

Morgan Lewis

seminar
**HIPAA/HITECH
Breach Notification and Reporting**

Presenters

**Jessica Bernanke
Reece Hirsch
Georgina O'Hara**

October 28, 2009

HITECH Act

- The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is part of the American Recovery and Reinvestment Act (ARRA)
- The HITECH Act:
 - Through amendments to HIPAA, marks the beginning of a new era of health care privacy and security regulation and enforcement
 - Applies to HIPAA Covered Entities (“CEs”) and Business Associates (“BAs”)
 - Includes \$20 billion in funding for healthcare information technology projects

Major HIPAA Amendments in HITECH Act

- Extended the reach of the HIPAA Privacy and Security Rules to Bas
- Clarified “minimum necessary standard”
- Limited certain uses and disclosures of PHI
- Increased individuals’ rights with respect to PHI maintained in electronic health records (EHRs)
- Increased enforcement, of and penalties for, HIPAA violations
- ***Imposed breach notification requirements on HIPAA CEs and BAs***

Morgan Lewis

Recent Guidance re: HITECH

- HHS (applicable to CEs and BAs):
 - April 17 - guidance on the technologies and methodologies to secure health information
 - August 24 - interim final regulations regarding breach notification requirements (adds new subpart D to 45 CFR Part 164)
- Additional guidance and regulations are anticipated

The Dreaded Security Breach



Morgan Lewis

Pre-HITECH Breach Notification Requirements

- Prior to the HITECH Act, CEs were required to:
 - Mitigate any harmful effect of a use or disclosure of PHI in violation of its policies or HIPAA (Privacy Rule)
 - *Applies to electronic and paper PHI*
 - Adopt security incident procedures (Security Rule)
 - *Applies only to electronic PHI*
- But, there was no affirmative obligation to notify individuals or HHS of a breach

HITECH Act Breach Notification General Rule

- If security of “*Unsecured PHI*” is “*breached*,” CE must provide notice without unreasonable delay and within 60 days after “*discovery*” of breach to “*impacted individuals*,” media (in certain instances) and HHS
- Impacted Individuals are those whose “Unsecured PHI” has been or is reasonably believed by CE to have been accessed, acquired or disclosed as a result of a breach
- This rule creates a functional safe harbor, if the PHI is “secured,” there is no obligation to notify under HITECH
- Unlike many state laws, applies to breaches involving both electronic and paper records

What Is A Breach?

- The unauthorized acquisition, access, use or disclosure of Unsecured PHI
 - In a manner not permitted under the Privacy Rule (unauthorized)
 - Which compromises the security or privacy of the information
 - Except where unauthorized person “would not reasonably have been able to retain” the information

What Is A Breach?

- PHI is “compromised” if the breach poses a SIGNIFICANT RISK OF FINANCIAL, REPUTATIONAL OR OTHER HARM to individual
- To determine if PHI is “compromised,” CE should:
 - Conduct a fact specific risk assessment
 - Risk assessment should be documented
 - CE has burden of proof that no significant risk is posed
- If there is no significant risk of harm to individual, then no reportable breach has occurred

Breach Risk Assessment

- Risk assessment may take into account:
 - What type and amount of information was disclosed?
 - *Some forms of PHI may not raise risks such as financial fraud, medical identity theft or reputational harm*
 - *Just the name of a person receiving services at a hospital or enrolled in a health plan is less sensitive*
 - *Name of a person, in combination with SSN and other identifiers, or name of person treated for a specific illness is more sensitive*
 - Who used or received the information?
 - *Less risk if the recipient is a HIPAA covered entity*
 - Have steps been taken to mitigate the harm?
 - *Has the recipient of the PHI certified in writing that the information was returned or destroyed?*

Breach Risk Assessment - Example

- Example:
 - Laptop is lost or stolen, then recovered. Forensic analysis of the computer shows that information contained Unsecured PHI, but that information was not opened, altered, transferred or otherwise compromised
 - This breach likely does not pose a significant risk of harm to the individuals, and therefore, notification is probably not required

