Patient Privacy and Security: Data Breach Reporting and other HIPAA Changes

Paul T. Smith, Partner, Davis Wright Tremaine
James B. Wieland, Shareholder, Ober | Kaler

OBER | KALER
Attorneys at Law

Davis Wright Tremaine LLP

Developments

- The Health Information Technology for Economic and Clinical Health (HITECH) Act
- State Data Security Breach Notification Laws

The HITECH Act

- Title XIII of the American Recovery and Reinvestment Act of 2009
- Enacted February 17, 2009
- Most provisions effective February 17, 2010
- Others depend on issuance of Regulations or Guidance

The HITECH Act

- **Promotion of HIT, with a view to universal EMRs by 2014**
  - Standards and certification criteria
  - Testing
  - Financial incentives for adoption
- **Health information privacy and security**
  - Strengthens HIPAA
  - 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 – 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

  http://www.dwt.com/LearningCenter/Advisories?find=126206
- HHS published interim final rule for covered entities August 24, 2009

  http://www.dwt.com/LearningCenter/Advisories?find=130345
  - Effective September 23, with 60-day comment period
  - HHS will delay enforcement 180 days

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 be violation of 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 (including for 2009)

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

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
- Note, New HITECH provision allows enforcement by State Attorneys General. See Connecticut A.G.'s action against HealthNet

State Security Breach Notification Laws

- Many Covered Entities' PHI includes SSNs or other information that implicates State Breach laws. California Breach Notification law specifically includes medical information.
- A harbinger of things to come: The Massachusetts Standards for the Protection of Personal Information (201 CMR 17:00, effective 03/01/10)

The HITECH Act – Breach Reporting

- Begin logging data breaches
- Assign compliance responsibility
- Prepare policies and procedures
  - Detection and investigation of breaches
  - Determining whether reportable
    - HIPAA analysis
    - Exceptions
    - Risk assessment
  - Coordinating with state reporting requirements
- Develop form of notice
- Train workforce
- Communicate with business associates
- Check security, especially portable media

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 – Business Associates

Must BAAs be amended?

"The additional requirements of this title that relate to [privacy][security] and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity."

HITECH Act § 13401(a), 13404(a)

The HITECH Act – Privacy Provisions

- Will allow patient to restrict disclosure of PHI to health plan if patient pays out of pocket in full (2/17/2010)
- Will restrict use and disclosure to "limited data set" – or to the minimum necessary when minimum necessary rule applies (2/17/2010)
  - Statutory provision to be replaced by guidance to be issued by HHS within 18 months
  - CE to determine minimum necessary disclosure
- Will require accounting of routine disclosures from qualified EHRs (requires regulations; earliest effective date 1/1/2011)

The HITECH Act – Privacy Provisions

- Will restrict sale of PHI (requires regulations to be issued within 18 months)
- Will permit patient to obtain copy of EHRs in electronic format (2/17/2010)
- Will prohibit remunerated marketing (2/17/2010)
- Will require opt-out for fundraising (2/17/2010)

Questions?

Speaker Contact Information:

- Paul Smith: paulsmith@dwt.com, 415.276.6532
- James Wieland: jbwieland@ober.com, 410.299.4418