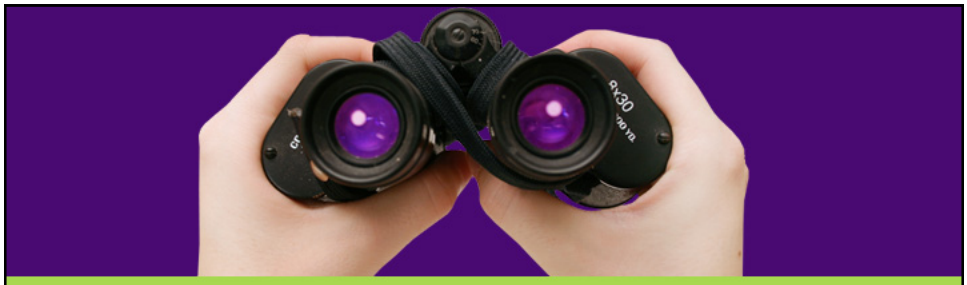

HITECH: What You Need to Know About the Security Breach Notification Regulations

Presenters:
Lisa Acevedo
Leeann Habte
Peter McLaughlin
Aaron Tantleff

FOLEY
FOLEY & LARDNER LLP

Tuesday, August 25, 2009

1:00 p.m. – 2:00 p.m. CT

Today's Presenters

Lisa Acevedo

Leeann Habte

Peter McLaughlin

Aaron Tantleff

Housekeeping

- We will take questions throughout the program via the Q & A tab located on your menu bar at the top of your screen and live questions at the end of the program
- Foley will apply for CLE credit after the Web conference. If you did not supply your CLE information upon registration, please e-mail it to mlopez@foley.com
- Materials and a recording of today's program will be available on our Web site
- For audio assistance please press *0
- For full screen mode, go to "View" on your toolbar and select "Full Screen" or press F5 on your keyboard

HITECH Act

- Background
  - Security breach notification requirements outlined in the Act
  - April 17, 2009: HHS issued "Guidance Specifying the Technologies that Render PHI Unusable, Unreadable, or Undecipherable to Unauthorized Individuals"

Breach Notification for Unsecured Protected Health Information

- August 19, 2009 – HHS issues interim final rule with request for comments
  - 60 day comment period
  - Impact

New Regulations

- Clarify and provide interpretive guidance on:
  - Reportable breaches
  - Exceptions that may apply to relieve covered entities and business associates from providing notification of otherwise reportable breaches

Security Breach Notification Regulations

- Attempt to provide clarification
  - e.g., Definitions triggering obligation to notify
  - "Harm" factor
- Attempt to provide interpretive guidance
  - e.g., Notification: when, how and to whom

HIPAA Security Rule Requirements

- ePHI and "unsecured PHI"
- Required vs. Addressable
- Compensating controls

HHS Technology Guidance

- Guidance vs. Requirement
- Relation to Security Rule
- Safe Harbor effect

NIST Standards

- What is NIST?
- Data at rest
- Data in motion
- Data destruction

Practical Considerations

- Benefit of clearly defined standard
- Challenge for smaller Covered Entities (CEs) and Business Associates (BAs)
- Risk assessment and compensating controls
- Relation to state data breach laws

Unsecured PHI

- Notification obligations under the Regulations only apply to breaches involving "Unsecured PHI"
- The HITECH Act defines "Unsecured PHI" as PHI that is not secured through the use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals
  - On April 27, 2009, HHS published guidance to further define methods to create "secure" PHI not subject to the notification requirements

Unsecured PHI (cont'd)

- The Guidance specified encryption and destruction as the technologies and methods for securing PHI
  - Encryption must be an algorithmic process with a confidential process or encryption key
  - Hard copies of PHI must shredded or destroyed and electronic media copies of PHI must be cleared, purged, or destroyed
  - Use of National Institute of Standards and Technology (NIST) standards for valid encryption processes for data at rest, data in motion, and for media sanitization

Unsecured PHI: Clarifications

- When PHI is secured by means of encryption, the encryption key must be kept on a separate device from the encrypted data to ensure that the key is not itself breached
- Redaction does not satisfy the requirements for destruction
  - Redaction is an acceptable method for de-identification of PHI
- Refer to NIST guidance on the development of security guidelines for enterprise-level storage devices, such as RAID (redundant array of inexpensive disks), or SAN (storage-attached network) systems

What is a Breach?

- Unauthorized acquisition, access, use, or disclosure means that the acquisition, access, use, or disclosure
  - is ***impermissible*** under the HIPAA Privacy Rule.
- Harm threshold
  - Unauthorized activity is considered to "compromise the privacy or security of PHI" if it ***poses a significant risk for financial, reputational, or other harm to the individual***

Risk Assessment

- Factors to Determine Risk of Harm to Individual
  - Who impermissibly used or to whom the information was impermissibly disclosed
  - Whether immediate steps to mitigate the harm render the risk to the individual to be less than "significant"
  - Whether impermissibly disclosed PHI was returned prior to it being accessed for an improper purpose
  - The type and amount of PHI involved in the impermissible use or disclosure

Limited Data Sets

- Limited data sets (except those that have been stripped of zip code and date of birth) are subject to the breach reporting requirements
  - Risk assessment requires evaluation of risk of re-identification of the PHI, given the geographic area and related factors.
  - CEs and BAs are not responsible for the breaches of limited data set recipients unless that recipient received the limited data set in the role as an agent for the CE or BA.

