

SEVENTH NATIONAL

MARCH 11-13, 2009

# MEDICAL BANKING INSTITUTE

BUILDING AN ELECTRONIC  
Medical Banking  
Community



ORGANIZED BY



EDUCATIONAL GRANTOR



PLATINUM SPONSOR



Seventh National Medical Banking Institute | March 11-13, 2009 | Nashville, TN

BUILDING AN ELECTRONIC  
**Medical Banking  
Community**

**The Great Privacy Debate: Impact of ARRA 2009**

Deven McGraw

Director, Health Privacy Project  
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
- ❖ Failure to build foundation of trust is an obstacle to achieving greater health information exchange

## Health Privacy Project at CDT

- ❖ 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

# Evolution of Federal Privacy Protections

- ❖ 1996 – Enactment of Health Insurance Portability and Accountability Act (HIPAA)
  - ❑ Congress gives itself 3 years to enact privacy legislation
- ❖ Rulemaking
  - ❑ 1999 – Proposed rules
  - ❑ 2000 – Final rule
  - ❑ 2002 – Regulatory changes
  - ❑ 2003 – Effective for most

## Era of Health Information Technology

- ❖ Health IT bills stalled in 108<sup>th</sup> & 109<sup>th</sup>
  - ❑ Privacy was framed as the obstacle – but it wasn't the only issue
- ❖ Legislation moved furthest in 110<sup>th</sup> – but economic woes stalled progress

## 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

- ❖ 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

- Definition of breach
- Safe harbor for “protected” data
- Detailed requirements re: timing and content of notice; how provided to individual and HHS
- Business Associates must notify covered entities

## ❖ 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

## 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
  - Designated by Secretary in regulations

## 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
- ❖ Ability to civilly enforce where violation qualifies as criminal but no criminal penalties pursued

## HIPAA Enforcement (cont)

- ❖ Requirement to impose civil penalties in cases of willful neglect
  - ❑ Corrective action may still be pursued for lesser offenses
- ❖ 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
  - Same safe harbor for protected information
  - Enforced by FTC

## 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 with respect to inclusion of 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

# Thank You

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

❖ <http://www.cdt.org/healthprivacy>