HITECH Panel: Breach Notification and Other HITECH Updates
Jennifer Landrum Elliott, Esq.
Federal Regulatory Regime for Health Care Businesses

- EFFECTIVE February 17, 2009

HITECH Act significantly revised the HIPAA Privacy and Security Rules applicable to Health Care Providers, Health Plans, and Health Insurers.

3 Most Significant Changes:

1. Breach Notification Rule
2. Increase in Enforcement
3. Extends HIPAA obligations to Business Associates
I. HITECH’s Impact on HIPAA: Breach Notification Rule

- **Incident must be a HIPAA Violation**
  - Unauthorized use, access, disclosure of PHI

- **PHI involved must be “unsecured”**
  - Information that is either *not encrypted* or *not destroyed*.
    - All PHI in paper form is “unsecured.”
    - All unencrypted ePHI is “unsecured.”

- **“Pose a significant risk of financial, reputational, or other harm to the individual”**
  - Must perform a “facts and circumstances” risk assessment for each breach

- **Not subject to an exception for inadvertent, harmless mistakes**
  - Unintentional access by an employee made in good faith, within scope of authority, and no further impermissible use or disclosure
  - Inadvertent disclosure between persons authorized to access PHI, so long as no further impermissible use or disclosure
  - Disclosure to an unauthorized person, if good faith belief that the person would not be able to retain the information
Breach Notification Rule:
Risk Assessment

- **Does breach pose a significant risk of financial, reputational, or other harm to the individual?**

**Factors to consider:**

- Who impermissibly used/received the PHI?
  - Was it another covered entity or federal agency (less risk), or someone without separate privacy obligations?

- Can you take immediate steps to mitigate (e.g., obtain recipient’s assurances that the info will not be further disclosed or will be destroyed)?

- Was information returned without being opened or accessed (forensic analysis would be required on laptops, etc.)
Notification Risk Assessment: What type of information was involved?

- **Greater Risk of Harm:**
  - Name of individual, along with sensitive service types or provider types:
    - Oncology services
    - Substance abuse treatment
    - AIDS treatment
    - Abortion clinic
    - Plastic surgery
  - Name of individual, along with information that increases risk of identity theft:
    - SSN
    - Credit card info
    - Mother’s maiden name

- **Lesser Risk of Harm:**
  - Name of individual and fact that he/she received services from a particular hospital as long as service type was not disclosed or sensitive and no financial info.

**OCR Cautions:**

“[K]eep in mind that many forms of health information, not just information about sexually transmitted diseases or mental health, should be considered sensitive . . . especially in light of fears about employment discrimination.”
HITECH’s Impact on HIPAA: Breach Notification Rule

- Notification must be made “without unreasonable delay” but no later than **60 calendar days** after discovery

- **Notification to some or all of the following:**
  1. Individual whose PHI was subject of breach
     - when, what, efforts to investigate, steps to mitigate, contact for additional information
     - Company’s website if outdated contact info for **10+ individuals**
     - *immediately* if **500+** individuals;
     - Log and report *annually* for < 500 people
  3. Prominent Media Outlets
     - if breach involves **500** individuals who are residents of one state or jurisdiction
Breach Reports to HHS

- To date, **157 breaches affecting 500+ individuals** have been reported, resulting in over **4,854,200 notifications to individuals**.
  - *Mostly ePHI* that was contained in *lost or stolen unencrypted media* or portable devices

- OCR has also received over **6,000 reports** of smaller breaches (from September 2009 through April 2010)
  - *Mostly paper records* sent to wrong fax number, wrong address, wrong individual

Considerations for Determining Response

- Legitimate argument that information did not pose a “significant risk of reputational, financial, or other harm to the individual?
  What are results of risk assessment?
  - Consider using independent advisors to help with assessment
  - Independent advisors may have different reaction to level of risk and may help protect your business from claims that internal assessment was self-serving

- Any defensible way to narrow the scope of the number of individuals receiving notice (particularly if it is possible to reduce the number below 500)?
  - Is a subset of individuals more likely to be at risk of identity theft or reputational harm?

- Should your “offer” of protection and suggestions to individuals vary based on category of risk?
  - e.g., targeted risk of identity theft?
II. HITECH’s Impact on HIPAA: Increase in Enforcement

- **Civil monetary penalties**
  range from $100 to $50,000 per violation, with annual caps ranging from $25,000 to $1,500,000 for violations of the same requirement.

- **Criminal penalties**
  vary from $50,000 and/or 1 year imprisonment to $250,000 and/or 10 years.
HITECH’s Impact on HIPAA: Increase in Enforcement

- **HHS** to conduct mandatory “**periodic audits**” to ensure compliance with the new provisions
  - Approximately $10 Billion has been appropriated to fund audits
  - Expect an audit if you have reported a breach involving > 500 individuals

- **State Attorneys General** - action in U.S. District Court on behalf of residents of the state who have been threatened or adversely affected by a HIPAA violation
  - May collect fines/penalties as damages, as well as costs and attorneys fees

- “**Whistleblowers**” coming soon – GAO to make recommendations to HHS on apportioning CMPs to those harmed by violations
  - HHS must adopt methodology by February 2012
  - Increases incentives for individuals to file complaints

- New “**Breach Notification**” rules establish affirmative reporting duties and make penalties easier to assess
Attorney General and OCR Enforcement

- **January 13, 2010**
  Connecticut AG filed suit against Health Net, which lost a portable external hard drive containing 7 years of data for 446,000 CT residents. Plan waited 5 months to notify individuals.

  - Demanded identity theft insurance, reimbursement for credit freezes, and credit monitoring for 2 years
  - Sought CMP of $5,000 per violation, court costs and attorney fees
  - On July 6, 2010, Health Net agreed to pay $250,000 to resolve alleged violations. Amount would increase to $500,000 if later determined that data was misused and 250 or more individuals file claims of identity theft.
July 2010
Rite Aid agrees to pay OCR $1 million to settle complaint involving improper disposal of prescriptions and pill bottles.

– Rite Aid also agreed to a 3 year corrective action plan
– Rite Aid also signed a consent order with the FTC which will be in place for 20 years. Order requires external, independent assessments of its stores’ compliance.
Other Litigation

- Minnesota. BCBS Plan Accidentally Prints a Member’s Unredacted Claims Processing Form in Member Handbooks sent to 95,000 members.
  - SSN was not included.
  - Plan discovered error and notified member.
  - Discontinued use of the booklet, changed member’s ID number, and offered credit monitoring.
  - Member filed lawsuit against plan in April 2010.

- Class action lawsuits pending in a number of jurisdictions based on privacy/security breaches.
III. HITECH’s Impact on HIPAA: Extension of HIPAA to Business Associates

- Prior to HITECH’s enactment, Business Associates (i.e., many vendors and independent contractors of health providers and health plans) were not directly liable for violations of the HIPAA Privacy and Security Rules.

- HITECH has extended the obligation to comply with the HIPAA Security Rule and much of the HIPAA Privacy Rule directly to Business Associates.
  - Should help Covered Entities with their own compliance and enforcement plans because Business Associates are now also “on the hook.”
  - Do you know whether your Business Associates are aware of its obligations and whether they have implemented effective policies and procedures?
Thank You

Jennifer Landrum Elliott, Esq.
Member

Stites & Harbison, PLLC
1800 West Market St.
Suite 1800
Louisville, KY 40202

Office: 502.681.0682
Fax: 502.779.8333
Cell: 502.552.4873
Email: jlelliott@stites.com

For More Information: www.stites.com