covered entity. (Section 13404(a) and (b)).

    Business associates are now subject to the same civil and criminal penalties as covered entities if business associates violate these provisions of the HIPAA privacy rule (Section 13404(c)).

2. Business Associates – Newly Defined Included Entities: Health information Exchange organizations (HIEO), Regional Health Information Organizations (RHIO), E-prescribing Gateways or vendors who contract with covered entities to provide a PHR to the covered entities' patients or health plan members must enter into a business associate contract with participating covered entities. These entities are now considered business associates and subject to the HIPAA security and parts of the HIPAA privacy rule as described in this analysis (Section 13408).

3. New Privacy Rule Requirements:
    a. **Restriction Requests –** If an individual requests (HPAA privacy rule Section 164.522(a)(l)(i)(A)) a covered entity restrict the disclosure of the individual's PHI, the covered entity must comply with the requested restriction if (Section 13405(a)):
        i. Except as otherwise required by law, the disclosure is to a health plan for purposes of payment or health care operations.
        ii. The PHI is only related to a health care item (such as durable medical equipment) or service the health care provider has been paid out of pocket in full for (versus paid by a health plan).

    b. **Releases Limited to Limited Data Set or Minimum Necessary –** The minimum necessary requirement (45 CFR 164.502(b)(1) is reemphasized and modified to require covered entities use and disclosure a limited data set of PHI instead of following the minimum necessary standard in cases where use and disclosure of the limited data set will satisfy use and disclosure requirements (Section 13405(b)(1)(A)). This does not limit or eliminate any exceptions to the application of minimum necessary requirement upon ARRA enactment or following publication of a definition of "minimum necessary" such as for treatment purposes.

    HHS is required to specifically define the meaning of "minimum necessary." HHS is required to take into account what information is necessary to improve patient outcomes and to detect, prevent, and manage chronic disease. HHS is required to publish a definition of "minimum necessary" within 18 month of the effective date of ARRA. Following finalization and publication of the definition of "minimum necessary," the new requirements regarding the use of a limited data set and minimum necessary requirements will sunset(Section 13405(b)(1)(B).

    c. **Accounting of Disclosures from an Electronic Health Record (EHR), General Requirements –** Any covered entity that has or intends to implement an electronic health record (EHR) must include in any accounting of disclosures all disclosures made from the EHR including disclosures made for treatment, payment and healthcare operations. The exceptions to what needs to be included in an accounting of disclosures for other purposes (e.g., to the individual, pursuant to an authorization, etc.) still apply and do not need to be included in the accounting of disclosures from the EHR.

    The accounting of disclosures from an EHR that includes disclosures for treatment, payment and healthcare operations only includes disclosures for the three year

 

period prior to the date the accounting is requested (Section 13405(c)(1)).

d. **Accounting of Disclosures from an EHR, Process –** A covered entity who receives a request for an accounting of disclosures can elect to provide either (Section 1405(c)(3)):
    i. An accounting of disclosures made by the covered entity and the covered entity's business associate(s); or
    ii. Accountings of disclosures made by the covered entity and provide a list of the covered entity's business associates, including contact information (such as mailing address, phone, and email address). If the covered entity elects this option, the covered entity's business associate(s) are required to provide an accounting of disclosures made by the business associate upon a request from the individual made directly to the business associate.

e. **Accounting of Disclosures from an EHR, Effective Date –** Covered entities are required to provide an EHR accounting of disclosures that includes disclosures made for treatment, payment and healthcare operations (Section 13405(c)(4)(A) and (B)):
    i. Covered entities that implemented an EHR January 1, 2009 or earlier must comply by January 1, 2014.
    ii. Covered entities that implemented an EHR after January 1, 2009 must comply by January 1, 2011 or the date it implements an EHR. It is implied that compliance with this provision can occur no earlier than on or after HHS has finalized the rule defining what must be included in an EHR accounting of disclosures.

