Hickman & Lowder Co. L.P.A.
Attorneys at Law

Franklin J. Hickman
Janet L. Lowder
David A. Myers
Elena A. Lidrbauch
Sandra J. Buzney
Judith C. Saltzman
Mary B. McKee
Amanda M. Buzo
Lisa M. Garvin

Penton Building
1300 East Ninth Street
Suite 1020
Cleveland, OH 44114
Telephone (216) 861-0360
Fax (216) 861-3113

5062 Waterford Dr.
Sheffield Village, OH 44035
Telephone (440) 323-1111
Fax (440)323-4284

CHANGES IN HIPAA AND OHIO LAW

Slide text

Elena A. Lidrbauch
Franklin J. Hickman
December 3, 2009

Major Changes in Privacy Laws

- Ohio
- Federal

Vocabulary (refresher)

- HIPAA
- PHI
- Covered Entity
- TPO
- BA
- ARRA

Changes in Ohio Law: 5126.044

- Allows disclosure of identity of eligible individual for treatment and payment
- Eliminates accounting requirement

Changes in Federal Law

- Notification of Breach of unsecured PHI
- Increased BA obligations
- Minimum Necessary standard
- Accounting Requirements

Changes in Federal Law (cont'd)

- Increased Civil Penalties
- Expanded enforcement tools

SSAs: Use Releases

- Allows release of reports and other info under Ohio law
- Avoids need for accounting
- Minimum necessary compliance
- Maximize self-determination

What is a breach?

- Acquisition, Access, Use, Disclosure of PHI
- Unauthorized manner
- Compromises PHI security or privacy

Notice of Breach

- Covered entity must provide notice of breach
- Applicable to unsecured PHI only
- Secured v. Unsecured PHI

Secured PHI

- Defined in guidance issued by Secretary of HHS
  - Encryption
  - Destruction
- www.hhs.gov/ocr/privacy

When notice of breach is required

Secured	**No notice**
Unsecured - exception	**No notice**
Unsecured - no exception	**Notice**

Exception:

- Unintentional acquisition, access, use,
- By Covered Entity or BA
- Within scope of Authority
- No further use or disclosure

Exception:

- Inadvertent disclosure
- Between employees of CE/BA
- No further use or disclosure

Exception:

- Disclosure by CE/BA
- Good faith belief that recipient will not retain PHI

Who Gets Notice

- Individual
- Media if >500
- HHS
  - Promptly if >500
  - Annually if <500
- CE if BA breached

Timing of Notice

- Without unreasonable delay
- No later than 60 days after discovery of breach
- Delay if notice would:
  - Impede criminal investigation
  - Affect national security

Content of Notice

- What happened and when
- PHI involved in breach
- Steps to protect from potential harm
- Corrective steps by CE
- Contact information

Method of Notice

- Written
  - First class mail
  - E-mail with consent
- Substitute
  - <10 – written, phone, other
  - >=10 Web site 90 days or media with toll free number for 90 days

Method of Notice (cont'd)

- Urgent – imminent misuse of unsecured PHI
- CE may contact by phone or other means

BA Changes

- Security rules apply to BAs
- BAs have duty to notify CE about breaches
- BAs have affirmative duty to terminate agreement or report violations by CE under some circumstances

Minimum Necessary Req.

Use, disclosure or request of records must be limited to the minimum which is reasonably necessary to accomplish the purpose of the use, disclosure or request

Minimum Necessary Exceptions

- Treatment
- Requested by individual
- Authorization
- Investigations/legal process

Minimum Necessary Reqs

- Current compliance
  - Limited data set or
  - Minimum info necessary to accomplish purpose
- Future compliance
  - HHS to issue guidance
  - August 2010 deadline
  - Will replace current standard

Accountings

- Ohio law removes blanket requirement for all disclosures
- HIPAA: accounting required:
  - TPO stored electronically: 3 years
  - Other covered disclosures: 6 years
- BA agreement must define procedure for accountings

Implementation dates

- Electronic records for TPO
- Jan. 1, 2011
  - For disclosures of records in existence after 1/1/09
- Jan. 1, 2014
  - For disclosures of records in existence on or before 1/1/09

Accounting Recommendation

- Use authorizations to eliminate need for accounting
- Bring prior accounting requirement in line with HIPAA standards
- Consider continuing prior accounting procedures if in line with HIPAA

Civil Penalties

- Penalties apply equally to CE and BA
- Prior to revisions, penalty was $100 per violation up to $25,000 for identical violation per year

Penalties: Did not know

Each violation	**$100 - $50,000**
Max. per year for identical violations	**$1,500,000**

Penalties: Reasonable Cause

Each violation	**$1,000 - $50,000**
Max. per year for identical violations	**$1,500,000**

Penalties: Willful Neglect Corrected

Each violation	**$10,000 - $50,000**
Max. per year for identical violations	**$1,500,000**

Penalties: Willful Neglect Not Corrected

Each violation	**$50,000**
Max. per year for identical violations	**$1,500,000**