How the Stimulus Act has Rewritten HIPAA Regarding Data Breach Notification and Enforcement, Patients' Rights and Business Associates

Gerry Hinkley

gerryhinkley@dwt.com

Overview

- Individual's Right to Access to PHI
- Minimum Necessary
- Individually Requested Privacy Restrictions
- Extension of HIPAA to business associates (BAs)
- Federal breach notification and reporting rules applicable to covered entities (CEs)
- Accounting of disclosures
- Marketing
- No Sale of PHI
- New Enforcement Approaches and Penalties

Individual's Right to Access to PHI

- Existing law: Individual has a right to access/receive a copy of medical record (45 CFR 165.524)
- HITECH: If CE uses/maintains an EHR
  - Right to electronic copy of records
  - Right to direct CE to transmit electronic copy to another entity or person
  - Delivery options include media such as CD-ROM, USB drives, Websites
  - An element of "meaningful use" for Medicare/Medicaid incentives
  - Effective: February 18, 2010

Minimum Necessary

- Preference for Limited Data Sets and de-identified information
- Disclosure should be of the limited data set or, if not practical, the “minimum necessary” information to accomplish the purpose of the disclosure
- Minimum necessary is determined by the disclosing party
- Exclusions for disclosures for treatment and law enforcement retained
- Effective: 2/18/10; Regulations required by 8/18/10

Individually Requested Privacy Restrictions

- Existing Law: Individual has right to request privacy restrictions but binding on CE only if CE agrees
- HITECH: No disclosure to health plans for self-pay services
- Effective: 2/18/10

Business Associates

- Existing Law: BAs have not been directly regulated by HIPAA
  - Instead Covered Entities were required to enter into BA contracts with their BAs.
  - Way to backdoor some of the HIPAA requirements
- HITECH: BAs directly regulated effective 2/18/10 (except as noted)

Business Associates

- HITECH clarification of BA status
  - HIEs
  - RHIOs
  - e-Prescribing Gateway
  - PHR vendors that provide PHRs to CEs

Business Associates

- HITECH: BAs are required to:
  - Directly comply with administrative, physical and technical safeguards and documentation requirements under the HIPAA security rule — as if they were CEs
  - Not use or disclose PHI in a manner that is not in compliance with the privacy portions of their BA contracts
  - Notify CEs if they discover a data breach (Effective 9/23/09)

Business Associates

- Other HITECH privacy and security requirements that apply to CEs will be applicable to BAs and shall be incorporated into BA agreement
- Implications for existing BA agreements:
  - Amendment of existing agreements probably not required
  - Notice to BAs of new obligations a better practice
  - Make reference to new obligations in new BA agreements

Business Associates

- BAs now obligated to comply with BA requirements with respect to BA's subcontractors (question: are BA's subcontractors BAs for purposes of HITECH?)
- BAs now subject to civil and criminal enforcement and penalties under HIPAA
  - Criminal enforcement has always been a possibility
  - Civil enforcement and audits are new

Expanded Accounting of Disclosures

- Existing law: No TPO in accounting
- HITECH: if CE uses/maintains an EHR
  - Right to accounting of disclosures including TPO through EHR
  - 3-year period (as opposed to 7 in existing law)
  - Fees = labor costs
- Affected by rulemaking (within 6 months)
- Compliance Dates: 1/11/11; existing EHRs (as of 1/1/09) have until 1/1/14
- CEs should raise this issue with current/prospective EHR vendors
- Element of “meaningful use” for Medicare/Medicaid incentives

Notification in Case of Breach – The Rule

- First federal mandatory breach notification requirement imposed on HIPAA Covered Entities (CEs) and Business Associates (BAs) eff. 9/23/09
- The rule: Each CE that accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses unsecured PHI must notify each individual whose unsecured PHI has been, or is reasonably believed by the CE to have been, accessed, acquired or disclosed due to a breach (HITECH Section 13402(a), 42 USC §17932(a); 45 CFR Parts 160, 164 (pub. 8/24/09))
- Burden of proof compliance is on CE

Breach – What is it?

- "Breach" means unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of the PHI (*i.e.,* poses a significant risk of financial, reputational or other harm to the individual)
- "Access" means the ability to read, write, modify or communicate data or otherwise use any system resource

Breach – What is it? (2)

- "Breach" does not mean
  - By authorized persons:
    - Unintentional acquisition or use in good faith in the course and scope of employment to someone authorized to access PHI OR
    - Inadvertent disclosure by an authorized person to another authorized person within the same CE or BA
    - AND the information is not further acquired, accessed, used, disclosed
  - By CE or BA, if good faith belief that the disclosure was to an unauthorized person who would not be able to retain the PHI

Breach – "Unsecured PHI"

- Per guidance of HHS issued April17, 2009: PHI is secure if is rendered unusable, unreadable or indecipherable to unauthorized individuals by
  - Encrypted and process or key has not been breached: examples in National Institute of Standards and Technology (NIST) publication 800-111, Federal Information Processing Standards (FIPS) 140-2
  - Media is destroyed
  - Media is purged consistent with NIST publication 800-88

Breach – Limited Data Set + is Secure

- Per 8/24/09 Regulations: data consisting of the limited data set (45 CFR section 164.514(e)(2)), not including date of birth and zip code is not subject to breach notification because its disclosure does not compromise the security or privacy of PHI

Breach – Patient Notification

- "Without reasonable delay" – 60 days after discovery by a work force member or agent of the CE (or would have been discovered with reasonable diligence)
- Recordkeeping of notifications
- First class mail or email if requested (multiple mailings if required)
- Next of kin if subject is deceased
- Substitute if contact information out of date or insufficient (may be informal if less than 10 subjects)

Breach – Patient/Other Notification

- If imminent danger – telephone or other means in addition to required notice
- Plus, if more than 500 residents of a state or region are affected –
  - promptly disclose to prominent media outlets after discovery
  - at the same time notify Secretary of HHS
- Annual notice to Secretary if fewer than 500 subjects
- Notice can be delayed at request of law enforcement

Breach – Notification -- Contents

- What happened, date of discovery and date of breach
- Types of unsecured PHI involved (*e.g.,* whether full name, SS#, DOB, home address, account #, diagnosis, disability code)
- Steps affected individuals should take for protection
- Investigation, mitigation and protection measures by CE
- Contact information including toll-free number, e-mail address, website or postal address

Breach – Business Associates

- Business Associates (BAs) must provide CE with notice of breach, including
  - identification of each subject
  - any other available information that the CE is required to include in CE's notice

Breach - Implications for Policy Development

- Regulations are effective 9/23/09
- Sanctions will not be imposed with respect to any breach occurring before 2/23/10
- Important elements
  - Technology: measures to ensure all PHI is secure
  - Leadership and responsibility
  - Role of legal counsel for compliance, privilege protections
  - Reconciliation with state requirements
  - Training
    - Before
    - After
  - BA compliance
    - Amending BA agreements
    - Aligning processes and procedures
  - Complaint mechanism regarding polices and procedures, compliance

Breach – Policy Development

- Processes for discovering breaches
- Procedures and forms for reporting
- Mechanisms for determining
  - if unsecured PHI involved
  - individuals affected
  - applicable notification requirements
- Processes for
  - determining appropriate mitigation
  - developing advice to affected individuals
  - creating and distributing notices
  - determining and creating other forms of communication
  - accounting for notification
  - reporting to Secretary of HHS

Marketing

- Existing Law: exceptions to "marketing" (treatment, care coordination, part of plan of benefits, etc.)
- HITECH: Exceptions do not apply if CE receives direct or indirect payment for communication unless:
  - payment is for a communication regarding a drug currently prescribed for the recipient if the communication and such payment are "reasonable in amount"
  - the communication is made by the CE and the CE obtains a valid authorization in accordance with HIPAA section 164.508 from the recipient; or
  - the communication is made by a BA of a CE, on behalf of such CE, and such communication is consistent with the applicable BA agreement
- Effective: 2/18/10

No Sale of PHI

- Existing law: Except in the area of marketing, the HIPAA privacy rule does not prohibit a CE from being paid for PHI as long as the disclosure is otherwise permitted
- HITECH: Prohibits a CE or BA from directly or indirectly receiving remuneration in exchange for any PHI without a valid authorization from the individual that includes a specification of whether the protected health information may be sold by the entity receiving the PHI
- Effective: 2/18/10

No Sale of PHI

- Exceptions:
  - Public health activities
  - Research and the price reflects the costs of preparation and transmittal
  - Treatment of the individual, subject to any regulation
  - Sale, transfer, merger or consolidation
  - Payment to BA for its BA services
  - To provide an individual with a copy of his/her record
  - As otherwise determined by the Secretary by regulation issued before 8/2010

New Enforcement Approaches

- Civil penalties for unknowing, knowing and willfully neglectful violations of HIPAA
- Civil money penalties to be shared with enforcers and harmed individuals
- State Attorneys General may bring civil actions
- Clarifies/expands who is liable for criminal violations: apply to unauthorized individuals who obtain or disclose PHI maintained by a CE
- Effective: 2/17/09

New Penalties

- Tier A (if offender did not know, and by exercising reasonable diligence would not have known, that he or she violated the law): $100 for each violation, up to $25,000 for identical violations
- Tier B (if the violation was due to reasonable cause and not willful neglect): $1,000 for each violation, up to $100,000 for identical violations
- Tier C (if the violation was due to willful neglect but was corrected): $10,000 for each violation, up to $250,000 per year
- Tier D (if the violation was due to willful neglect and was not corrected): $50,000, up to $1,500,000 per year

Take Aways

- Create a compliance plan focusing on
  - Patient access to PHI
  - Minimum necessary
  - Business associates
  - Requests to limit disclosure of self-pay care
  - Breach notification
- Update and generate new policies and procedures
- Train affected personnel
- This is a good opportunity to do a HIPAA house-cleaning

- This is a publication of the Health Information Technology Group of Davis Wright Tremaine LLP with a purpose to inform and comment upon recent developments in health law. It is not intended, nor should it be used, as a substitute for specific legal advice, as legal counsel may only be given in response to inquiries regarding particular situations.

Thank you

- Questions?
  - Gerry Hinkley
  - Davis Wright Tremaine LLP
  - gerryhinkley@dwt.com