    HHS may adopt a later effective date if HHS (likely in response to analysis and public/industry comment) determines a later compliance date is appropriate. HHS, though, may not set an effective date later than (Section 13405(c)(4)(C)):
        1. 2016 for covered entities who implemented EHRs January 1, 2009 or earlier.
        2. 2013 for covered entities who implemented EHRs after January 1, 2009

f. **Accounting of Disclosures from an EHR, Rule Publication –** HHS is required to promulgate rule regarding what information must be included in an accounting of disclosure of disclosures made from an EHR no later than 6 months after the date the HIT Policy Committee and HHS adopts standards on accounting for disclosure (Section 3002(b)(2)(B)(iv)). Rules may only require the disclosure of information

 

collected through an EHR in a way that takes into account the interests of the individuals in learning the reason their PHI was disclosed. Also, the rules must take into account the administrative burden of accounting for EHR disclosures (Section 13405(c)(2)).

g. **Prohibition on the Sale of PHI, General Requirements –** Covered entities and business are prohibited from directly or indirectly receiving payment for the exchange of PHI unless the covered entity obtains an authorization from the individual that specifies the PHI may be exchanged for payment to the covered entity and whether or not the entity the covered entity discloses the individual's PHI may or may not also receive payment for further disclosure (Section 13405(d)).

h. **Prohibition on the Sale of PHI, Exceptions –** The prohibition against a covered entity or business associate receiving any payment for the disclosure of PHI does not apply if the purpose is for (Section 13405(d)(1) and (2)):
    i. Exchange for public health activities.
    ii. Exchange for research and payment reflects the costs of preparation and transmittal of the data for research purpose.
    iii. Exchange is for the treatment and subject to any rules HHS may promulgate to prevent PHI from inappropriate access, use, or disclosure.
    iv. Exchange is for health care operation.
    v. Payment covers the cost of the exchange between a covered entity and a business associate for activities related to the support of the covered entity's business and pursuant to a business associate contract.
    vi. Payment is for the cost to provide an individual a copy of the individual's PHI.
    vii. An exchange approved by HHS where HHS has determined that such an exchange is necessary and appropriate.

i. **Prohibition on the Sale of PHI, Publication of Rules –** No later than 18 months from the effective date of ARRA, HHS is required to promulgate rules regarding any remuneration associated with the exchange of PHI. When developing rules, HHS is required to (Section 13405(d)(3)):
    i. Evaluate the impact of remuneration restrictions to reasonably ensure remuneration reflects the costs of the preparation and transmittal of PHI for any of the noted exceptions such as for research, public health and activities of the Food and Drug Administration (FDA).
    ii. Determine if any additional restrictions to any listed exceptions actually reflects the cost of preparation and transmittal of PHI if established

 

restrictions will not impede research or public health activities.

j. **Prohibition on the Sale of PHI, Effective Date –** Exchange restrictions are effective on or after 6 months from the date final rules are published that implement restrictions on remuneration for the disclosure of PHI (Section 13405(d)(4)).

k. **Access to PHI in Electronic Format –** If a covered entity uses or maintains an EHR or other applications/databases that store an individual's PHI, the individual has the right to request and obtain a copy of such PHI which is part of the medical record or related application/database in an electronic format. Also, if the individual chooses, the covered entity is required to transmit the PHI requested directly to an entity or person designated by the individual (such requests must be clear and specific), provided that any such choice is clear, conspicuous, and specific. Any fee charged for providing an electronic copy cannot be any greater than the costs associated with the release or transmission of PHI to the individual or designated third party (Section 3405(e)).

l. **Use of PHI for Marketing Purposes, Generally –** Any communication from a covered entity or business associate about a product or service and for the purpose of marketing that product or service shall not be considered health care operations unless the communication is currently permitted marketing pursuant to the HIPAA privacy rule. Marketing requirement changes are effective 12 months from the effective date of ARRA (45 CFR 164.501) (Section 13406(a)(1) and (c)).

m. **Use of PHI for Marketing Purposes, Additional Exceptions –** A communication by a covered entity or business associate is not considered health care operations if the covered entity receives payment in exchange the communication except where (Section 13406(a)(2):
    i. Either – Each of the following conditions apply
        1. Communication describes a drug or biologic currently prescribed for the recipient of the communication; and
        2. Payment received is considered reasonable in amount (reasonable must be defined by HHS)
    ii. Or – Each of the following conditions apply
        1. Communication is made by the covered entity
        2. The covered entity obtains a valid authorization allowing the communication
    iii. Or – Each of the following conditions apply

 

1. The communication is made by a business associate on behalf a covered entity; and
2. The communication is consistent with the with the business associate contract between the business associate and covered entity

n. **Opportunity to Opt Out of Fundraising –** HHS is required to promulgate rule that defines that any written fund raising communication be clear and directly identify the communication as related to fund raising, inform the recipient that he or she has the right to request no further fund raising communication. When an individual elects not to receive any further fund raising communication it shall be treated in the same matter as the revocation of authorization. This does not represent a significant change from current HIPAA privacy rule requirements. The minor changes to fund raising communications are effective 12 months after the effective date of ARRA (Section 13406(b) and (c)).