What is Not a Reportable Breach?

- Violations of the HIPAA Security Rule and certain violations of the HIPAA Privacy Rule
- Use or disclosure of de-identified information
- Impermissible use or disclosure of PHI that is *incident to* an otherwise permissible use or disclosure, and
  - Occurs despite reasonable safeguards and proper minimum necessary procedures.

Exceptions

- *Unintentional* acquisition, access, or use of PHI by an workforce member or individual acting under the authority of a CE or BA
  - If such unintentional activity was done in good faith, within the course and scope of employment or other professional relationship, and
  - Does not result in further use or disclosure that not permitted by the Privacy Rule.

Exceptions (cont'd)

- *Inadvertent* disclosure of PHI from one person with authority to access PHI at a CE or a BA to another person who also has authority to access PHI
  - If such inadvertent recipient is part of the same CE, BA or Organized Health Care Arrangement as the individual who made the inadvertent disclosure, and
    - HITECH Act required that recipient be within the same "facility" as the disclosing individual
  - Provided the recipient does not further disclose the information in violation of the Privacy Rule.

Exceptions (cont'd)

- *Unauthorized* disclosures in which the person to whom PHI is disclosed would not reasonably have been able to retain the information
  - Based on "good faith" belief by disclosing individual

Whether to Notify

- Determine whether there has been an ***impermissible acquisition, access, use or disclosure*** of PHI in violation of the Privacy Rule.
- Conduct a risk assessment to determine whether the impermissible activity ***compromised the security or privacy*** of the PHI.
  - *Harm threshold*
- ***Document the results*** of that risk assessment.
- *Evaluate whether the incident* ***falls under one of the exceptions*** to the notification obligations.

Effective / Compliance Date

- Breaches discovered on or after 30 calendar days from publication of interim final rule
  - Securing PHI not required
  - Some are securing PHI to avoid having to provide notice
  - Will use "enforcement discretion" and are not planning to impose penalties for first 180 calendar days to allow entities to become compliant and train workforce
  - Must be able to indentify, record, investigate and report breaches that occur 30 calendar days after Regulations are published

Notification Requirements

- Upon determination that a reportable breach has occurred, the CE or BA must provide notification
- In General
  - CEs timely notify individuals
  - CEs notify HHS Secretary
    - Concurrently with individual notification if $\geq$ 500 individuals
    - Provide on annual log if < 500 individuals
  - CEs timely notify media if $\geq$ 500 individuals have their unsecured PHI breached in a State or jurisdiction
  - BAs notify CEs when individual's unsecured PHI is breached

Notification for Individuals

- CEs to notify without unreasonable delay, and in no case later than 60 calendar days from "discovery"
  - Actual discovery or when should have discovered using reasonable diligence
  - Someone other than the person who committed the breach finds out
  - CEs are not liable for failure to provide notice where the CE did not know or have reason to know of breach

Effect of "Discovered" and Reasonable Diligence

- Timeliness of notification begins once the breach is "discovered"
  - Time starts when breach is discovered, not when the CE or BA determines it is reportable
  - Implement reasonable systems to detect and discover potential breaches
  - Educate and train workforce members on importance of timely reporting potential breaches and consequences for failing to do so

Timeliness of Notification *Covered Entities*

- Without unreasonable delay, but not later than 60 days from discovery
  - CE allowed to conduct a reasonable investigation to determine cause and to gather information for providing notice, but investigation does not extend time frame for providing notice
  - Exception for law enforcement

Content of Notification

- General
  - Written notification
  - Plain English
  - Appropriate reading level
  - No page limitation

Content of Notification (cont'd)

- Content
  - Brief description, including date of breach and discovery
  - Type of unsecured PHI
  - Recommended steps for individuals to take to protect themselves
  - Brief description of what CE is doing to investigate, mitigate harm, and prevent future, similar breaches
  - Contact information of CE
  - Any sanctions CE imposed on a workforce member involved in breach

Content of Notification (cont'd)

- CEs may need to take reasonable steps to ensure individuals receive notification
  - Civil Rights Act of 1964
  - Rehabilitation Act of 1973
  - American with Disabilities Act of 1990

Methods of Notification

- Actual Notification
  - Written notification given to each individual
- Substitute Notification
  - Only when actual notification is not possible
- Media Notification
- HHS Secretary Notification

Actual Notification

- Delivered via first class mail to last known address
  - May be sent via e-mail if individual previously consented
  - Sent to parent or guardian if individual is a minor or otherwise incapable of understanding
  - Individual known to be deceased, then notification sent to next-of-kin or personal representative

Actual Notification (cont'd)

