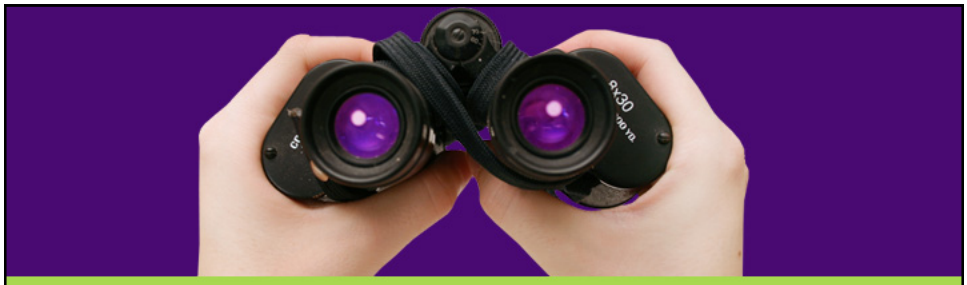

Security Breach Notification and Identity Theft Detection: Putting All the Pieces Together

Moderator:
Lisa Acevedo

Panelists:
Leeann Habte Shirley Morrigan Jennifer Rathburn
Peter McLaughlin Michael Overly Michael Scarano

FOLEY
FOLEY & LARDNER LLP

Thursday, April 30, 2009

11:30 a.m. – 1:00 p.m. CT

09 5521

Today's Presenters

Lisa Acevedo
Chicago

Shirley Morrigan
Los Angeles

Mike Scarano
Del Mar/San Diego

Leeann Habte
Los Angeles

Mike Overly
Los Angeles

Peter McLaughlin
Boston

Jennifer Rathburn
Milwaukee

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
- Today's program is being recorded and 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
- Materials can be found on our Web site at www.foley.com/fridayfocus or by clicking the printer icon on the bottom right hand side of your screen

HITECH Act

- Health Information Technology for Economic and Clinical Health Act (HITECH Act) within the American Recovery and Reinvestment Act of 2009
  - Subtitle D - Privacy
    - Expansion of privacy and security requirements to forward adoption of EHRs
    - Impacts covered entities, business associates, and vendors not currently subject to HIPAA

Heightened Enforcement

- Mandatory formal investigation and penalties for "willful neglect"
- Increased CMP amounts based on level of intent
  - Starts at $100; can go as high as $1.5 million

Heightened Enforcement (cont'd)

- State Attorneys General
  - Provided enforcement authority to bring actions on behalf of individuals
  - Courts can award damages, costs and attorney fees

Heightened Enforcement (cont'd)

- Penalties will be used to fund OCR enforcement activities
  - Portion of penalties to ultimately go to patients
- Business associates will be subject to criminal and civil penalties
- Employees of covered entities now clearly subject to criminal liability

Heightened Enforcement (cont'd)

- Audits
  - Covered entities **and** business associates will be subject to periodic audits

Heightened Enforcement (cont'd)

- Effective Date
  - Most changes become effective immediately, with recommendations and regulations to be issued

Security Breach Notification

- Patients must be notified of any unauthorized acquisition, access, use or disclosure of their unsecured PHI that compromises the privacy or security of such information
- There are exceptions related to unintentional or inadvertent use or disclosure by employees or authorized individuals within the "same facility"

Security Breach Notification (cont'd)

- Timeliness and Content of Notification
  - Without unreasonable delay and in no case later than 60 calendar days after "discovery" of the breach
  - Brief description of what happened, types of unsecured PHI involved, steps individuals should take to protect themselves, brief description of what covered entity is doing to investigate the breach, mitigate harm, etc., and contact information

Security Breach Notification (cont'd)

- Methods of Notice
  - Individuals
    - Detailed requirements about how notification must be sent (e.g., first class mail, web-site or media posting, telephone)
  - Media
    - 500+ residents in area
  - Secretary
    - 500+ individuals - immediate notice (will be posted on HHS website)
    - Less than 500 - annual log

HITECH Act Breach Notification Guidance

- HHS was required to define the term "unsecured PHI" within 60 days of enactment of the HITECH Act
- Guidance Specifying the Technologies that Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals issued on April 17, 2009
- Applies to breaches 30 days after publication of the forthcoming interim final regulations to be issued by August 16, 2009
- Comments must be submitted on or before May 21, 2009