4. Security Education/Guidance Provision Requirements:
   a. **Security Technology Safeguards –** The HIPAA security rule will continue to be enforced by the Center for Medicare and Medicaid Services (CMS). CMS is now required by statute, beginning immediately following ARRA enactment (February 17, 2009) and annually thereafter, to work with stakeholders and issue guidance on the most effective and appropriate technical safeguards to implement or follow to meet the requirements of the HIPAA security rule. This guidance would be available to both business associates and covered entities (Section 13401(c)).

   b. **Methods of Securing/Encrypting PHI –** No later than 60 days after the effective date of ARRA, HHS is required to work with stakeholders and publish guidance that defines technologies and methodologies that can be used to make PHI unusable, unreadable, or indecipherable to unauthorized individuals. Guidance must be updated annually (Section 13402(h)(2)).

5. Privacy Education/Guidance Provision Requirements:
   a. **Regional Educational Requirements –** HHS (likely the Office for Civil Rights (OCR)) is required to designate an individual in each regional office who is responsible for providing guidance/education to covered entities, business associates, and individuals on HIPAA privacy and security rule rights and responsibilities. HHS is required to designate that individual no later than 6 months from the effective date of ARRA (Section 13403(a)).

 

b. **Health Information Use Educational Initiatives –** OCR is required to develop and maintain a national education initiative that is intended to increase transparency regarding the uses of PHI which includes programs to educate individuals about potential uses of their PHI, the effects of such uses, and individual rights of individuals. The educational program must be conducted in different languages presented in a clear and understandable manner. The education initiative must be implemented no later than 12 months after the date of enactment of ARRA (Section 13403(b)).

6. Breach Notification Requirements: Covered entities, business associates and personal health record (PHR) vendors are required to notify individuals in the event a breach of any unsecured protected health information (PHI)/individually identifiable health information (IIHI). This applies to electronic and non-electronic unprotected PHI. PHI includes data that is broader than just health information or financial information, pursuant to the definition found in the HIPAA Administrative Simplification rules (Section 13402).

   a. **Definition of "Unsecured PHI" –** It is the responsibility of HHS to fully define the definition of "unsecured PHI." HHS published a final definition of "unsecured PHI" August 24, 2009 (included in preamble to Breach Notification interim final rule). "Unsecured" electronic PHI is PHI that has not been encrypted in accordance with the standards published by the National Institute on Standards and Technology (NIST). "Unsecured" paper PHI is any PHI that is not shredded or destroyed. (Section 1402(h)(1)).

   b. **General Breach Description Notification Requirements –** Covered entities have an obligation to notify individuals of the breach. The definition of a breach and the notification requirements are as follows (Section 13401(c) and (d)):
      i. A breach is considered to be discovered as of the first day the breach is discovered or should reasonably have been known to have occurred.
      ii. Notifications must be made "without unreasonable delay" but no later than 60 calendar days after the breach discovery by the covered entity or business associate to the covered entity.
      iii. The business associate has no more than 60 days to notify the covered entity of any breach.
      iv. The covered entity has no more than 60 days from the date the covered entity was notified by the business associate or the date the covered entity discovered the breach to notify individuals and, if appropriate, HHS.
      v. The covered entity or business associate has the burden of demonstrating notifications were made timely. This includes retaining appropriate

 

documentation related to breach notification.

