Strafford

presents

HIPAA Privacy and Security Mandates and New Breach Notification Guidance

Preparing for Tougher Enforcement and Increased Penalties

A Live 90-Minute Teleconference/Webinar with Interactive Q&A

Today's panel features:

Stephen W. Bernstein, Partner, **McDermott Will & Emery**, Boston

Gina M. Kastel, Partner, **Faegre & Benson**, Minneapolis

Wednesday, November 18, 2009

The conference begins at:

1 pm Eastern

12 pm Central

11 am Mountain

10 am Pacific

Please refer to the dial-in/log-in instructions emailed to registrants to access the audio portion of the conference.

CLICK ON EACH FILE IN THE LEFT HAND COLUMN TO SEE INDIVIDUAL PRESENTATIONS.

If no column is present: click **Bookmarks**  or **Pages**  on the left side of the window.

If no icons are present: Click **View**, select **Navigational Panels**, and chose either **Bookmarks** or **Pages**.

If you need assistance or to register for the audio portion, please call Strafford customer service at **800-926-7926 ext. 10**

For CLE purposes, please let us know how many people are listening at your location by

- closing the notification box,
- clicking the chat button in the upper right corner,
- and typing in the chat box your company name and the number of attendees.
- Then click send.

McDermott
Will & Emery

Best Practices for HIPAA Security Amidst a Sea Change: HITECH & Re-Visiting Your Security Program

Stephen W. Bernstein, Esq.
28 State Street
Boston, MA 02109
617-535-4062
sbernstein@mwe.com

www.mwe.com

©2009 McDermott Will & Emery LLP. McDermott operates its practice through separate legal entities in each of the countries where it has offices. This communication may be considered attorney advertising. Previous results are not a guarantee of future outcome.

McDermott Will & Emery

HITECH Sure, but Don't Forget HIPAA Security Fundamentals

- Ensure the confidentiality, integrity and availability of all electronic protected health information ("EPHI") the CE creates, receives, maintains or transmits
- Protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI
- Protect against any reasonably anticipated uses or disclosures or EPHI that are not permitted or required under the Privacy Rule
- Ensure compliance by workforce

McDermott Will & Emery

Remember this Map? Déjà vu all over again!

Privacy Rule

Workforce Policies
- Access/Minimum necessary standard
- Training

Patient Rights Policies
- Access, Inspect, Copy
- Alternative means of communications
- Accounting of disclosures
- Amendments
- Restrictions
- Complaints

Notice of Privacy Practices
Acknowledgement of Receipt
Authorizations/Consents
Required and Permitted Disclosures
Business Associates
Employee Sanctions
Mitigation
Whistleblower Protections

Security Rule

Administrative Safeguards
- Security management process(R)
  - Risk analysis (R)
  - Risk management (R)
  - Sanction policy (R)
- Assigned security responsibility (R)
- Workforce security (R)
  - Authorization/Supervision (A)
  - Workforce clearance (A)
  - Termination procedures (A)
- Information access management(R)
  - Isolate clearinghouse functions (R)
  - Access authorization (A)
  - Access establishment/modification (A)
- Security awareness and training (R)
  - Security reminders (A)
  - Protection from malicious software (A)
  - Log-in monitoring (A)
  - Password management (A)
- Security incident procedures (R)
- Contingency plan (R)
  - Data backup plan (R)
  - Disaster recovery plan (R)
  - Emergency mode operation plan (R)
  - Testing and revision procedures (A)
  - Applications and data criticality analysis (A)
- Evaluation (R)
- Business associate contracts (R)

Physical Safeguards
- Facility access controls (R)
  - Contingency operations (A)
  - Facility security plan (A)
  - Access control and validation (A)
  - Maintenance records (A)
- Workstation use (R)
- Workstation security (R)
- Device and media controls (R)
  - Disposal (R)
  - Media re-use (R)
  - Accountability (A)
  - Data backup and storage (A)

