

HITECH and HIPAA: Highlights for Health Departments

Aimee Wall
UNC School of Government

November 9, 2009



UNC
SCHOOL OF GOVERNMENT

www.sog.unc.edu

Roadmap

- Breach notification requirements
 - HITECH
 - State law
- Business associates
- Enforcement
- Individual rights

Breaches

- HITECH
 - What is a breach?
 - What must a LHD do if it discovers a breach?
- State Identity Theft Law
 - What is a security breach?
 - What must a LHD do if it discovers a breach?

HITECH

- What is a breach?
 1. Acquisition, access, use, or disclosure of PHI
 2. In a manner not permitted by the HIPAA Privacy Regulation
 3. Which poses a significant risk of financial, reputational, or other harm to the individual

HITECH

- Notification required: If LHD discovers a breach of “unsecured PHI,” LHD must notify:
 - Individuals
 - DHHS
 - Media (if >500 individuals affected)
- Law enforcement may request delay

HITECH

“Discovered”

- A breach is discovered as of the first day on which such breach is
 - Known to the LHD or
 - By exercising reasonable diligence would have been known by the LHD

“Unsecured PHI”

- Technical guidance available from DHHS Office of Civil Rights
- Guidance focuses on encrypted data or destroyed media

HITECH

- What should LHDs do NOW?
 - Update BA agreements
 - Identify LHD's secured vs. unsecured information
 - Revise policies and procedures to reflect notification requirements
 - Train staff

HITECH

- What should LHD do if it discovers a possible breach?
 - Revisit the definition of breach
 - Violates HIPAA Privacy Regulation?
 - Risk of harm threshold?
 - If breach occurred:
 - Duty to mitigate
 - Notifications
 - Accounting of disclosures

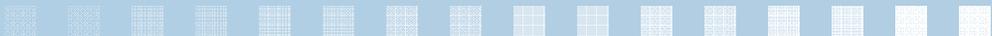
State ID Theft Law

- What is a security breach?
 1. Incident of unauthorized access to and acquisition of unencrypted and unredacted records or data
 2. Containing personal information
 3. Where illegal use of the personal information
 - Has occurred
 - Is reasonably likely to occur or
 - Creates a material risk of harm to a consumer

State ID Theft Law

- Notification required: If LHD discovers a security breach, must notify
 - The affected person
 - If > 1000, Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies
- Law enforcement may request delay

QUESTIONS?



Business Associates

- Originally, HIPAA Privacy and Security enforceable only against covered entities
- HITECH
 - May enforce directly against BAs
 - Provider may still pursue contract action
- Impact on LHD?
 - BAs may pay closer attention to contracts and information sharing

Enforcement

- CMPs: Civil monetary penalties collected will go to OCR to support enforcement
- States: Authorizes the Attorney General's Office to enforce HIPAA Privacy
- Impact on LHD: May see an increase in enforcement activity

Individual Rights

- Request restrictions
 - Providers **MUST** agree to request if
 - Request relates to disclosure to plan for TPO and
 - Provider has been paid in full out of pocket
- Accounting
 - If LHD maintains electronic health records, TPO disclosures must be included in accounting for 3 years rather than 6 years

Individual Rights

- Access
 - If LHD maintains electronic health records, must allow patients to have access to PHI in electronic format

QUESTIONS?

