Fifth National HIPAA Summit West

Privacy and Security under the HITECH Act

W. Reece Hirsch
Partner,
Morgan Lewis

Paul T. Smith,
Partner,
Hooper, Lundy & Bookman, P.C.

Morgan Lewis

Hooper, Lundy & Bookman

Developments

- The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
- FTC final data breach reporting rule for PHR providers August 25, 2009
  - Effective September 24, 2009; compliance required by February 22, 2010
- HHS interim final data breach reporting rule for covered entities August 24, 2009
  - Effective September 23, 2009; compliance required by February 22, 2010
- Interim final enforcement rule October 30, 2009
  - Effective November 30, 2009
- Proposed HITECH rule for privacy, security & enforcement, July 14, 2010
  - Not yet final
- Proposed accounting rule, May 31, 2011
  - Not yet final

The HITECH Act

- Title XIII of the American Recovery and Reinvestment Act of 2009
- Enacted February 17, 2009
- Most provisions effective February 17, 2010

The HITECH Act

- Builds on Executive Order 1335, April, 2004—
  - Created position of National Coordinator for Health Information Technology
  - Adopted a federal HIT Strategic Plan, calling for widespread adoption of interoperable EHRs within 10 years

The HITECH Act

- Establishes position of National Coordinator for Health Information Technology to--
  - Update the goals of the federal HIT Strategic Plan, with the same target of 2014
  - Adopt programs for the testing & certification of health information technology
- Establishes a HIT Policy Committee to make policy recommendations relating to the implementation of the national Health IT Strategic Plan.

The HITECH Act

- Establishes a HIT Standards Committee to recommend standards, implementation specifications, and certification criteria for the electronic exchange of health information.

- Provides Medicare and Medicaid incentives for meaningful use of certified EHR technology by providers.
  - Initial set of standards, implementation specifications, and certification criteria for EHR technology issued July 28, 2010.
  - Final rule on Meaningful Use incentives issued July 28, 2010

The HITECH Act

- Strengthens HIPAA privacy and security standards
- Creates new data breach notification requirements

The HITECH Act - Enforcement

- Increases penalties for HIPAA violations (effective immediately)
- Penalties tiered, based on fault & whether corrected
- $100 per violation for innocent violations
- Up to $50,000 per violation for violations due to willful neglect that are not corrected

The HITECH Act - Enforcement

- Permits states' attorneys general to bring civil suits under HIPAA to recover penalties and attorneys' fees
- Clarifies that individuals who are not covered entities can be prosecuted criminally under HIPAA
- Beginning 2012, requires formal CMP investigations for violations involving willful neglect
- Requires HHS to conduct periodic HIPAA compliance audits

The HITECH Act - Enforcement

- Providence Health & Services (2008) - $100,000
- CVS Pharmacy (2009) - $2.25 million
- Rite Aid (2010) - $1 million
- Cignet (2011) - $4.3 million
- Massachusetts General Hospital (2011) - $1 million
- UCLA Health System (2011) - $865,000
- June 10, 2011 – HHS contracts with KPMG for 150 HIPAA audits through 2012

The HITECH Act – Business Associates

Effective February 17, 2010—

- BAs must comply with the HIPAA Security Rule safeguards and documentation requirements
- BAs must comply with the required terms of the BA agreement
- BAs subject to the additional privacy and security provisions of the HITECH Act that apply to CEs

The HITECH Act – Special Restrictions

- HITECH Act allows patient to restrict disclosure of PHI to health plan for payment or operations if patient pays out of pocket in full (2/17/2010)
  - Proposed regulations would implement this, and request comments on notification of downstream providers, such as pharmacies

The HITECH Act – Minimum Necessary

- Restricts use and disclosure to "limited data set" – or to the minimum necessary "if needed" (2/17/2010)
  - Statutory provision to be replaced by guidance to be issued by HHS within 18 months of enactment of HITECH
  - CE or BA making disclosure to determine minimum necessary
- In the proposed rule:
  - HHS interprets this as requiring CEs to consider use of limited data set
  - HHS does not address who decides
  - HHS does not issue guidance, but requests comments on what aspects of the rule it should address

Accounting under the Privacy Rule

- Individuals have right to accounting of disclosures of PHI
- Does not apply to disclosures for treatment, payment and health care operations (TPO)

What's Left?