Technical Safeguards
- Access control (R)
  - Unique user Id (R)
  - Emergency access (R)
  - Automatic logoff (A)
  - **Encryption and decryption (A)**
- Audit controls (R)
- Integrity (R)
  - Authenticate ePHI (A)
- Person or entity authentication (R)
- Transmission security (R)
  - Integrity controls (A)
  - Encryption (A)

Security Standards – But . . . with some new twists

- Grouped into 5 categories
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards*
  - Organizational Requirements
  - Policies and Procedures and Documentation Requirements*

Addressable Specifications

- Assess whether Implementation Specification is "reasonable and appropriate" in the particular department's environment

  - If so, implement
  - If not, document why not and identify and implement equivalent alternative measure
- Ultimately must satisfy the standard
- Document, Document, Document!!!!

Risk Assessment Itself

- Evaluating what you have and what risk there is of a problem
- Planning on how to reduce/limit the risk
- Conducting the assessment
  - Doing so with a purpose
  - Inform your policies and procedures
- Documenting it
  - Addressable standards: why you adopted something; why you did not

TECHNICAL SAFEGUARDS

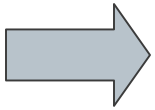
- STANDARD: Transmission Security - technical security measures to guard against unauthorized access while EPHI is being transmitted over an electronic communications network
  - ADDRESSABLE: Integrity controls
  - ADDRESSABLE: Encryption (note that it is not required under HIPAA, but strong language in preamble)
    - Note: Special State Law Requirements, e.g., Massachusetts mandated encryption for mobile devices
    - http://www.mwe.com/info/news/DataSecurityComplianceManual_TOC.pdf
  - Based on Results of Risk Assessment per regulations
  - Life Has Now Changed!

Two New Twists:

- Secure PHI vs. Unsecured PHI
- Security Incident/Security Breach Reporting

Twist 1: August 24, 2009 HHS Guidance

- Per HITECH, Secretary issued Guidance as to what is "secure" PHI.

  http://www.nacua.org/documents/FR_HITECHActInterimFinalRule_NotificationBreaches.pdf
- If PHI is not secure, if in the hands of a CE or BA (or a PHR related entity), then gives rise to a notification requirement if the unsecure PHI is accessed or acquired without authorization, But . . . Risk Assessment following event
- If PHI is "rendered unusable, unreadable, or indecipherable to unauthorized individuals", then PHI is considered "secure"  no reporting duty

"the" Technologies to Secure PHI

- Encryption: by 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
- The Guidance then cross-refers to several standards tested by the National Institute of Standards and Technology (NIST) and judged to meet the Encryption Standard above

NIST Standards (Unpacking the Details)

- Encryption for Data "at Rest" (http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf)
- Use case(s): E.g., Transferring Files Between Computers
  - Acquire and use a flash drive with self-contained storage encryption capabilities, such as encryption software and secure key storage, or
  - Acquire volume, virtual disk, or file/folder encryption solution that works on both PCs (office and home), and deploy it. Encrypt documents and store encrypted data on a flash drive.

NIST Standards (cont)

- Encryption for data “in motion”
- 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*

  http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf
- Federal Information Processing Standards

