**HIPAA Group, Inc.**
**4409 Hoffner Avenue, # 171, Orlando, FL 32812**
**Phone: 888-494-6987**
**www.HIPAAgroup.com**
*University of Central Florida - Authorized Training Partner*

# Summary of Recent HIPAA Changes

Changes to HIPAA are contained in the "HITECH Act", which is Title XIII of the ARRA, the "American Recovery and Reinvestment Act". Both became law on February 17, 2009, and most changes to HIPAA became effective on February 17, 2010. See the list of abbreviations used at the end of this document.

- **New Enforcement Rules**
  Effective: Applies to penalties issued 24 months after enactment.
  Effective: Implementing Regs within 18 months after enactment.
  - Mandatory investigations for "willful neglect" cases.
  - Mandatory civil penalties for "willful neglect" violations.
  - Periodic compliance audits for CE's and BA's.
  - Fines & penalties paid will go to OCR for increased investigations & enforcement.
  - Harmed individuals will get a percent (t.b.d.) of CMP or settlement.
    - Recommendations report in 18 months.
    - System in place within 3 years.
  - In addition to CE's, individuals now made subject to HIPAA criminal provisions.
  - State AG's can bring civil suits in federal courts on behalf of state residents.

- **New HIPAA Penalties**
  Effective: Immediately.
  - Increased penalties for violations.
  - Penalties calculated on variety of factors.
  - Four tiers of penalties, depending on nature of offense…
    - **Tier A** - Offender didn't know, and by reasonable diligence would not have known, that he or she violated the law.
      - $100 per violation
      - $25,000 annual maximum total per violator
    - **Tier B** - Violation due to reasonable cause and not willful neglect.
      - $1,000 per violation
      - $100,000 annual maximum total per violator
    - **Tier C** - Violation due to willful neglect but was corrected.
      - $10,000 per violation
      - $250,000 annual maximum total per violator
    - **Tier D** - Violation due to willful neglect and was not corrected.
      - $50,000 per violation
      - $1,500,000 annual maximum total per violator

- **Breach Notifications to Consumers**
  Effective: Implementing Regs from HHS due within 6 months after enactment.
  Effective: Beginning with breaches 30 days after Regs are published by HHS.
  - CE's, BA's, and PHR Vendors are subject to breach notification requirements.
  - Notify consumers if "unsecured" PHI was accessed, acquired, or disclosed in breach.
  - "Unsecured" essentially means "unencrypted" data, including all physical media.
  - Notices must be sent "without reasonable delay" – no later than 60 days after breach.
  - Minimum content of notifications is specified in the regs.
  - Notices sent by 1st class mail – email only if consumer stated a preference for email.
  - If 10 or more victims can't be located, notice on website or in media must be posted.
  - Breaches involving > 500 victims: Mandatory, immediate reporting to HHS.
  - Breaches involving < 500 victims. Entity keeps log, provides to HHS annually.
  - If over 500 victims, HHS will publicly post on Internet.
  - PHR breaches get reported to FTC, and FTC in turn notifies HHS.

- Guidance from Sec of HHS within 60 days after enactment.

- **Business Associates Must Comply with HIPAA Security Rule**
  Effective: 12 months after enactment.
  - BA's subject to same civil & criminal penalties as CE's.
  - BA's must comply with Administrative, Technical, and Physical Safeguards.
  - BA's must establish and maintain appropriate policies and procedures.
  - BA's must document all Security Rule compliance activities.
  - BA's must report breaches just like CE's.
  - BA Contracts must be created or amended to include new requirements.
  - BA's don't comply with Privacy Rule, but are restricted from PHI uses and disclosures not in compliance with BA contract. This represents "de-facto" Privacy compliance.
  - PHR Vendors and Health Information Exchanges become Business Associates.

- **Disclosure Accounting Includes TPO Disclosures if EHR Used**
  Effective: January 01, 2011 and January 01, 2014.
  - If EHR used, patient has new Right to accounting of disclosures for TPO.
  - Such accounting can go back 3 years from date of request.
  - Can charge reasonable fees for accounting, but no greater than direct labor cost.
  - HHS must adopt & publish standards within 6 months from enactment.

- **New Right to Obtain Copies of Electronic Health Records**
  Effective: 6 months after enactment.
  - When CE uses an EHR, individual has Right to an electronic copy of their records.
  - Individual can direct CE to send an electronic copy directly to another party or entity.
  - Maximum fees are the direct labor costs associated with fulfilling the request.

- **Expanded Right to Privacy Restrictions**
  Effective: 12 months after enactment.
  - CE's must agree to individual disclosure restriction requests – previously was optional.
  - Some exceptions exist with regard to health plans and payments.
  - Much CE confusion, some push-back, expected over this.

- **New Restrictions on Marketing & Fundraising**
  Effective: 12 months after enactment.
  - Definition of "Marketing" clarified.
  - Recipients must have clear & conspicuous way to "opt out" of future communications.
  - Opt-out must be regarded as "revocation of authorization" to market-to.
  - Restrictions apply to communications made after Feb. 17, 2010. (12 mo. > enactment)

- **No Selling of PHI**
  Effective: New Regs from HHS within 6 months after enactment.
  Effective: Compliance is 18 months after new Regs from HHS.
  - HIPAA previously allowed payment to CE for PHI as long as disclosure was otherwise lawful and permitted by Privacy Rule.
  - CE will not be able to receive payment for PHI, even if disclosure is permitted, without an auth from patient that includes permission to sell from patient.
  - A number of exceptions exist, for research, public health activities, sale or transfer of practice, etc.

- **Priority for Limited Data Sets and De-identified Data**
  Effective: 12 months after enactment.
  - Limited Data Set (LDS) disclosures are preferred over "minimum necessary" disclosures.
  - Provides a simpler, clearer approach to de-identifying data for uses and disclosures not involving treatment or payment.

- **Clarification of Minimum Necessary Rule**
  Effective: New Guidance from HHS within 18 months after enactment.
  - Aims to clarify definition and practical use of "Minimum Necessary" and LDS's.
  - Scope of PHI requests from one CE to another treating same patient was major concern.
  - No CE's or BA's held to new standard till new Guidance is issued.

# Important ARRA and HITECH Act Dates

**Upon enactment (February 17, 2009)**
- Application of new tiered civil monetary penalties (for offense occurring post−enactment).

**Upon enactment (February 17, 2009)**
- State Attorneys General enforcement powers take effect.

**April 17, 2009**
- HHS secretary's deadline to define "unsecured PHI." The new law forces providers to notify individuals whose "unsecured PHI" has been accessed because of a privacy or security breach. If HHS does not define "unsecured PHI" by this date, the definition defaults to one produced by the National Institute of Standards and Technology.

**Within 60 days of enactment (April 20, 2009)**
- HHS Secretary must set forth list of technologies and methodologies that render information "unusable, unreadable or indecipherable" (relevant for breach notification provisions).

**Within 180 days of enactment (August 17, 2009)**
- HHS and FTC must each promulgate interim final regulations on breach notification (apply to breaches discovered on or after the interim final regulations have been published).

**August 17, 2009**
- Deadline for Secretary of HHS to identify what must be included when a patient requests an accounting of disclosures on electronic health records (EHR). Individuals can now access disclosures for treatment, payment, or healthcare operations.

**By 12/31/2009**
- HHS must adopt (through rulemaking) the initial prioritized set of standards (which should include the accounting for disclosures new technical standard. Regs to implement that standard are due 6 months after the technical standard has been adopted).

**By February 17, 2010**
- HITECH Act's restrictions on marketing and fundraising take effect.
- Deadline for the HHS secretary to issue guidance on how covered entities must comply with "de-identification" of PHI, or limits that apply when CE's use patients' information for research purposes.
- HHS (& FTC) study on privacy and security requirements for PHR vendors and applications.
- GAO study on best practices for disclosures for treatment (and use of electronic informed consent).
- First annual report on HIPAA enforcement.
- First annual guidance on the most effective and appropriate technical safeguards for health information.
- HHS study on de-identification.
- HHS implements health information privacy educational initiative.

**Effective February 17, 2010**
- Application of rules to, and accountability for, business associates.
- Clarification of which entities are required to be business associates (although arguably already accomplished for most RHIOs & HIEs through HIPAA guidance issued by HHS in December 2008).
- Right to restrict disclosures to health plans.
- Deeming of limited data set as satisfying minimum necessary standard.
- Right of electronic access/electronic copy.
- Clarification of marketing provisions.
- Opt−out for fundraising communications (although current HIPAA Privacy Rule provisions remain in effect).
- Clarification of ability to impose criminal penalties against individuals.
- Civil monetary penalties and settlements flowing to OCR for enforcement.
- Requirement for Secretary to periodically audit entities covered by HIPAA.

**Within 18 months of enactment (August 17, 2010)**

- Secretary's guidance on minimum necessary.
- Regulations re: sale of data prohibition (effective 6 months post promulgation).
- GAO report on methodology for providing individuals with a percentage of HIPAA penalties.
- Regulations on imposition of civil monetary penalties in cases of willful neglect (and with respect to when the Secretary can civilly pursue violations of HIPAA that qualify as criminal).

**January 1, 2011**
- Initial deadline for complying with new accounting for disclosure rules for entities implementing electronic record systems after 1/1/09.

**24 months post enactment (February 17, 2011)**
- Clarification of ability to pursue civil penalties when criminal penalties are not pursued (applies to violations discovered on or after 02-17-2011).
- Requirement to impose civil monetary penalties in cases of willful neglect (same date).

**Three years post enactment (February 17, 2012)**
- Regulations for methodology for providing individuals with a percentage of HIPAA penalties.

**By 2013**
- Extended deadline for newer systems to comply with new accounting for disclosure rules.

**January 1, 2014**
- Initial deadline for older systems to comply with new accounting for disclosure rules.

**Five years post enactment (February 17, 2014)**
- GAO study on impact of ARRA.

**By 2016**
- Extended deadline for older systems to comply with new accounting for disclosure rules.

## Abbreviations Used in this Document

**AG –** Attorneys General of individual US states.
**ARRA** – The American Recovery and Reinvestment Act, which contains the HITECH Act (Title XIII).
**BA** – Business Associate as defined by HIPAA.
**CE** – Covered Entity as defined by HIPAA.
**CMP** – Civil Monetary Penalty, one of several types of HIPAA punishments.
**FTC** – The US Federal Trade Commission
**HHS** – The US Department of Health and Human Services.
**HITECH Act** – Title XIII of the ARRA, containing most of the recent changes and expansions to HIPAA.
**OCR** – The Office for Civil Rights, that part of the US Department of Health and Human Services responsible for enforcing HIPAA's Privacy and Security Rules.
**PHI** – Protected Health Information: individually identifiable health information protected by HIPAA law.
**PHR** – Personal Health Record: generally an individual's electronic health record
**Regs** – The HIPAA regulations.
**t.b.d.** – To be Determined.
**TPO** – Treatment, Payment, and Operations: three categories of uses and disclosures that Covered Entities can generally make *without* a patient authorization.

==========