c. **Methods of Notification –** Notice must be provided to the individual using the following form Section 13401(e)):
   i. It is the responsibility of the covered entity to notify affected individuals even if the breach was reported to the covered entity by the business associate.
   ii. Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address or, if e-mail is the specified notification preference of the individual, by e-mail. There may be several individual notifications if additional information about the breach becomes available after the first notice is sent.
   iii. If there is insufficient or out-of-date contact information (including phone number, e-mail address, or available contact information) that prevents direct individual notification, a substitute notice is required.
   iv. The substitute notice is required if there are 10 or more individuals where there is insufficient or out-of-date contact information. The substitute notice includes conspicuous posting of the breach for at least 90 days on the home page of the Web site of the covered entity or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside.
   v. Media and/or Web notices need to include a toll-free phone number the individual can call to learn whether or not the individual's unsecured PHI was or potentially was a part of the breach and the toll free number must be active for a minimum of 90 days.
   vi. If the notice is made through the media, the notice must be made to well known media outlets in the state or jurisdiction. Also, if the breach involved 500 or more residents of a given state or jurisdiction is, media announcement is required.

d. **Notification Content –** The breach notice must include, to the extent possible, the following (Section 13402(f)):
   i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
   ii. A description of the types of PHI breached or inappropriately disclosed (e.g., full name, Social Security number, date of birth, home address, account number, health condition, etc.).
   iii. The steps individuals should take to protect themselves from potential harm resulting from the breach.

 

iv. A brief description of what the covered entity is doing to investigate the breach, mitigate losses and protect against further breaches.
v. Covered entity contact information (must include a toll-free number, e-mail address, Web site or postal address).

e. **Notification Delay for Law Enforcement Purposes –** If a law enforcement official determines that required notification would impede a criminal investigation or cause damage to national security, notification shall be delayed for the period defined by law enforcement (Section 13402(g)).

f. **Congressional Notification –** No later than 12 months after the effective date of ARRA and annually thereafter, HHS is required provide Congress a report regarding reported breaches (Section 13402(i)(1). The notice shall include (Section 13402(i)(2)):
   i. Number and nature of reported breaches.
   ii. Actions taken in response to reported breaches.

g. **Specific Covered Entity Requirements –** In the event of a breach, a covered entity that stores, uses or discloses unsecured PHI is required to notify each individual whose unsecured PHI has been, or is reasonably believed to have been breached or inappropriately accessed by an individual or entity (includes internal and external breaches/inappropriate disclosure) within 60 days (Section 13402(a)).

   Covered entities are required to notify HHS if a breach occurs that involves 500 or more individuals. This notice is required immediately following the discovery of the breach. If the breach involved fewer than 500 individuals, the covered entity is required to maintain a breach log (may be addition to disclosure accounting; breaches and inappropriate disclosures already must be recorded in any patient or individual disclosure accounting). The breach log must be reported annually to HHS for the preceding year within 60 days from the end of that year. HHS will post on its public Web site a list that specifically identifies each covered entity involved in a breach that involved 500 or more individuals (Section 13402(f)).

h. **Specific Business Associate Requirements –** In the event of a breach, a business associate that stores, uses or discloses unsecured PHI is required to notify the covered entity of the breach. The notice needs to include the identification of each individual whose unsecured protected health information has been, or is reasonably believed to have been breached or inappropriately accessed (includes internal and external breaches/inappropriate disclosure) and sufficient detailed information to

accommodate the covered entity's individual notification requirements (Section 13402(b)).

i. **PHR Vendor Requirements –** Following the discovery of a security breach of unsecured IIHI, all vendors of personal health records (PHR) (includes vendors providing or managing PHRs on behalf of another entity or vendors directly marketing PHRs to individuals) vendors shall (Section 13407):
   i. Notify each individual who is a citizen or resident of the US whose unsecured IIHI was breached; and
   ii. Notify the Federal Trade Commission (FTC).

   If the vendor is a third party service provider under contract with the PHR vendor and discovers a breach of IIHI, the third party service provider notify the vendor or entity the third party service provider is contracted with of the breach. The notice must include identification of each individual whose unsecured IIHI was or is reasonably believed to have been breached or inappropriately disclosed.

   Timeliness of reporting, the reporting method and the contents of any notifications shall be determined by the FTC. The FTC is required to notify HHS whenever notified of a breach of IIHI from a PHR. A violation of the PHR breach notification requirements shall be treated as an unfair and deceptive act or practice in violation of FTC Act, Section 18(a)(1)(B).

   The FTC is required to promulgate interim final rules within 180 days after enactment of ARRA. The breach notification requirements apply to breaches discovered on or after 30 days following the effective date of interim final rules.