- Required by law
- Public health activities
- Victims of abuse & neglect
- Health oversight activities
- Legal proceedings
- Law enforcement
- Decedents
- Organ procurement
- Research
- Threat to public safety
- Military & veterans' activities
- Workers' compensation

- Disclosures in violation of the Privacy Rule

Accounting under the HITECH Act

- Removed the TPO exception for disclosures made through an electronic health record, but limited look-back to three years
- Required HIT Policy Committee to make recommendations on standards for technologies as part of a qualified electronic health record to allow for accounting of disclosures for TPO
- Following adoption of these standards, required HHS to publish regulations "on what information shall be collected about each disclosure"
- Regulations to take into account--
  - The interests of individuals in learning the circumstances under which their health information is being disclosed
  - The administrative burden of accounting for such disclosures

Certification Standards

- Optional certification standard issued July 28, 2010, 75 Fed. Reg. 44590

Record treatment, payment, and health care operations disclosures. The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations

HIPAA Security Rule

Technical Safeguards (§ 164.312(b)):

Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Administrative Safeguards (§ 164.308(a)(1)(ii)(D)):

Implementation specification: Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. 45 CFR 164.308(a)(1)(ii)(D).

No requirement regarding content or retention period

Proposed Regulations

- Issued May 31, 2011
- Comment period expired August 1, 2011
- Would—
  - Modify the existing rule for written accounting
  - Add a more comprehensive “access report” for electronic data
- Would go into effect:
  - For written accounting, 240 days after publication of final rule
  - For access report:
    - EHR acquired on or before January 1, 2009:
      - January 1, 2014 (no extension)
    - EHR acquired after January 1, 2009:
      - January 1, 2013 (2-year extension)

Proposed Regulations

- Access Report
  - Would have to indicate who has *accessed* PHI in an *electronic designated record set* held by the CE or a BA within three years prior to the request
    - No option to provide list of business associates
    - Would affect only business associates holding designated record set
  - Would not be limited to electronic health record
  - Would include internal access (i.e., use) as well as disclosure
  - Would have to include
    - Date and time of access
    - Name of natural person, if available, otherwise entity having access
    - Description of information accessed, if available
    - Description of action if available, e.g., create, modify, access or delete
  - Would not have to include the purpose

Proposed Regulations

Gives this example of an access report:

Date	Time	Name	Action
10/10/2011	02:30 p.m.	John, Andrew	Viewed

The HITECH Act – Sale of PHI

- HITECH Act will restrict sale of PHI without authorization
- Effective 6 months after final regulations
- Requires regulations to be issued within 18 months of enactment
- HITECH Act includes exceptions:
  - Public health
  - Costs of preparation and transmittal of data for research
  - Treatment
  - Sale of the entity
  - Payment to BAs
  - Payment by individual for copy of record

The HITECH Act – Sale of PHI

- Proposed regulation would add exceptions:
  - Disclosures for payment
  - Disclosures required by law
  - Reasonable cost-based fee for preparation and transmittal of information for any permitted purpose

The HITECH Act – Electronic Copy

HITECH Act—

- Permits patient to obtain electronic copy of PHI in an EHR, and to direct the CE to transmit electronic copy to a third party (2/17/2010)
- Fee not to exceed CE's labor costs

Proposed regulation would--

- Extend the right to any electronic PHI, whether or not in an EHR
- Require CE to provide copy in format requested by patient, if readily reproducible in that format; otherwise, in an agreed format
- Allow CE to charge for electronic media
- Permit patient to direct CE to transmit paper PHI to third party
  - But request must be written and signed

The HITECH Act – Marketing

- HIPAA restricts marketing without authorization
- Under HIPAA, the following are not marketing:
  - Communications about treatment
  - Communications about the CE's products and services
  - Communications about care coordination
- HITECH Act makes these "marketing" if the CE receives remuneration for them, except--
  - Reasonable remuneration for communications concerning drugs and biologicals currently being prescribed
  - Payment to BAs for communications on behalf of CEs

The HITECH Act – Marketing

- Proposed regulation would—
  - Permit a CE to continue to receive remuneration from third parties for treatment-related communications concerning the CE's own products and services
    - Restricted to communications tailored to an individual's health care needs
      - Population-based communications would be health care operations, and would require authorization
    - Must be disclosed in NPP, and patient given opportunity to opt out
  - Require remuneration for communications relating to drugs and biologicals to be reasonably related to the CE's cost of making the communication
  - Define remuneration as direct or indirect payment from a third party whose products and services are being marketed