HITECH Act Breach Notification Guidance (cont'd)

- Guidance specifically states that de-identified information is not PHI, thus not subject to the HIPAA Privacy and Security Rule
- HHS requested comments on whether a LDS should be treated as unusable, unreadable, or indecipherable to unauthorized individuals for purposes of breach notification

HITECH Act Breach Notification Guidance (cont'd)

- PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals and thus is not "unsecured PHI" if one or more of the following "safe harbors" apply:
  - Encryption. All encryption can be "cracked," but sometimes don't need to crack (e.g., key logger brings down the mafia). Computationally infeasible. Security depends on:
    - Strength of the encryption algorithm; and
    - Security of decryption key/process
  - Destruction
    - Paper records
    - Electronic media

HITECH Act Breach Notification Guidance (cont'd)

- Encryption
  - Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of 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" and such confidential process or key that might enable decryption has not been breached
  - List of technologies and methodologies identified in guidance for "safe harbor" is meant to be exhaustive not illustrative

HITECH Act Breach Notification Guidance (cont'd)

- Data is vulnerable in the following states:
  - Data in motion (e.g., network, wireless transmission)
  - Data at rest (e.g., databases, file systems, other storage)
  - Data in use (e.g., being created, retrieved, updated)
    - Most problematic to secure
  - Data disposed (e.g., discarded paper records and electronic media)
- With the possible exception of "data in use", PHI in each of these states may be secured using one or more methods

HITECH Act Breach Notification Guidance (cont'd)

- Encryption processes that have been tested by the National Institute of Standards and Technology (NIST) and judged to meet the HIPAA encryption standard
  - "Data at rest" means data that resides in databases, file systems, and other structured storage methods
  - Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.* (*www.csrc.nist.gov*)

HITECH Act Breach Notification Guidance (cont'd)

- "Data in Motion" means data that is moving through a network, including wireless transmission
- Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2, including:
  - Standards described in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations,*
  - *800-77, Guide to IPsec VPNs,*
  - 800-113, *Guide to SSL VPNs,* and
  - May include others which are FIPS 140-2 validated

HITECH Act Breach Notification Guidance (cont'd)

- Data in Use means data in the process of being created, retrieved, updated, or deleted
  - HHS Guidance has not addressed ways to protect such data
  - Most complex to secure
    - Screen capture/printing
    - Screen orientation
    - Sharing of passwords
    - Failure to logoff (timeouts)
    - Caching (cause of many compromises)

HITECH Act Breach Notification Guidance (cont'd)

- Data disposed means discarded paper records or recycled electronic media
  - The media on which the PHI is stored or recorded must have been destroyed in one of the following ways:
  - Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed
  - Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved
  - Beware hardware support vendors, removable media, and e-bay

Breach Detection

- Detection of Breaches of Unsecured PHI
  - Monitoring use of PHI
    - Review of audit trails – All applications and operating systems generate audit/log files. Can be voluminous. All relevant information may not be captured.
      - Sometimes improperly configured, turned off, or records overwritten
    - Systems that help monitor access, use, and disclosure of PHI

Breach Investigation

- Investigation of Potential Breaches of Unsecured PHI
  - Determining whether a breach of and Electronic Health Records occurred
    - Audit trails
    - Computer Forensics
    - Other

HITECH Act Breach Notification Guidance (cont'd)

- HHS is seeking comment on:
  - Electronic media configurations such as a fingerprint protected Universal Serial Bus (USB) drive, which guidance should specifically address
  - Other methods that should be considered for rendering paper and electronic PHI unusable, unreadable, or indecipherable to unauthorized individuals
  - Circumstances under which the methods discussed above would fail to render information unusable, unreadable, or indecipherable to unauthorized individuals
  - Whether future guidance should specify which off-the-shelf products, if any, meet the encryption standards identified in this guidance

Security Breach Hits Credit Cards

HSBC Notifies 180,000 People Who Shopped At Ralph Lauren; Other Banks May Be Affected

DSW Shoe Says Theft of Data Involved 1.4 Million Credit Cards

Reed Elsevier PLC

LexisNexis, After Breach Scare, To Bolster Security Procedures

File Sharing

For Big Vendor of Personal Data, A Theft Lays Bare the Downside

ChoicePoint Struggles to Gauge How Much Information Fell Into Wrong Hands

BJ's Wholesale Club Inc.