7. Criminal Activities – New Categories:
   a. **Release of PHI Without Authorization –** If a workforce member discloses PHI for purposes other than allowed by the HIPAA Privacy Rule, other federal law, other state law or as authorized by an individual, such an act shall be considered a criminal violation and subject to the HIPAA Administrative Simplification Provisions criminal penalties (Section 13409).

   b. **Willful Neglect –** If a covered entity is found non-compliant with HIPAA rules due to willful neglect, the covered entity shall be subject to criminal penalties described pursuant to the HIPAA Administrative Simplification Provisions. HHS is required to investigate any such violations to determine if the cause of a violation is due to willful neglect if a preliminary finding indicates that the violation was due to willful

 

neglect (Section 13410(a)).

Willful neglect will be considered a criminal violation effective for any violation occurring 24 months from the date of ARRA enactment. HHS shall promulgate rules regarding investigation and penalties associated with a finding of willful neglect no later than 18 months from the date of ARRA enactment (Section 13410(b)).

8. Increased Enforcement:
    a. **Increase or Changes in Civil Penalties Assessed –** The amount of civil penalties is changed to Section 13410(d)):
        i. If the violation was due to the fact that the person did not know, and by exercising reasonable diligence would not have known, the person violated HIPAA privacy and security provisions ("reasonable person" concept), the penalty for each violation shall be not less than $100 for each such violation (total amount imposed for the same violations in a calendar year not to exceed $25,000) and not more than $50,000 for each violation (total amount imposed for the same violations in a calendar year not to exceed $1,500,000).
        ii. If the violation was due to reasonable cause but not willful neglect, the penalty for each violation shall be not less than $1,000 for each violation (total amount imposed for the same violations in a calendar year not to exceed $100,000) and not more than $50,000 for each violation (total amount imposed for the same violations in a calendar year not to exceed $1,500,000).
        iii. If the violation was due to willful neglect –
            1. If the violation is corrected timely, the penalty for each violation shall be not less than $10,000 for each violation (total amount imposed for the same violations in a calendar year not to exceed $250,000) and not more than $50,000 for each violation (total amount imposed for the same violations in a calendar year not to exceed $1,500,000).
            2. If the violation is not corrected timely, penalty for each violation shall be $50,000 for each violation (total amount imposed for the same violations in a calendar year not to exceed $1,500,000).

    b. **Effective Date of New Penalty Amounts –** The new penalty amounts and the criteria for determining the amount of any civil penalties levied is effective upon enactment of ARRA.

c. **Distribution of Civil Penalties Collected –** Any penalties collected under the enhanced enforcement provisions shall be paid to OCR to be used for purposes enforcement (Section 13410(c)(1)).

d. **Report from the General Accounting Office (GAO) –** GAO shall submit a report to HHS no later than 18 months following the effective date of ARRA that includes recommendations for a methodology to be used to calculate the percentage of any civil penalties collected to be paid to any individual harmed by a civil violation (Section 13410(c)(2)).

e. **Distribution of a Percentage of Penalties Collected to Harmed Individuals –** HHS shall promulgate rule based on the recommendations from GAO within three years of the effective date of ARRA a methodology to pay a percentage of penalties collected to any harmed individual (Section 13410(c)(3). The methodology will apply to all penalties or settlements imposed on or after the date the rule is promulgated.

f. **Enforcement Through State Attorney Generals' Office, General –** If the attorney general of any state believes one or more individual within a state has been threatened or harmed by a person violating the HIPAA privacy and security rules, the attorney general may bring a civil action on behalf of these individuals in US District Court to (Section 13410(e)(1)):
    i. Enjoin further violations by the defendant; or
    ii. Obtain damages on behalf of these individuals

    Action may be taken by state attorney generals' offices beginning on the effective date of ARRA (Section 13410(e)(3)).

g. **Enforcement Through State Attorney Generals' Office, Statutory Damages –** The amount of damages is calculated by multiplying the number of violations by $100 and the total amount of damages cannot exceed $25,000. Violations have the same meaning as the definition of a violation pursuant to the HIPAA Administrative Simplification Provisions rules (Section 13410(e)(2)). The court may also assess reasonable legal fees against the violator (Section 13410(e)(3).

h. **Enforcement Through State Attorney Generals' Office, Notice to HHS –** The state attorney general must notify HHS and provide a copy of the complaint prior to taking any legal action or, if that is not feasible, immediately upon taking legal action. HHS has the right to (Section 13410(e)(4):
    i. Intervene in the action;

 

ii. After intervening, be heard on all matters relating to the civil action; and
iii. File petitions for appeal

i. **Enforcement Through State Attorney Generals' Office, Limitations –** If federal action is pending for the same violations, the state attorney general has no right of action (Section 13410(e)(7)). Also, the right to bring civil action by a state attorney general's office against a person for violations does not prevent OCR from imposing corrective action without penalty in cases where the person did not know, and by exercising reasonable diligence would not have known, the person had committed a violation (Section 13410(f)).