  http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

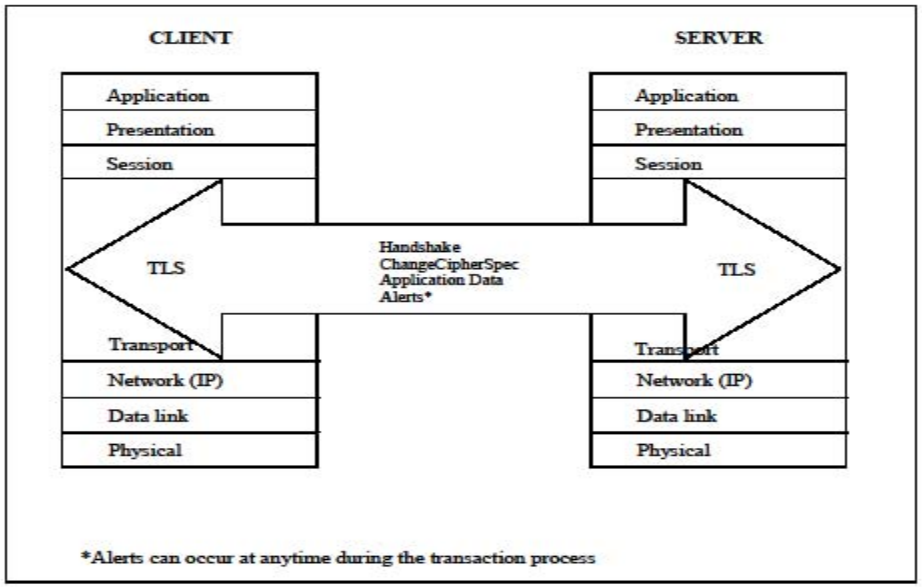


Figure 2: The Transport Layer Security Protocol Entity

The Transport Layer Security handshake protocol establishes a secure channel inside of a TCP/IP connection before passing any data from the application.

- The handshake protocol initializes both the client and server to use optional cryptographic capabilities by negotiating a cipher suite of algorithms and functions including key establishment, digital signature, confidentiality and integrity algorithms with their respective key sizes, and hash functions. This negotiation begins with the "ClientHello" message and continues with the "ServerHello" message.
- The handshake protocol may exchange public key digitally signed X.509 certificates[14] to optionally authenticate the server to the client and vice versa. In most cases, the server presents a certificate to the client, but the client does not present a certificate to the server. However, TLS and SSL allow for certificates to be presented by a server, by a client, by both, or by neither in negotiating a

[14] The use of X.509 certificates is fundamental to TLS/SSL, as well as other PKI-enabled services. For a comprehensive explanation of X.509 certificates see, for example, [Adams99] or [Housley01].

NIST Standards (cont)

- Paper, film, other hard copy media: Shred or destroy consistent with NIST 800-88, *Guidelines for Media Sanitization* (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
- Clearing (over-write)
- Purge (demagnetize)
- Destroy (shred, pulverize)

McDermott Will & Emery

Twist 2: FTC Rules re: Security Breach Reporting of PHR Identifiable health information

- For the most part, tracks ARRA statutory language
- http://www.ftc.gov/os/2009/08/R911002hbn.pdf
- Adds 2 keys points for PHR breach notifications:
  - Distinction between ACCESS to information and ACQUISITION of Information
    - Access means available; Acquisition means "in fact obtained";
    - Statutory language for PHR breaches requires "acquisition" whereas breach language for HIPAA covered entities includes both "access" and "acquisition"

Twist 2: FTC Nuances re: Security Breach Reporting of PHR Identifiable health information (cont)

- Presumption Approach
  - FTC will presume that unauthorized persons have acquired information if they have access to it, creating a reporting obligation . . .
  - Unless . . . the presumption can be rebutted with reliable evidence showing that the information was not or could not reasonably have been acquired
  - E.g., Evidence obtained through interviews of employees, contractors, other third parties; reviewing access logs and sign-in sheets, and/or examining forensic evidence (Recovered lap top example)

III. Let's Get Real: What to do Next

- Assemble or Re-Assemble Your Teams
  - Privacy and Security Officers
  - CIO
  - Legal
  - Risk Management
  - Human Resources
  - Marketing/Fundraising
  - Get Senior Management Buy-In

Risk Assessments

- Two Types:
  - Pre-Security Event Assessment as to what risks exist with respect to future risk of harm across the covered entity/business associate's business where PHI exists, is obtained, used and disclosed
  - Post-Security Event Assessment "as to Risk of Harm to the Individual"