Net Rises 27% on Brisk Sales; Security-Breach Claims Levied

PETCO TO IMPROVE COMPUTER SECURITY

http://breach.scmagazineblogs.com/category/health-care/

Why do These Incidents Occur?

- Sometimes completely accidental
- Sometimes related to identity theft -- the fastest growing crime in the United States
  - Stolen or fraudulently-acquired personal information enables identity theft
  - Black market for identity theft
  - Most sensitive data is social security number, financial information (including credit card #s), health information, passwords, pin numbers, etc.

Security Breach Notification Laws

- Enacted in 44 States (including NY, FL, PA, CA and IL)
- Generally, requires notice to affected individuals in the event of a breach in the security, confidentiality, or integrity of computerized personal information
- Typically does not apply to encrypted information (unless encryption key is compromised)
- Applies even if there is simply a reasonable belief that there was an acquisition of data

State Identity Theft Laws

- Alaska
- Arizona
- Arkansas
- California
- Connecticut
- Delaware
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Texas
- Utah
- Vermont
- Virginia
- Washington
- Washington D.C.
- West Virginia
- Wisconsin
- Wyoming

Certain Issues

- What good is encryption?
- Electronic v. non-electronic
  - North Carolina's law applies to non-electronic
- Is there a general duty?
- Is notice required if there is no likelihood of identity theft?

Who Must be Notified

- Affected individuals
  - Standard
  - Employees?
- Government / law enforcement?
  - Federal
  - State
- Business partners?
  - Pennsylvania: Specifically states that service provider to provide notice to its customer who in turn notifies individuals
  - Florida: Requires notice to business partners for which you maintain personal information
- Credit bureaus?
- Insurance company?

Service Provider Obligations

- State laws often apply directly to service providers
- Contractually
  - Data security and privacy requirements broader and more detailed than traditional BA agreements
  - Data incident obligations – cost shifting
- Internally
  - Implement appropriate policies
  - Educate employees about handling inquiries

The California Experience: S.B. 541, Health and Safety Code Section 1280.15

- Requires clinics, health facilities, home health agencies or licensed hospices ("providers") to prevent unlawful or unauthorized access to, use of, or disclosure of medical information

S.B. 541 (cont'd)

- Companion bill: A.B. 211
  - Not the subject of today's talk
  - Applies to a wide variety of licensed providers
  - Enforcement authority is limited to persons or providers not governed by SB 541

S.B. 541 (cont'd)

- Violation = misdemeanor
- Administrative penalties
  - Up to $25,000 per patient for violation
  - Up to $17,500 per subsequent access, use, or disclosure

S.B. 541 (cont'd)

- Requires reporting by provider
  - To CDPH within 5 days of detection AND
  - To patient or representative within 5 days of detection
- Fines
  - $100/day for not reporting/notifying up to $250,000 total per event

S.B. 541 (cont'd)

- Special considerations
  - History of compliance
  - Preventative action to immediately correct and prevent past violations from recurring
  - Factors outside provider's control that restricted ability to comply
  - Special circumstances of small and rural hospitals

S.B. 541 (cont'd)

- Disputes
  - Provider can dispute
    - within 10 days
  - In lieu of dispute
    - Pay 75% of total within 30 business days

Follow-on Issues Re: S.B. 541

- Are these "adverse events?" No
- Are these "unusual occurrences?" No
- What is detection?
  - Psychiatric patient complaints
  - Employee complaints against each other
  - Union representation
  - Need to assess

Follow-on Issues Re: S.B. 541 (cont'd)

- Telephone calls
- Faxes
- Leaving computer on

Follow-on Issues Re: S.B. 541 (cont'd)

- What needs to be in a report?
  - Patient names? No
  - Information itself? No
  - Names of Employees No
- THERE ARE NO REGULATIONS, BUT:
  - Facts
  - Name and telephone number of contact person

Follow-on Issues Re: S.B. 541 (cont'd)

- Misdirected faxes
  - Stay internal
  - Proper purpose

  > probably not reportable

  - Go external

  } report

  - Much is unknown!