Three Breach Exceptions

- Breach Exception No. 1 (not a breach):
Unintentional acquisition, access or use of PHI by a workforce member or other person acting under authority of a CE or BA if:
 - Access made in good faith and within scope of employment or other professional relationship
 - The information was not further acquired, accessed, used or disclosed (which means not further used or disclosed in a way that is impermissible under Privacy Rule)
- Example: Office receptionist opens email sent by nurse by mistake. Receptionist recognizes she is not proper recipient, she notifies the nurse, deletes the email and does not further use or disclose the information (no breach)
- **Example: Office receptionist “snoops” in her friend’s medical records and reports back to her friend’s husband (breach)**

Three Breach Exceptions

- Breach Exception No. 2 (not a breach):
Inadvertent disclosure from an individual authorized at a CE or BA to another authorized person at the same CE, BA or organized health care arrangement, so long as:
 - The sender and recipient are “similarly situated” (both authorized to access PHI)
 - The information was not further acquired, accessed, used or disclosed (which means not further used or disclosed in a way that is impermissible under Privacy Rule)

Three Breach Exceptions

- Breach Exception No. 3 (not a breach):
Where CE or BA has a good faith belief that an unauthorized person to whom the PHI was disclosed would not have been able to able to retain the PHI
- Example: Plan sends EOB to wrong person, but the envelope is returned to the Post Office unopened
- For all three breach exceptions, the CE has the burden of proving (and documenting) that the exception applies

Summary Analysis of Breach

- To analyze if a breach has occurred, ask whether:
 1. There has been an impermissible use or disclosure of Unsecured PHI under the Privacy Rule
 2. The impermissible use or disclosure compromised the security or privacy of the Unsecured PHI
 - Is there a significant risk of financial, reputational or other harm to the individual?*
 3. The incident satisfies one of the three exceptions to breach
- Each step of the process should be documented

“Discovery” of Breach

- A breach is “**discovered**” as of the first day that it is known (or reasonably should have been known) to the CE or BA (not when the “breach risk assessment” is completed)
- The CE or BA has knowledge of the breach on the day that any employee, workforce member, officer or other agent has such knowledge (except for the individual who committed the breach)
- Discovery starts the time period for providing notice

What is Unsecured PHI?

- PHI not secured through use of a technology or methodology specified by HHS as rendering the information unusable, unreadable or indecipherable to unauthorized persons
- HHS has identified certain encryption and destruction technologies and methodologies that must be implemented to meet this standard
- The Security Rule requirements may be met without “securing” PHI – encryption is still an “addressable specification”

Encryption – General Requirements

- “Secure” PHI must be encrypted at rest, in use and in transmission
- Encryption must include "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 any such process or key that might enable decryption must not be breached
- Encryption keys and decryption tools need to be stored on a device or at a location that is separate from the data that they encrypt or decrypt

Encryption – Specific Guidance

- For data at rest: encryption consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*
- For data in motion: encryption consistent with:
 - NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*
 - NIST Special Publications 800-77, *Guide to IPsec VPNs*
 - NIST Special Publications 800-113, *Guide to SSL VPNs*
 - Other processes that are Federal Information Processing Standards (FIPS) 140-2 validated

Encryption vs. Access Control

- Firewalls and access controls, such as password protection, are reasonable and appropriate safeguards under the Security Rule
- HOWEVER, they are no substitute for encryption if a CE is seeking to ensure that it is not required to notify in the event of a breach

Security Guidance – Destruction

- Media on which PHI is stored or recorded must be destroyed:
 - Paper, film or other hard copy media must be shredded or destroyed such that PHI cannot be read or otherwise reconstructed
 - Electronic media must be cleared, purged or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*

Document Destruction vs. Redaction

- Redaction of PHI is not an acceptable alternative to destruction of paper PHI for purposes of “securing” PHI under the HITECH functional safe harbor

Notice – Timing and Recipients

- **To Impacted Individuals:** Written notice must be provided to individuals, without unreasonable delay and in no case later than 60 days after discovery, by first class mail to last known address. Email notice is only permitted if the individual agrees to it
 - Don't assume that CEs have 60 days to notify – it's an outer limit
 - CEs have burden of demonstrating timing was appropriate (and justifying any delay)
 - CEs may delay notification while they investigate the breach, but investigation can't take an unreasonable amount of time.
 - If information about the breach trickles in, CE can send multiple notices