Let's Get Real: Self-Evaluation

- Pre-Security Event Risk Assessment
  - Evaluating what you have and what the risk is of a problem
  - Planning on how to reduce/limit the risk
  - Implementing the Plan
  - Documenting It
  - Conducting it under Attorney-Client Privilege
- Policies and Procedures
  - Matching them to your plan
  - Telling and working with your team on expectations
  - Documenting your internal/external rules
- Inside and Outside Technical and Policy Writing Help

Pre-Security Event Risk Assessment

Elements of the Assessment Itself

- Example:

  §164.308(a)(3)(i):

  Workforce Security Standard – Implement policies and procedures to ensure that all members of workforce have appropriate access, and prevent those who shouldn't from gaining access

  Identified Threat: Unauthorized disclosure among workforce

  Risk Rating: Low – Medium – High?

  Context Based: Principal Investigators, CROs, Research Assistants?

  Recommendation/Risk Mitigation: E.g., Review application menus, passwords

See e.g., MWE Assessment Tool

http://www.mwe.com/info/news/HIPAA_CoveredEntities.pdf

POLICIES, PROCEDURES AND DOCUMENTATION

- *STANDARD: Implement reasonable and appropriate policies and procedures to comply with the Security Rule, taking into account four factors:*
  - *Size, complexity and capabilities*
  - *Technical infrastructure, hardware and software security capabilities*
  - *Cost of security measures*
  - *Probability and criticality of potential risks to ePHI*

McDermott Will & Emery

POLICIES, PROCEDURES AND DOCUMENTATION (con't)

- *Required policies and procedures (con't):*
  - Does not permit or excuse any violation of any other Standard or Implementation Specification
  - Policies and procedures may be changed at any time; changes must be documented and implemented pursuant to the Security Rule

Pre-Security Event Policies/Procedures

A. Rules of the Road as they apply in your context

B. Example: Workforce Security

Rule – Implement policies and procedures to ensure that all members of workforce have appropriate access and prevent those who don't have access from gaining access

Policy: Only those with authorized need to access ePHI may do so; Authorization is determined by _____

Procedures: User ID, passwords, training

Preventing access to former members of workforce; checklist of Termination Procedures

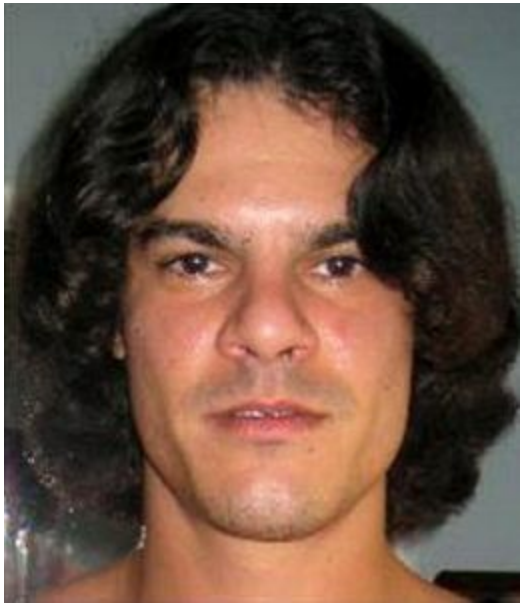
See e.g., MWE Template Policies and Procedures

http://www.mwe.com/info/news/HIPAA_CoveredEntities.pdf

http://www.mwe.com/info/news/HIPAA_BusinessAssociates.pdf

Security Incident/Breach Response Team, Policies & Procedures

- Policy: Identify, Report, Mitigate
- Scope: What type of information is covered
- Team
- Types of Breaches
  - Employee or Contractor
  - Outside Party
- Procedures



Security Incident/Breach Response Team, Policies & Procedures (cont)

- Evaluation: Fact Gathering
  - Post-Event Risk Assessment as to "risk of harm to the individual"
  - Did a Breach, in fact, occur?
    - "If the nature of the protected health information does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach."
    - Type and Amount of PHI Involved
    - Now, controversial; Congress pushing back