Red Flag Rules

- Mandated by Fair & Accurate Credit Transactions Act of 2003
- Requires "creditors," including health care providers who accept payment after services rendered, to establish a written program to detect, prevent and mitigate "identity theft"

Red Flag Rules (cont'd)

- Compliance Date: May 1, 2009
  - Policies should be drafted
  - Board or committee approval obtained
  - Party (Board, Committee or senior manager) responsible for oversight should be designated
  - Staff should be trained, "as necessary"
  - Mechanisms should be in place for oversight of "service providers"

Written Policies

- FTC: "high risk entities [should] have more elaborate Programs, while low risk entities could have streamlined and less complex Programs"
- Review and incorporate applicable HIPAA policies, e.g., by cross-referencing

Training

- Not required to train all staff
  - If less than all, identify categories of staff to be trained in Policies
- Consider integrating with HIPAA training

Oversight of Service Providers

- Must exercise effective and appropriate oversight of all service providers who "perform an activity in connection with one or more covered accounts"
- Service providers would include most if not all Business Associates

Oversight of Service Providers (cont'd)

- Could contractually require SPs
  - To have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities and
  - To either report the Red Flags to the creditor, or to take appropriate steps to prevent or mitigate identity theft, or both

Oversight of Service Providers (cont'd)

- Can amend Business Associate Agreement, the Service Provider's Primary Agreement or separate new agreement
- Issue: whether to amend Business Associate Agreements to meet HITECH's new HIPAA requirements now or wait until the regulations are enacted

Accounting

- Accounting Rules Change for EHRs
  - Must account for disclosures related to treatment, payment and health care operations (as well as all other accountable disclosures)
  - Three year period
  - Business Associates may be impacted
  - Regulations to be issued regarding the information that must be collected for an accounting

Accounting (cont'd)

- Effective Date
  - Current users of EHRs: 1-1-14
  - Future users of EHRs (after 1-1-09): 1-1-11 or date EHR is acquired (whichever is later)

Accounting (cont'd)

- System capabilities
  - Information that can be logged
  - How logs can be created
  - When information can be tracked
  - Whether audit trails can be used for accounting

HITECH Act Audit Trail Capabilities

- Audit Trail Capabilities:
  - Determine what is tracked and by which application
  - Confirm an audit trail is created by all relevant systems for all relevant data and actions. Look for gaps
  - Audit trail data must be backed up and retained for a period consistent with relevant document retention requirements
  - Audit trails may be intentionally or unintentionally modified, corrupted, or destroyed
  - Consider use of WORM drives or other technology to ensure the integrity of audit trail data
  - Make audit trail functionality part of all relevant IT contracts, including outsourcing engagements

What the HITECH Act Means for Business Associates

- HITECH Act
  - Requires Business Associates to Comply with HIPAA Security Rule
    - Security rule applies to business associate of a covered entity in the same manner that such sections apply to the covered entity (45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316)
    - Allows Secretary of HHS to conduct periodic audits of covered entities *and* business associates for compliance with security rules
  - Security requirements must be incorporated into Business Associate Agreements
  - Effective 12 months after enactment of HITECH Act

What the HITECH Act Means for Business Associates (cont'd)

- HITECH Act –
  - Requires Business Associates to report breaches of unsecured PHI to Covered Entities
    - Effective 30 days after interim final regulations are issued on breach notification
  - Requires Business Associates to Comply with HIPAA Privacy Rule
    - Subjects Business Associates to enforcement provisions, *e.g.* civil and criminal penalties for HIPAA violations
    - Effective 12 months after enactment of HITECH Act

Business Associate Compliance with the HIPAA Security Rule

- Written Security Plan and Documentation is Required
  - Maintain the policies and procedures in written form
    - Must address standards and implementation specifications
      - Some implementations are required; others are addressable
      - If addressable, entity can assess reasonableness and appropriateness of safeguard to its environment and either implement or document and implement an equivalent alternative measure
  - Maintain a written record of the security assessment
    - Time Limit (Required) – 6 years
    - Availability (Required)
    - Updates (Required)

HIPAA Security Rule: Administrative Safeguards

- Security Management Process
  - Risk analysis (Required)
  - Risk management (Required)
  - Sanction policy (Required)
  - 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