Notice – Timing and Recipients

- Special Delivery Rules:
 - If CE lacks contact information for less than 10 individuals, it can notify by phone, email or other means
 - If CE lacks contact information for 10 or more people, it must provide substitute notice:
 - *By conspicuous posting on website for 90 days, OR*
 - *By conspicuous notice to major print or broadcast media in geographic area where individuals reside*
 - *In either case, must provide toll-free number for at least 90 days*

Notice – Timing and Recipients

- Special Delivery Rules (con't):
 - If there is urgency due to possible imminent misuse, CE may provide notice via phone or other means. This notice is in addition to (not in lieu of) regular written notice
 - For minors or individuals who lack legal capacity, notice may be sent to parent, guardian or personal representative
 - For deceased persons, notice must be sent to personal representative or next of kin (if known)
 - If a law enforcement official determines that notification would impede a criminal investigation or damage national security, notification may be delayed

Notice – Timing and Recipients

- **To the Media:** If breach involves more than 500 impacted individuals in state or jurisdiction, notice must be provided through prominent media outlets
 - This is in addition to written notice to impacted individuals
 - This notice must be provided in same time frame, and have same content as notice to impacted individuals

Notice – Timing and Recipients

- **To HHS:**
 - If breach involves more than 500 impacted individuals, CE notifies HHS at same time as individuals and HHS identifies CE on its website
 - If breach involves less than 500 impacted individuals, CE logs the breach and provides an annual log to HHS within 60 days of the end of the calendar year
 - HHS website contains forms to report breaches at: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>

BAs and Timing of Breach Notification

- BAs must notify CEs of any breach of which they become aware without unreasonable delay but no later than 60 days
 - Notice must identify each affected individual (to extent possible)
 - Notice must provide any other information CE may need to include in its notice to individuals
 - BA is not required to notify individuals
- But, notification obligations may be shifted to BAs through business associate agreements

BAs and Timing of Breach Notification

- If a BA is acting as an agent of a CE, then the BA's discovery of the breach will be imputed to the CE
 - 60-day timeframe for notification begins for CE
- If the BA is acting as an independent contractor of the CE (i.e., not an agent), then the CE must notify within 60 days of receiving notification of breach from the BA
- Federal common law of agency will govern whether a BA is an agent of a CE
- CEs should clarify timing of notification by specifying time frame in business associate agreement (but, that may not change legal "agent" status)

Content of Notice

- Brief description of facts surrounding breach
- Type of Unsecured PHI involved
- Steps individuals should take to protect themselves
- Brief description of what CE is doing to investigate and mitigate
- Contact information for inquiries
- More specific than most state laws, but not unreasonable

Content of Notice

- Notice must be in plain language
 - At appropriate reading level
 - No confusing, extraneous information

Administrative Requirements

- Regulations also impose administrative requirements on CEs with respect to breach notification, including:
 - Training for workforce members
 - Process for filing complaints
 - Sanctions for failure to comply with policies
 - Refrain from intimidating or retaliatory acts
 - IMPLEMENT/UPDATE POLICIES AND PROCEDURES

Effective Date for Breach Provisions

- Notification required for breaches discovered 30 days after publication of regulations (September 23, 2009)
- HHS has decided to not impose sanctions for failure to notify of breaches discovered during the 180 days following publication of the regulations (mid-February 2010)
- HHS provides little opportunity for industry comment

HITECH Cost Benefit Analysis

- As a first step, perform cost/benefit analysis to determine whether to operate within the functional safe harbor:
 - **What is the likelihood of a reportable breach?**
 - *How much PHI is maintained on site? Healthcare providers have a lot, by employer plan sponsors may have very little.*
 - *What is your history of breaches? How many has your organization experienced? How many individuals have been impacted?*
 - **What is the cost/burden of upgrading your technology to “secure” PHI?**
 - **What harm would your organization suffer if it had to report a breach to individuals? to HHS? to the media?**

HITECH and State Breach Laws

- HITECH Act reflects growing concerns about medical identity theft
 - California broadened its breach notice law to apply to medical information
- HHS notes that contrary state laws will be preempted by HITECH breach notification provisions
- HHS interprets HIPAA preemption provisions saving more stringent state laws as not applicable to breach provisions
- In general, ERISA covered health plans do not need to comply with state privacy laws due to ERISA preemption