Security Incident/Breach Response Team, Policies & Procedures (cont)

- Evaluation: Fact Gathering
- Reporting Duties, Time Frames
  - Federal
  - State (including Multi-State) (Yes, the dreaded 50-state survey)
- Public Relations
- Document

Security Incident/Breach Response Team, Policies & Procedures (cont)

- Once Concluded that there was a Breach . . .
- Reporting Duties, Time Frames
  - Federal
  - State (including Multi-State) (Yes, the dreaded 50-state survey)
- Public Relations
- Document

Security Incident/Breach Response Team, Policies & Procedures (cont)

- Mitigation
  - Technical (E.g., turning off application)
  - Non-Technical (E.g., law enforcement, get data back)
  - Reporting
    - Individuals, State/Federal Authorities, Websites
  - Personnel: Disciplinary Action
  - Post-Incident Review and Modification
  - Additional Training
- Start All Over Again

McDermott Will & Emery

Questions & Answers

Stephen W. Bernstein, Esq.
28 State Street
Boston, MA 02109
617-535-4062
sbernstein@mwe.com

FAEGRE & BENSON LLP

HIPAA Privacy & Security Mandates New Breach Notification Guidance

Gina Kastel

Agenda

- Summary of American Recovery and Reinvestment Act ("ARRA") changes to privacy and security provisions of Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Emphasis on new security breach notification regulations, which were published in August

Business Associates

- Business associates are persons providing administrative services to covered entities that receive or create PHI
- HIPAA privacy and security requirements do not currently apply directly to business associates—contract obligation but no direct enforcement
- ARRA requires business associates to comply with privacy rule provisions regarding business associate agreements, but not others
- ARRA requires business associates to comply with security rule provisions on administrative safeguards, physical safeguards, technical safeguards, and policies and procedures

Business Associates (continued)

- Expands definition to include regional health information organizations, health information exchange organizations, e-prescribing gateways
- Requires updates to existing business associate agreements to incorporate new requirements
- Effective date is February 17, 2010

Other Changes

- Minimum necessary changes require use of limited data set where possible (2/17/10)
- Individuals may restrict disclosures of PHI to health plans for payment or health care operations for services paid by individual in full out of pocket (2/17/10)
- Certain marketing communications formerly treated as health care operations will require authorization (2/17/10)
- Fundraising disclosures must include clear and conspicuous opt out notice (2/17/10)
- Sales of PHI are more restricted (6 months after regs published)

Other Changes

- Patient has right to accounting of disclosures for treatment, payment and health care operations made from electronic health record (Not before 2011)
- Patient has right to access to data in electronic health record in electronic format (2/17/10)

Enforcement

- Civil penalties are enhanced with maximum penalties for willful neglect rising to $1.5 million in a single year
- State attorney general now has authority to enforce HIPAA with reason to believe the interest of one or more persons is threatened or adversely affected by a HIPAA violation
  - May sue to enjoin a violation or for damages
  - May be awarded attorney fees
- HHS has new authority to perform periodic audits

Security Breach Notification

Security Breach Notification

- No current obligation to report unauthorized disclosures or security incidents involving protected health information to individuals or to Health and Human Services
- New requirement for covered entities and business associates to give notice of breaches of unsecured PHI
- Regulations published August 24, 2009 (74 Fed. Reg. 42740)

Key Concepts– Unsecured PHI

PHI not rendered unusable, unreadable or indecipherable to unauthorized persons through a technology or methodology specified by the Secretary of Health and Human Services ("HHS")

- Note:
  - This is not just an issue for electronic PHI—paper and other hard copy information and oral information are also subject to the notification requirement
  - Compliance with the HIPAA security rule does not make PHI secure for breach notification purposes

Key Concepts-Unsecured PHI

- Two methods to render PHI unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction
- First guidance published April 17, 2009, see www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html
- Guidance updated August 24, 2009, see 74 Fed. Reg. 42740

Key Concepts-Unsecured PHI

FAEGRE & BENSON LLP

Encryption continued

- Data at rest: processes consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.
- Data in motion: processes consistent with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security Implementation*; 800-113, *Guide to SSL VPNs*, or others which are Federal Information Processing Standards 140-2 validated.

Key Concepts-Unsecured PHI

FAEGRE & BENSON LLP

Destruction

– Paper and other hard copy data is destroyed by shredding or destroying it in a manner that ensures it cannot be read or reconstructed.

– Electronic media is considered destroyed if it is cleared, purged or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, and cannot be retrieved.

– Redaction is specifically excluded as a method of data destruction.

Key Concepts-Breach

The unauthorized acquisition, access, use or disclosure of protected health information in a manner not permitted by the HIPAA privacy regulations that compromises the security or privacy of the protected health information.

- *Unauthorized* means an acquisition, access, use or disclosure that violates the HIPAA privacy rule. This could include violations of minimum necessary requirement.
- *Compromises the security or privacy of the PHI* means the breach poses a significant risk of financial, reputational, or other harm to the individual.
- Breach of the HIPAA privacy rule or security rule, standing alone, is not a breach for notification purposes, though it could lead to a breach.

Key Concepts-Exceptions to Breach

Any unintentional acquisition, access or use of PHI by a covered entity's workforce member, a person acting under the authority of the covered entity, or a business associate, if the acquisition, access or use was made in good faith and within the scope of authority, and does not result in further use or disclosure in a manner that violates the privacy rule.

Key Concepts—Exceptions to Breach

- Inadvertent disclosure by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or an organized health care arrangement in which the covered entity participates, if the information received is not further used or disclosed in a manner that violates the privacy rule.
- A disclosure of PHI where the covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI.

Key Concepts – Risk Assessment

- Risk assessment is needed to determine whether a significant risk of financial, reputational, or other harm may occur.
- Aims for consistency with state security breach notification laws.
- Factors for consideration:
  - Who impermissibly used or received the PHI
    - Use by another covered entity may be less risky than entity with no obligation to maintain privacy and security
  - Whether mitigation steps have eliminated or reduced the risk
  - Whether the PHI was returned
  - The type and amount of PHI involved
- Risk assessments must be documented.

Key Concepts-Discovery of Breach

- A breach is treated as discovered as of the first day on which the breach is known to the covered entity, or, by exercising reasonable diligence, would have been known.
- A covered entity is deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (using federal common law of agency) of the covered entity.
  - Agents may include business associates, depending on circumstances

Questions to Ask

- Did the incident involve unsecured PHI?
- Was there an unauthorized acquisition, access, use or disclosure that violated the privacy rule?
- Does an exception apply?
- Is there a significant risk of harm to the affected individual?

Notice Requirements-Individuals

- Covered entities must notify an individual whose unsecured PHI has been or is reasonably believed to have been accessed, acquired, used or disclosed as a result of a breach.
- Notice must be given in writing by first class mail at the last known address of the individual (or next of kin for deceased individuals) or by electronic mail if the individual agrees to electronic notice and the agreement has not been withdrawn.
  - Notice may be provided in one or more mailings as information is available.
  - If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative, written notice may be made to the next of kin or personal representative.

Notice Requirements - Individuals

- Substitute notice:
  - Required if insufficient or only out-of-date contact information is available.
  - For fewer than 10 individuals, provide by an alternative form of written or telephone notice or other means.
  - For 10 or more individuals, provide by conspicuous posting for a period of 90 days on the home page of the covered entity's web site or a conspicuous notice in major print or broadcast media in geographic areas where the individuals are likely to reside, along with a toll-free number that remains active for at least 90 days.
  - Substitute notice is not required if there is insufficient or out of date contact information that precludes written notice to the next of kin or personal representative of a deceased individual.

Notice Requirements - Individuals

The notice must be written in plain language and include:

- A description of what happened, including the date of the breach and date of discovery, if known
- A description of the types of PHI involved (such as name, home address)
- Any steps the individual should take to protect herself from potential harm resulting from the breach
- A brief description of the entity's action to investigate the breach, mitigate harm to individuals, and prevent further breaches
- Contact procedures for individuals to ask questions, including a toll free telephone number, email address, web site, or postal address.

- If applicable, covered entity must comply with Civil Rights Act, Rehabilitation Act, and Americans with Disabilities Act, so notice may need to be in alternate languages or formats.

Notice Requirements - Media

Notice to prominent media outlets is required from breaches involving more than 500 residents of a single state or jurisdiction.

- The media notice must be provided in addition to the notice provided in writing to the affected individuals.
- The notice must include the elements described above for individual notice.
- What qualifies as prominent media outlet depends on the facts.

Notice Requirements - HHS

- Breaches involving 500 or more individuals must be reported immediately to HHS.
  - » Immediately means concurrently with the notification to the individuals.
  - » Note that this is not limited to 500 individuals in a particular state or jurisdiction
- Breaches involving under 500 individuals may be kept in a log and must be reported annually to HHS.
  - » Breaches maintained in a log must be reported no later than 60 days after the end of each calendar year.

Notice Requirements - Timing

- All notices must be made without unreasonable delay and no later than 60 calendar days after the discovery of the breach.
  - Delay for law enforcement. If a law enforcement official states to a covered entity or business associate that notice would impede a criminal investigation or cause damage to national security, the covered entity or business associate shall:
    - If the statement is made in writing, and specifies the time for which delay is required, delay the notice for that time frame, or
    - If the statement is oral, document the statement and delay notification no longer than 30 days from the date of the oral statement unless a written statement is submitted in that time frame.

Notice Requirements – Business Associates

- Business associates that access, maintain, retain, modify, record, store, destroy or otherwise hold, use or disclose unsecured PHI must provide notice of a breach of such PHI.
  - Notice is made to the covered entity, not the individual.
  - Breach is treated as discovered as of the first day on which the breach is known to the business associate, or, by exercising reasonable diligence, would have been known.
  - Business associate is deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or agent (using federal common law of agency) of the business associate.

Notice Requirements – Business Associates

- A business associate must provide notice to the covered entity without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.
- The notice must include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate, to have been accessed, acquired or disclosed, as well as any other available information the covered entity is required to provide in its notice as the information becomes available.

Burden of Proof

- In the case of a use or disclosure that violates the HIPAA privacy rule, the covered entity or business associate has the burden of demonstrating either
  - that all notifications were made, or
  - that the use or disclosure did not constitute a breach

Administrative Requirements

- Covered entities and business associates must develop and document policies and procedures, train workforce members on, and have sanctions for failure to follow these policies and procedures.
- Covered entities and business associates must also permit individuals to file complaints regarding such policies and procedures and refrain from intimidating and retaliatory acts.

Effective Date

- Notice requirements apply to breaches occurring on or after the date that is 30 days after the date of publication of the rule (September 23, 2009)
- HHS will not impose sanctions for failure to provide notifications of breaches that are discovered within 180 calendar days after the publication of the rule (before February 22, 2010).
- HHS will work with covered entities through technical assistance and voluntary corrective action to achieve compliance.

Preemption

- The breach notification requirements preempt contrary state security breach notification laws.
- State law is contrary only if a covered entity would find it impossible to comply with HIPAA and the state law or the state law stands as an obstacle to the accomplishment and execution of the objectives of HIPAA.
- Covered entities generally will be able to comply with HIPAA's breach notification requirements as well as state law requirements
- Preemption will be rare. Be sure to follow applicable state law.

FAEGRE & BENSON LLP

Gina Kastel
612.766.7923
gkastel@faegre.com