9. Compliance Audits: OCR and CMS shall periodically audit covered entities and business associates to reasonably ensure compliance with the HIPAA privacy and security rules and new provisions included in ARRA (Section 13411).

10. HHS Reporting Requirements:
    a. **Report of Violations –** HHS is required to report to Congress beginning one year after the effective date of ARRA and annually thereafter complaints of alleged violations of law relating to privacy and security of PHI received by OCR and CMS during the year covered by the report (Section 13424(a)(1). The report shall include:
        i. Number of complaints;
        ii. Number of complaints resolved informally, a summary of the types of complaints resolved informally, the number of covered entities that received technical assistance from OCR and CMS during the reporting year to comply with the HIPAA privacy and security rules and the types of such technical assistance provided;
        iii. Number of complaints that have resulted civil penalties or monetary settlements, including the complaints involved and the penalty or monetary settlement associated with each assessment;
        iv. Number of compliance reviews conducted and the outcome;
        v. Number of subpoenas or inquiries issued;
        vi. HHS' plan to improve compliance and enforcement for the following year; and
        vii. Number of audits performed and a summary of audit findings

    b. **Report Publication –** The annual report presented to Congress by HHS will be posted on the HHS public web site (Section 13424(a)(2)).

 

11. HHS Guidance on Specification Implementation for the De-identification of PHI: HHS in consultation with stakeholders shall issue guidance on best practices for de-identification of PHI no later than 12 months from the effective date of ARRA (Section 13424(c)).

12. HHS Study of Non-covered Entities: HHS in consultation with the FTC is required to conduct a study and submit a report regarding the results of that study within one year from the effective date of ARRA. The report shall focus on privacy and security requirements for entities that are not covered entities or business associates at the time of ARRA enactment (Section 13424(b).

    The report shall include a study of appropriate privacy and security requirements and breach notification (including notice exemptions because the breach involved secure PHI) requirements that should be applied to:

    a. Vendors of PHRs;
    b. Entities that offer products or services through the website of a vendor of PHRs;
    c. Entities that are not covered entities and offer products or services through the websites of covered entities who offer individuals PHRs;
    d. Entities that are not covered entities with access to PHR information or send information to a PHR; and
    e. Third party service providers used by a vendor or entity to assist in providing PHR products or services;

    The report shall include a determination of which Federal agency is best equipped to enforce privacy and security requirements non-covered entity and business associates described above along with a time line for regulatory implementation. The report shall then be submitted to Congress.

13. HHS Study – Definition of Psychotherapy Notes: HHS is required to study the definition of "psychotherapy notes." The study needs to include an evaluation of test data related to patient direct responses, scores, items, forms, protocols, manuals or other materials that are part of a mental health evaluation (as determined by the mental health professional providing treatment or evaluation). The purpose of the study is to determine if the regulatory definition of “psychotherapy notes” needs to be revised (Section 13424(f)).

14. GAO Report Regarding Use and Disclosure for Treatment Purposes: GAO is responsible for submitting to Congress a report on the best practices related to disclosure of PHI between health care providers for the purpose of treatment within one year from the effective date of ARRA. The report shall include an examination of best practices implemented by states and other entities such as HIEOs, RHIOs, etc. Best practices examined shall include practices

 

improving the quality of health care, the ability of the provider to manage those practices and an examination of the use of an electronic consent form related to the use and

disclosure of PHI for treatment, payment and healthcare operations. The report will include successes and failures regarding attempts to implement best practices (Section 13424(d)).

15. GAO Report Regarding the Impact of ARRA, Title XIII on the Healthcare Industry: GAO is responsible for reporting to Congress and HHS within five years of the enactment of ARRA the impact of this Act on health insurance premiums, overall health care costs, adoption of EHRs by providers and reduction in medical errors and other quality improvements (Section 13424(e).

 