HIPAA UPDATE: Just When You Thought The Waters Were Safe

James F. Doherty, Jr.
Kathleen Pennington
Pecore & Doherty, LLC
Columbia, Maryland

HIPAA HITECH FINAL RULE

- Omnibus Final Rule became effective March 26, 2013
- Compliance is required by September 23, 2013
- New Business Associate Agreements after September 23, 2013, must comply with Final Rule
- Existing Business Associate Agreements are "grandfathered" through September 23, 2014

Business Associates

- Expanded definition of BA:
  - "Person who, on behalf of a covered entity, creates, receives, maintains or transmits PHI, including business subcontractor"
- BAs must comply with technical, administrative, and physical safeguard requirements under Privacy and Security Rules, can be directly liable for Security Rule violations, and liable for civil and criminal penalties

Business Associates II

- **What's New?**
  - Definition of BA now includes Health Information Organizations (HIOs), E-Prescribing Gateways and Personal Health Record Vendors (PHR)
- Excludes:
  - Providers who receive information for treatment purposes
  - Covered Entities with respect to function or activity of Organized Health Care Arrangement (OCHA)

Business Associates III

- Status as BA is fact specific, the existence of a BA agreement is not determinative
- "Mere conduits" or digital couriers are not included as BAs, but entities storing PHI, even without intent to view it, are included
- Cloud Models are implicated

Business Associates IV

- Subcontractors of a BA are now defined as BAs
- Includes all downstream contractors who access patient information on behalf of a provider
- Covered Entity does not need to have a direct BA with the subcontractor of a BA

Business Associates V

- BAA requirements:
  - Written agreement
  - Permitted and required uses and disclosures of PHI
  - Appropriate safeguards
  - No use or disclosure other than as authorized in BAA
  - Security rule compliance, safeguards
  - Subcontractor compliance

Business Associates VI

- Reports to Covered Entity
- Compliance with all rules Covered Entity is subject to for particular uses or disclosures
- Books and records available to HHS for inspection
- Termination:
  - Return or destroy PHI
  - If not feasible, BAA protections continue in effect

Business Associates VII

- **BAA Considerations**:
  - Is vendor a BA?
  - Use of OCR Standard Template or AMA's sample BA
    - http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
    - http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act.page
  - Use a single form unless acting as BA for another entity who has their own form
  - Preapproval of subcontractors?
  - Breaches: who receives notice, cooperation and mitigation, costs of notification, content of notification

Business Associates VIII

- Audit Rights
- Books & Records
- Indemnification?
- Equitable Relief (injunctions)?
- Insurance
- Reporting time frames
- State law that applies
- Representations and warranties
- Termination, cure period
- Amendment for changes in law
- Price renegotiation based on compliance cost?

Breach Notification

- Elimination of "harm" standard (substantial risk of financial, reputational or other harm")
- ***Rebuttable presumption*** that unauthorized disclosure is a reportable breach
- Risk analysis:
  - Nature and extent of PHI involved
  - Identity of person who made disclosure or received PHI
  - Whether PHI was actually acquired or viewed
  - Extent to which risk has been mitigated

Breach Notification II

- Exclusions from definition of Breach remain the same:
  - Within the Scope of Authority
  - Inadvertent disclosure
  - Recipient is unable to retain PHI

Patient Access

- If PHI is maintained electronically, patient may request electronic copy
- Must be offered in any format readily producible, otherwise in a readable format agreed to by the provider and the patient
- Provider may charge for cost of media (CD, USB, other portable media) and labor for responding to request

Patient Access II

- Provider must respond within 30 days, with one 30 day extension permitted
  - Prior provision allowing 60 days for PHI stored of-site has been removed
- No requirement to purchase new equipment or scan had copy records to electronic format
- Unencrypted email may be used if patient is notified of risks
- No continuing obligations once PHI is delivered to patient or designated third party

Patient Access III

- Right to restrict disclosures to health plans if patient pays out of pocket
- Previously restricted PHI may be submitted to support follow-up care.
- Right to request restrictions from downstream vendors
- Providers may not require patients to restrict "all or none" of their PHI
- Restricted PHI must be flagged in medical records

Notice of Privacy Practices

- New templates available through OCR and AMA
  - http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html
  - http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act.page
- Must now include:
  - Sale or marketing of PHI
  - Other purposes that require patient authorization
  - For providers engaging in fundraising, opt out statement
  - Health Plan restrictions
  - Right to receive breach notifications

Miscellaneous Provisions

- Individually identifiable health information no longer considered PHI 50 years after patient's death
- Genetic information is now defined as PHI
- Release of student immunization records:
  - If school is required by law to have proof
  - Written or documented verbal permission form parent

Best Practices

- Mandatory BA self-audits
- BA implementation strategy
- BA inventory
- Revise BA agreements
- Breach notification response plan
- Revise Notice of Privacy Practices
- Develop and implement training strategy
- Revise Policies and Procedures

Penalties

- **OCR Audit Protocol:** http://ocrnotifications.hhs.gov/hipaa.html
- **Covered Entity did not know** (and it would not have been reasonable for them to know):
  - $100 to $50,000 per violation; $1.5 Million maximum per standard violated per year.
- **Due to reasonable cause** (and not willful neglect):
  - $1,000 to $50,000 per violation; $1.5 Million maximum per standard violated per year.
- **Due to willful neglect (corrected within 30 days):**
  - $10,000 - $50,000 per violation; $1.5 Million maximum per standard violated per year. At least $50,000 if not corrected within 30 days

Recent Enforcement Actions

- Hospice of North Idaho: $50,000 settlement for theft of laptop affecting less than 500 individuals (Jan. 2013)
- Phoenix Cardiac Surgery: $100,000 settlement for clinical appointment calendar that was publicly accessible on internet (April 2012)
- Mass Eye & Ear: $1.5 million settlement for theft of laptop (Sept. 2012)
- Alaska Medicaid: $1.7 million settlement for theft of portable USB hard drive (June 2012)
- BCBST: $1.5 million settlement for theft of 56 unencrypted hard drives (March 2012)
- UCLA Health System: $865,000 settlement for employees' improper access of celebrity patients' EMRs (July 2011)
- Cignet Health: $4.3 million civil monetary penalty for failure to provide access to medical records and failure to cooperate with investigation (Feb. 2011)
- Mass. Gen. Hospital: $1 million settlement for failure to safeguard PHI containing SSNs and HIV/AIDS left on subway (Feb. 2011)