HITECH and State Breach Laws

- HHS believes covered entities can comply with both HITECH and state breach laws
- In most cases, a single notice is sufficient
- If state law requires additional content elements in a notice, include them
- Additional state law requirements will still apply (like notifying specific state agencies)

Increased Enforcement Mechanisms

- Increased HHS Audits
- “Willful Neglect” Standard (Effective Feb. 2011)
- Enforcement by State Attorneys General (Effective Immediately)
- Mechanism for Individual Compensation – would incentivize complaints, a qui tam-like process (Effective on or after Feb. 2012 regs issue)
- Annual Report to Congress
- HIPAA and HITECH still do not provide for a private right of action

Increased Tiered Penalties

- **Tier 1:** If person is not aware of the violation (and would not have known with reasonable diligence), penalty is at least \$100/violation, not to exceed \$25,000 for all violations of the same requirement in the same calendar year
- **Tier 2:** If violation is due to “reasonable cause” (but not willful neglect), penalty is at least \$1,000/violation, not to exceed \$100,000 for all violations of the same requirement in the same calendar year
- **Tier 3:** If violation is due to willful neglect and is corrected in 30 days, penalty is at least \$10,000/violation, not to exceed \$250,000 for all violations of the same requirement in the same calendar year.
- **Tier 4:** If violation is due to willful neglect and is not corrected in 30 days, penalty is at least \$50,000/violation, not to exceed \$1.5 million for all violations of the same requirement in the same calendar year.

Increased Tiered Penalties

- Effective immediately, except “Willful neglect” provisions not applicable until February 2011
- HITECH requires all civil money penalties collected to be transferred to OCR for purposes of enforcing the Privacy and Security Rules

Most Common Mistakes In Security Breach Response

- Understand whether you are legally obligated to notify
 - Don't overreact
 - Can't “unring the bell” once a notification letter has been sent.
- Remember that state breach notification laws differ (ERISA generally preempts state privacy laws with respect to ERISA covered plans)



Understand The Notification Triggers

- Is the company legally required to notify under applicable breach notification laws?
- Understand the triggers
 - Is “personal information” involved?
 - Is “Unsecured PHI” involved?
 - Has a “security breach” actually occurred?
 - Varying causation standards under state laws:
 - *Is there a “reasonable belief” that information has been acquired by an unauthorized person (California)?*
 - *Is there a “likelihood of harm” (Delaware)?*
 - *Is there a “significant risk of harm”? (HITECH Act)*

Common Incident Response Mistakes

- In the heat of a crisis, organizations often forget that they adopted a security incident response plan
- If regulators or plaintiffs in a class action charge that you acted unreasonably, being able to demonstrate that you followed a reasonable security incident response plan is a good way to show otherwise



Failing to Coordinate With Law Enforcement

- Consider whether it's appropriate to notify law enforcement
 - Choose the right agency:
 - *Local high tech crimes task force*
 - *FBI*
 - *Secret Service*
 - *National Infrastructure Protection Service*
 - Don't use a half-hearted law enforcement investigation as an excuse to delay notification!

Other Common Incident Response Mistakes

- Failure to train your workforce to spot and report a security breach immediately
- Failure to require prompt security breach notification in agreements with vendors/agents
- Organize your incident response team in advance so that you're prepared to respond quickly

Incident Response Plans

- CE should have incident response plans. To be effective those plans should:
 - **Establish an incident response team with representatives from all key areas of the organization (Compliance, Legal, HR, PR, investor relations, IT, etc.)**
 - **Identify necessary external resources in advance (forensic IT consultant, third party administrator, mailing vendor, call-center operator, credit monitoring service)**
 - **Provide for training of rank-and-file personnel to recognize and report security breaches**
 - **Outline media relations strategy and point person**
 - **ENSURE THAT THE ORGANIZATION CAN RESPOND QUICKLY TO A BREACH AND NOT LEARN ON THE FLY!**

Contact Information

- **Jessica Bernanke (Washington, DC)**
 - 202.739.5447, jbernanke@morganlewis.com
- **Reece Hirsch, CIPP (San Francisco)**
 - 415.442.1422, rhirsch@morganlewis.com
- **Georgina O'Hara (Philadelphia)**
 - 215.963.5188; go'hara@morganlewis.com

Disclaimer

- This communication is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship