MSPAlliance

MSPWORLD™

The HITECH Act and Its Impact on MSPs

Julie Machal-Fulks

September 13-15, 2011 • Austin Convention Center, Austin Texas

HIPAA / HITECH Overview

Health Insurance Portability and Accountability Act (HIPAA)

- Privacy and Security Rules define requirements for the appropriate use and safeguarding of protected health information (PHI)

Health Information Technology for Economic and Clinical Health (HITECH) Act

- Enacted as part of ARRA in February 2009
- Intended to strengthen the privacy and security of health information
- Applies Privacy and Security Rules to Business Associates
  - Includes breach notification requirements

HITECH Overview

Protected Health Information (PHI)

- Health information that relates to the past, present, or future physical or mental health, healthcare, or payment information which can or does identify the individual
- Transmitted or maintained in electronic media.

Breach Notification Requirement

- Covered Entities and Business Associates are required to report breaches of unsecured PHI

Business Associates

- Entities that either perform a function or provide a service involving the use of PHI

Are MSPs Business Associates?

The answer depends on the services provided to the Covered Entity.

- Service examples: consulting, data aggregation, management, administration, financial
- Activity examples: data analysis, processing or administration, and practice management

Covered Entities generally wish to treat most service providers as Business Associates

- If your client insists you sign a Business Associates agreement, you may be contractually obligated to comply with the HITECH breach notification requirements.

Definition of a Breach

Breach

- An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

Exceptions

- Unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or business associate
- Inadvertent disclosure of PHI from a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate

Safe Harbor - Encryption

Encryption

- an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key where
  - Note: if the key is also leaked, the information is no longer considered encrypted.

Technical Specifications

- Encryption methods published by the National Institute of Standards and Technology (NIST) have been adopted by HHS
- Data at Rest – data residing in a database or file system
  - Refer to NIST Special Publication 800-111
- Data in Motion - data moving through a network, including wireless transmission
  - Refer to NIST Special Publication 800-52, 800-77, or other FIPS 140-2 validated means.

Safe Harbor - Harm Threshold

- Breach notification is required only where a breach compromises the security or privacy of PHI and that compromise poses a "significant risk of financial, reputational, or other harm to the individual."

- "Risk of Harm" factors:
  - nature of the data elements breached;
  - likelihood the information is accessible and usable;
  - likelihood that the breach may lead to harm; and,
  - ability of the entity to mitigate the risk of harm.

- The current Interim Final Rule includes this harm threshold, though there is debate as to whether it should be included in the final rule.

Notification Requirement Overview

In the event of a breach of unsecured PSI, notice must be given "without unreasonable notice and in no case later than 60 days" after discovery.

- Date of discovery is the first day the entity knew or should have known of the breach.

<u>Elements of Notice</u>

1. Brief description of breach
2. Description of the type of PHI disclosed
3. Description of the steps affected individuals should take to protect themselves
4. Descriptions of the process the entity is using to investigate and mitigate
5. Entity contact information

Breach Event – Rec'd Procedure

In the event of any suspected breach, the following procedure is recommended:

1. Consult with the internal compliance management, senior technical staff, and outside legal counsel to evaluate the suspected breach.
2. If necessary, notify the Covered Entity of the breach and document the evaluation and notification process/
3. Work with the Covered Entity to further evaluate the breach:
   - Technical – determine whether there has been an impermissible use or disclosure of PHI
   - Risk of Harm – determine and document whether the impermissible use or disclosure of PHI compromises the security or privacy of the PHI
   - Exception – determine if the impermissible use or disclosure of PHI falls under one of the statutory exceptions

Notification to the Covered Entity must occur without unreasonable delay, but in any case within 60 days.

Parties to be Notified

Individuals

- Covered entities must notify affected individuals following the discovery of a breach of unsecured PHI via first-class mail or where individuals have previously consented, e-mail.

Secretary of HHS

- Over 500 individuals – within 60 days and without unreasonable delay.
- Under 500 individuals – annually

Media

- For breaches affecting over 500 individuals in a particular state or jurisdiction
- Required to provide notice to prominent media outlets serving the state or jurisdiction
- Generally in the form of a press release

Penalties for Non-Compliance

Tiered penalty structure for violations

Lowest tier: did not know and would not have known

- $100 per violation, up to $50,000 per year

Second tier: "reasonable cause" and not willful neglect

- $1,000 per violation; up to $100,000 per year

Third tier: "willful neglect" but corrected within a reasonable time

- $10,000 per violation; up to $250,000 per year

Fourth tier: "willful neglect" and not corrected within a reasonable time

- $50,000 per violation; up to $1.5M per year

Can also be subject to 10 years imprisonment

Effective and Compliance Dates

HHS published the Breach Notification Interim Final Rule in August of 2009

- Interim Final Rule is effective as of February 2010
- Expected Final Rule in March of 2011
  - Still waiting

Compliance

- HHS recognized a 6 month grace period is necessary for Covered Entities and Business Associates to adjust to the Final Rule once it becomes effective.

Additional HITECH Items

Accounting of Disclosures

- Technically requires Covered Entities to provide to a requesting individual an accounting of disclosures made in the course of providing treatment by either:
  1. Include disclosures made by Business Associates in their own accounting; or,
  2. Provide contact information of Business Associates to the requesting individual.
- In practice, some Business Associates will be required under the Business Associate Agreement to make such information available to the Covered Entity

Additional HITECH Items

Compliance Audit Program

- Currently being tested by the Office for Civil Rights (OCR)
- The final version will include a set of protocols on how audits will be conducted
- OCR is evaluating whether Business Associates will also be audited under this program
- Expect version of the Audit Program rules to be published late 2011, early 2012

Contact Information

Julie Machal-Fulks, Esq.
Partner
Scott & Scott, LLP.
1256 Main Street
Suite 200
Southlake, TX 76092

Phone: (800) 596-6176
Fax: (800) 529-3292

E-Mail: jfulks@scottandscottllp.com

Please Rate this Session

"What Every MSP Should Know about the HIPPA HITECH Act"

1) Please TEXT one of the following codes to 22333 (22333 acts as the phone number)

Excellent = 477583
Good = 477584
Fair = 477585
Poor = 477586

Or, use your web browser at http://pollev.com and text in the six digit code

Or, tweet @poll and the six digit code

(Standard text messaging rates may apply depending upon your plan. Your phone number will stay private and will not be spammed).

2) Have Comments? Text HIPPA and your message to 22333.

Example: "HIPPA This session was informative and I especially liked the specific examples given."