HIPAA Security Rule: Administrative Safeguards (cont'd)

- Assigned Security Responsibility
- Workforce Security
  - Authorization and/or supervision (Addressable)
  - Workforce clearance procedure (Addressable)
  - Termination procedures (Addressable)
- Information Access Management
  - Isolating health care clearinghouse functions (Required)
  - Access authorization (Addressable)
  - Access establishment and modification (Addressable)

HIPAA Security Rule: Administrative Safeguards (cont'd)

- Security Awareness and Training (for all workforce members)
  - Security reminders (Addressable)
  - Protection from malicious software (Addressable)
  - Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies
  - Password management (Addressable)
- Security Incident Procedures
  - Response and Reporting (Required)

HIPAA Security Rule: Administrative Safeguards (cont'd)

- Contingency Plan
  - Data backup plan (Required)
  - Disaster recovery plan (Required)
  - Emergency mode operation plan (Required)
  - Testing and revision procedures (Addressable)
  - Applications and data criticality analysis (Addressable)
- Evaluation
  - Perform a periodic evaluation
    - Evaluation must establish the extent to which an entity's security policies and procedures meet these requirements

HIPAA Security Rule: Physical Safeguards

- Facility Access Controls
  - Contingency operations (Addressable)
  - Facility security plan (Addressable)
  - Access control and validation procedures (Addressable)
  - Maintenance records (Addressable)
- Workstation Use
- Workstation Security
- Device and Media Controls
  - Disposal (Required)
  - Media re-use (Required)
  - Accountability (Addressable)
  - Data backup and storage (Addressable)

HIPAA Security Rule: Technical Safeguards

- Access Control
  - Unique user identification (Required)
  - Emergency access procedure (Required)
  - Automatic logoff (Addressable)
  - Encryption and decryption (Addressable)
- Audit Controls
  - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI

HIPAA Security Rule: Technical Safeguards (cont'd)

- Integrity
  - Mechanism to authenticate electronic PHI (Addressable)
- Person or Entity Authentication
- Transmission Security
  - Integrity controls (Addressable)
  - Encryption (Addressable)

Implementation Issues

- Implementation of HIPAA Requirements
  - Gap analysis
  - Determination of appropriate safeguards
    - Relative to
      - The size, complexity, and capabilities of the covered entity
      - The covered entity's technical infrastructure, hardware, and software security capabilities
      - The costs of security measures
      - The probability and criticality of potential risks to electronic protected health information
  - Development of a written security plan/requirements

Technical Safeguards

- Key technical requirements
  - Access control
  - Auditing and monitoring
    - No substitute for “on-the-ground” review of vendor security measures
  - Integrity
  - Authentication
  - Storage, transmission, use, and destruction security

Contractual Issues

- Contractual Issues for Business Associate Agreements
  - Due diligence
    - Use of standard questionnaire
    - Incorporate into final agreement
  - Documentation of security safeguards and information handling requirements
  - Security notifications and cooperation

Contractual Issues (cont'd)

- Liability issues
  - Covered entities not directly liable for actions of business associates
    - Not required to monitor or oversee how their business associates carry out their privacy or security safeguards
    - Must cure breaches or end violations and, if unsuccessful, terminate the contract with the business associate. [45 C.F. R. § 164.504(e)(1) and OCR HIPAA Privacy Guidance, December 3, 2002]
  - Indirect liability for breaches?
  - Be mindful of limitations of liability that render protections illusory

Questions and Answers

FOLEY

FOLEY & LARDNER LLP

Contact Us

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

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

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

Shirley Morrigan
Partner
555 S. Flower St., Ste. 3500
Los Angeles, CA 90071
Tel: 213.972.4668
smorrigan@foley.com

Michael Overly
Partner
555 S. Flower St., Ste. 3500
Los Angeles, CA 90071
Tel: 213.972.4533
moverly@foley.com

Jennifer Rathburn
Senior Counsel
777 E. Wisconsin Ave., Ste. 3800
Milwaukee, WI 53202
Tel: 414.297.5864
jrathburn@foley.com

Michael Scarano
Partner
11250 El Camino Real, St. 200
San Diego, CA 92130
Tel: 858.847.6712
mscarano@foley.com