

ARRA 2009:  
Privacy and Security Provisions

Deven McGraw

CENTER FOR DEMOCRACY & TECHNOLOGY

---

## Health Privacy Project at CDT

- Health IT and electronic health information exchange have tremendous potential to improve health care quality, reduce costs, and empower consumers
  - The public wants health IT – but also has significant privacy concerns.
  - For years there was no progress on resolving the privacy and security issues raised by e-health
  - Project's aim: Develop and promote workable privacy and security policy solutions for personal health information
-

---

## ARRA (Title XIII- HITECH)

- ❑ Broke the privacy “logjam”
  - ❑ Most significant change to the healthcare privacy and security environment since the original HIPAA privacy rule
  - ❑ Not a change to everything about HIPAA – but some significant changes that will need to be addressed by many entities handling health care information
  - ❑ Most provisions require further regulatory clarification
- 
-

---

## Privacy and Security Provisions – Overview – 4 broad areas:

- ❑ Substantive changes to HIPAA statutory provisions and privacy and security regulations.
  - ❑ Enhanced enforcement of HIPAA
  - ❑ Provisions to address health information held by some entities not covered by HIPAA
  - ❑ Misc:  
Administration/Studies/Reports/Educational Initiatives
-

---

## Substantive HIPAA Changes

- ▣ Breach notification requirement – In effect this September
    - ▣ Definition of breach – unauthorized access, use or disclosure; some exceptions
    - ▣ Safe harbor for “protected” data – per HHS guidance, must be encrypted (or appropriately destroyed)
  
  - ▣ Strengthened individual right to restrict disclosures to health plans for payment and operations
-

---

## Substantive HIPAA changes (cont.)

- ▣ Secretary guidance on minimum necessary
  - ▣ Use of limited data set where possible in interim
  - ▣ Discloser determines minimum necessary
- ▣ Minimum necessary still does not apply to treatment disclosures

---

## Substantive HIPAA changes (cont.)

- ▣ Accounting for disclosure requirements for entities using electronic health records
    - ▣ Requirement applies after standard and regulations are developed
    - ▣ Phased in over time
    - ▣ Covers only 3 years
  - ▣ Change with respect to how business associates comply
-

---

## Substantive HIPAA changes (cont.)

- ▣ Patient right of electronic access
    - ▣ Can direct record to another entity or individual (PHR)
  - ▣ Changes to definition of marketing
    - ▣ Limited right to use information for marketing if the communication is paid for by an outside entity
    - ▣ Exceptions for treatment communications and communications about current drugs and biologics
  - ▣ Opt-out for fundraising communications
  - ▣ BA contracts required for RHIOs – and PHRs in some instances
- 
-

---

## Substantive HIPAA changes (cont.)

- ❑ Prohibition on “sale” of health records or protected health information
  - ❑ Exceptions
    - ❑ Public health
    - ❑ Research
    - ❑ Treatment of an individual
    - ❑ Sale of a facility/business
    - ❑ Payments to business associates
    - ❑ Copies to individuals
-

---

## HIPAA Enforcement

- ▣ Business Associates accountable to authorities for compliance with *some* HIPAA privacy and security rules (+ new provisions)
  - ▣ Application of HIPAA criminal provisions to individuals
  - ▣ Requirement to impose civil penalties in cases of willful neglect
    - ▣ Corrective action may still be pursued for lesser offenses
- 
-

---

## HIPAA Enforcement (cont)

- ▣ Tiered increase in civil monetary penalties
  - ▣ Distribution of % of civil penalties to individuals (penalties also go to OCR)
  - ▣ State AG civil enforcement
  - ▣ Secretary required to do periodic audits
- 
-

## Provisions for Entities not Covered by HIPAA

- “Temporary” breach notification provisions for PHR vendors and internet applications
  - Breach definition – if not authorized by the individual
  - Same safe harbor for protected information
  - Enforced by FTC
  - FTC has made clear – if HIPAA breach notifications apply, FTC rules do not

## Provisions for Entities not Covered by HIPAA (cont.)

- ▣ Study by HHS & FTC with report to Congress on privacy and security recommendations for PHRs
  - ▣ Which agency should regulate?
  - ▣ Timeframe for regulations (no specific authority to regulate)

## Misc.

### (Administration/Studies/Reports/Educational Initiatives)

- ▣ Strengthened authority for ONC
- ▣ New advisory committees on policy and standards
- ▣ OCR public education initiative on uses of PHI and individual rights under HIPAA
- ▣ Privacy Officers in each HHS region
- ▣ Chief Privacy Officer within ONC
  - ▣ Not charged with HIPAA enforcement/oversight

## Misc. (Studies/Reports/Educational Initiatives)

- ▣ Studies/Reports by HHS Secretary
  - ▣ Annual report on enforcement
  - ▣ Study on implementation of the de-identification requirements
  - ▣ Study of HIPAA definition of psychotherapy notes to determine whether or not to include psychological test data and materials used for evaluative purposes

## Misc. (Studies/Reports/Educational Initiatives)

### □ GAO Studies:

- Methodology for providing individuals with a % of civil monetary penalties
- Report on best practices for disclosure of PHI for treatment purposes
- Report on Impact of ARRA provisions on health care costs and adoption of EHRs

For privacy to enable health IT, we  
have to enable privacy

[deven@cdt.org](mailto:deven@cdt.org)

CENTER FOR DEMOCRACY & TECHNOLOGY