- Exceptions to Actual Notification
  - Unknown next-of-kin or personal representative for deceased individuals
    - CE not obligated to seek out contact information if it was unaware individual was deceased
  - Last known address is out-of-date or incomplete
    - Must use substitute notification
  - Fear of imminent misuse of unsecured PHI
    - May use alternate contacts, such as telephone
    - Not a substitute for actual written notice

Substitute Notification

- When can it be used in lieu of actual notification?
  - Where individual's last known address is out-of-date or incomplete
  - Actual notifications are returned because they are undeliverable

Substitute Notification (cont'd)

- Must be reasonably calculated to reach the particular individuals to whom actual written notice could not be provided
- Must not unnecessarily disclose unsecured PHI
- Must include a toll-free number, active for at least 90 days

Substitute Notification (cont'd)

- Notification can be satisfied by the following
  - <10 individuals
    - Alternative written form, telephone call, or other means, even if individuals have not previously consented to such methods
  - ≥ 10 individuals
    - Conspicuous notice on home page of website for 90 days
    - Conspicuous notice in major print or broadcast media in geographic area where individuals reside

Media Notification

- > 500 residents of a State or jurisdiction
  - Jurisdiction is an area smaller than a State such as County, City or Town
- CE shall notify "prominent media outlet"
  - Defined by the geographical disbursement of the affected residents i.e. state-wide general newspaper or city-wide

Media Notification (cont'd)

- In addition to actual written notice, *not* in lieu of
- Can serve as substitute notice in the event actual written notice is not possible
  - Must conform to all other requirements of substitute notice
  - Must be reasonably calculated to reach such individuals that were not otherwise reachable via actual written notice

Media Notification (cont'd)

- Timeliness
  - Without unreasonable delay, no later than 60 calendar days from "discovery"
- Content
  - Must contain the same information as in the actual written notification

Media Notification (cont'd)

- Exceptions to media notification
  - Individuals spread out over several states and not one state as > 500 affected individuals
  - Breach occurred at BA and implicated several CEs and no one individual CE had > 500 affected individuals in a particular State or jurisdiction
    - However, if BA cannot determine which CEs' unsecured PHI was accessed, the Regulations advise that the BA provide media notification on behalf of all affected CEs

HHS Secretary Notification

- ≥ 500 individuals, provide notice concurrently with actual written notice
  - Regardless of geography
- < 500 individuals, maintain a log and submit annually
- Instructions will be posted to HHS website regarding content and how to submit notification
- HHS website will post listing of all CEs who submit breaches of ≥ 500 individuals

Business Associate Notification

- Significant new legislation
  - BAs were previously not directly liable under HIPAA
- Notify CEs of any reportable breach
  - CEs must notify individuals
- Must identify each individual, to the extent possible
- Without unreasonable delay, no later than 60 calendar days from "discovery"

Business Associate Notification When Discovery is Imputed to CE

- BA is an agent of CE
  - Date breach is "discovered" by BA imputed to CE
- BA is an independent contractor of CE
  - CE is not considered to have "discovered" breach until date BA notifies CE of breach

HHS Regulations & the FTC

- In some cases a BA may be subject to both HHS and FTC Regulations
  - BA provides PHRs to customers of a CE through a BAA and to the public generally
  - FTC will deem BA to be in compliance where BA follows certain provisions of the Regulations and also complies with other provisions of FTC Regulations, including notifying FTC in 10 days of discovering breach

Law Enforcement Delay

- Notification time frame may be delayed if law enforcement official determines that notification may impede a criminal investigation
  - Delay will last for duration of stated time
  - Written statement with time frame
  - If provided orally, only valid for 30 days, unless extended in writing

Notification Pointers

- Implement systems to detect and discover potential breaches
- Train workforce on new requirements
- Clearly layout sanctions for non-compliance
- CEs should identify all business associates
- BAs should identify all subcontractors
- BAAs and subcontract agreements should clearly set forth time frames for breach notification to be provided to CE or BA, as applicable
- Update all agreements to reflect new requirements in the Regulations
- Secure all PHI to avoid notification requirements

Preemption and State Security Breach Notification Laws

- HITECH preempts "contrary" state notification laws
  - "Contrary" = impossible to comply with both
  - Also contrary if the state law stands as an obstacle to accomplishment of the HITECH breach notification provisions

HITECH vs. State Laws

- Examples of State law approaches
  - Harm factor
  - Time periods
  - Notification to state government agencies
- Practical Impact

Questions and Answers

FOLEY
FOLEY & LARDNER LLP

Contact Us

Lisa J. Acevedo
Partner
321 N. Clark St., Ste 2800
Chicago, IL 60654
Tel: 312.832.4381
lacevedo@foley.com

Peter F. McLaughlin
Senior Counsel
111 Huntington Ave., 26th Flr.
Boston, MA 02199
Tel: 617.502.3265
pmclaughlin@foley.com

Leeann Habte
Associate
555 S. Flower St., Ste 3500
Los Angeles, CA 90071
Tel: 213.972.4679
lhabte@foley.com

Aaron Tantleff
Associate
321 N. Clark St., Ste 2800
Chicago, IL 60654
Tel: 312.832.4367
atantleff@foley.com