The HITECH Act – Fundraising

- HIPPA requires fundraising communications to contain an opt-out, and requires CEs to make reasonable efforts not to send fundraising communications to individuals who have opted out
- HITECH says that an opt out is treated as a revocation of authorization
- The proposed rule--
  - Would require CEs to include the opt-out right in their NPPs
  - Would prohibit sending fundraising communications to individuals who have opted out
  - Would prohibit onerous opt-out mechanisms
  - Requested comments on—
    - Scope of opt-out
    - Using more targeted data for fundraising, e.g., department

The HITECH Act – Decedents

Proposed rule would—

- Allow disclosure to friends and family
- End privacy protections after 50 years

The HITECH Act – Research

- HIPAA prohibits combining conditioned authorizations with unconditioned ones
- Proposed rule—
  - Would allow conditioned authorizations (e.g., clinical trials) to be combined with unconditioned authorizations for the same research (e.g., tissue banking), as long as they are clearly differentiated
  - Invites comments on whether to relax the rule that authorizations be research-specific

The HITECH Act – Immunizations

- HIPAA requires an authorization for a CE to provide immunization information to a school
- Proposed rule would allow this, if—
  - The state requires the school to obtain immunization information to admit the student
  - The parent, guardian or person in loco parentis consents
    - Informal, oral consent would suffice

The HITECH Act – Notice of Privacy Practices

- Proposed rule would require NPP to describe—
  - Individual's right to restrict disclosure of PHI where patient pays in full
  - CEs ability to send subsidized treatment communications
    - with opt-out right
  - Individual's right to opt out of fundraising communications
    - Presently just required in the communication itself
  - Need for authorization for sale of PHI and use of PHI for marketing

The HITECH Act – Breach Reporting

- Requires HIPAA covered entities and personal health record providers to report breaches of “unsecured protected health information”
- FTC published final rule for PHR providers August 25, 2009
- HHS published interim final rule for covered entities August 24, 2009
  - Enforcement began February 22, 2010

State Security Breach Notification Laws

HIPAA pre-emption rule applies

- State laws survive unless it is impossible to comply with both, or the state law stands as an obstacle to the federal law

The HITECH Act – Breach Reporting

Unsecured protected health information is protected health information that has not been encrypted or destroyed

- Initial guidance issued April 17, 2009; updated in interim final regs
- NIST encryption standards for electronic data in use
- Shredding or destruction of hard-copy media
- NIST standards for purging or destruction of electronic media

The HITECH Act – Breach Reporting

Conditions for reporting

- Breach must not be permitted by the Privacy Rule
- Breach must pose significant risk of harm
  - To whom disclosed
  - Possibility of mitigation
  - Type and amount of information disclosed
- Risk analysis must be documented if no disclosure made

The HITECH Act – Breach Reporting

Exceptions to reporting:

- Good faith unintentional access by authorized person
- Inadvertent disclosure by one authorized person to another
- Unauthorized disclosure to a person who cannot reasonably retain it

The HITECH Act – Breach Reporting

Report must be given to—

- The individual
- Prominent media outlets if ≥500 residents of the state are affected
- HHS concurrently if ≥500 individuals are affected; otherwise annual log

The HITECH Act – Breach Reporting

Notice must describe:

- What happened (including date of breach and date of discovery)
- Types of information involved
- Mitigation efforts
- Contact information

The HITECH Act – Breach Reporting

- Notice must be given without unreasonable delay, and no later than 60 days following discovery (i.e., when breach is known or should have been known with reasonable diligence)
- Notice must be delayed at request of law enforcement official for the period requested (but the request must be written for a delay of more than 30 days)

The HITECH Act – Breach Reporting

Notice must be given by first-class mail, except:

- Email notice is permitted if the individual has agreed to electronic notice
- Substitute notice if the CE does not have contact information
  - If < 10 individuals, by written notice, telephone or other means
  - If ≥ 10 individuals, by—
    - Conspicuous posting on web site home page for 90 days, or
    - Conspicuous posting in major print or broadcast media

  with toll-free telephone number

The HITECH Act – Breach Reporting

Business associates—

- Required to notify CE without unreasonable delay and in any event within 60 days
- Required to provide information that the CE must include in notification (but should not delay initial notification while they collect this information)

Covered entities deemed to discover breach—

- If the BA is an agent, when the BA discovers it (or is deemed to discover it)
- If the BA is an independent contractor, when the BA notifies the CE

Questions?

Speaker Contact Information:

- Reece Hirsch : rhirsch@morganlewis.com, 415-442-1422
- Paul Smith: psmith@health-law.com, 415-875-8488