



HIPAA and the HITECH Act Privacy and Security of Health Information in 2009

**Marc J. Zwillinger
Rebecca C. Fayed**

Your Speakers



Marc J. Zwillinger

Chair of Sonnenschein's Internet, Communications and Data Protection Group (“ICDP”)



Rebecca C. Fayed

Leading expert on HIPAA privacy and security issues

AGENDA

- HITECH Act's Breach Notification Requirements
- FTC Regulations for PHR vendors
- Avoiding the HITECH Act's Breach Notification Requirement - Securing PHI
- HITECH Act's Changes to the HIPAA Privacy and Security Rules
 - Expanded Applicability to Business Associates
 - Limitations on the Use and Disclosure of PHI
 - Additional Individual Rights
 - Increased Penalties and Enforcement

HITECH Act Breach Notification Requirements

Breach Notification Provisions in the HITECH Act

- Before the amended CA breach statute took effect on 01/01/09, only Arkansas included medical information in the definition of “personal information” triggering breach notification obligations.
- Breaches of medical information that did not involve financial information often went unreported.
- 2008 – California amended statute to include both “medical information” and “health insurance information”
- HITECH Act imposes breach notification requirements on all HIPAA-covered entities and business associates.
- Effective date – HHS required to issue interim final regulations NLT 180 days after enactment (August 16, 2009), which will become effective NLT 30 days after publication (Sept. 15, 2009).

Breach of unsecured PHI:

- Unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of PHI, except in situations when an unauthorized person to whom the information is disclosed “would not reasonably have been able to retain such information.”
- ****Applies to both electronic and hard copy information.****

Notice of Breach

- Notice must be provided “without unreasonable delay” and no later than 60 days after breach is discovered.
- Via first-class mail unless the individual has specified a preference for email.
- Media notice – if PHI of more than 500 individuals in one state is breached, the entity must notify “prominent media outlets” in the state.
- HHS notice – covered entities must notify HHS of the breach:
 - More than 500 affected individuals – must notify HHS immediately.
 - Less than 500 affected individuals – may notify HHS via an annual log of events.
- Business associates must notify the covered entity of the breach.

Content of Notice:

- Description of facts about breach.
- Type of PHI involved.
- Steps individuals should take to protect themselves.
- What the covered entity is doing to investigate the situation and prevent future breaches.
- Contact information for individuals to ask questions.

HHS to Issue Rule on Breach Notification

- HHS required to issue interim final regulations no later than 180 days after the HITECH Act enactment (August 16, 2009), (effective 30 days after publication).
- HHS sought comments (were due May 21, 2009) on the following:
 - Based on complying with state breach notification laws, are there potential conflicts or other issues that should be considered when promulgating the federal breach notification requirements. (Yes, Massachusetts law)
 - Will entities have to send multiple breach notices given current obligations under state law and/or are circumstances under which the required federal notice also would not satisfy state breach notification laws. (Yes, Massachusetts law)
 - Are there any circumstances under which breach notification still will be required under state law if the information has been rendered secure based on federal requirements?
- What will final rule look like? Look to FTC rule on EHR. .

FTC Already Issued a Proposed Rule

- A vendor of personal health records who discovers a breach of security of unsecured PHR that is in a personal health record maintained or offered by such vendor must:
 - Notify each individual who is a U.S. resident whose unsecured information was acquired by an unauthorized person (within 60 days); and
 - Notify the FTC (within 5 business days if more than 500 people involved, or at the end of 12 months if fewer than 500 per incident).

Definitions

- *Breach of Security* = acquisition of information without the authorization of the individual.
- *Personal Health Record* = an electronic record of identifiable health information about an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.
- *PHR identifiable health information* = “individually identifiable health information” as defined in 42 U.S.C. 1320d(6) that is provided by or on behalf of the individual and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Who does rule apply to?

- First, examples: a web-based application that helps consumers manage medications; a website offering an online personalized health checklist; and a brick-and-mortar company advertising dietary supplements online.
- Second, PHR related entities include entities that are not HIPAA-covered entities and that offer products or services through the websites of HIPAA covered entities.
- Third, PHR related entities include non-HIPAA covered entities “that access information in a personal health record or send information to a personal health record.” Online applications through which individuals, for example, connect their blood pressure cuffs, heart rate monitors, to track results through their personal health records. Could also include an online medication or weight tracking program that pulls information from a personal health record.

Content of Notice

- Notice shall include:
 - A brief description of how breach occurred, including date of breach and discovery.
 - A description of the type of information involved in the breach.
 - Steps individuals should take to protect themselves from harm.
 - Description of what entity is doing to investigate breach and mitigate losses.
 - Contact information for questions, including a phone number, email address or postal address.

Key Aspects

- Vendor must demonstrate compliance.
- Can delay if law enforcement requests it.
- Third party vendor must notify PHR vendor.
- Notice must be given by first-class mail (or by email if the individual has provided express affirmative consent), unless emergency requires telephone or other means of more prompt notice.
- If you cannot reach 10 or more individuals directly, must use substitute notice through 6-month website posting or through major media.
- Must notify media in every State if 500 or more residents of that state are affected.

What is Acquisition?

- FTC provides important guidance on what constitutes unauthorized acquisition.
 - “Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition of such information.”
 - Access to information creates presumption of unauthorized “acquisition” but can be rebutted by proof that it could not have reasonably been acquired

Practical Guidance – What do I do now?

- Identify systems that have covered data.
- Secure your PHI – Encrypt or Destroy. (See next section)
- Evaluate existing privacy and security policies and procedures and assess whether current administrative, technical and physical safeguards are sufficient to protect the privacy and security of PHI.
- Adopt Incident Response plan with breach notification policy.
- Establish procedures and incident response team to respond to breach.
- Assign internal roles and responsibilities, and identify external vendors.
- Consider incident response insurance policies.

What about HIPAA? What Role Does it Play in Security Breaches?

- The HIPAA Privacy Rule requires covered entities to:
 - Mitigate – Must mitigate any harmful effects of unauthorized disclosure (police reports, notification).
 - Sanction – Must apply appropriate sanctions against employees who fail to comply with privacy and security policies and procedures.
 - Account for Disclosures – Unauthorized disclosures of PHI must be accounted for on accounting log.
- Other Compliance Efforts:
 - Training – Retrain employees.
 - Policies and Procedures – Evaluate effectiveness of and modify, if appropriate, policies, procedures and safeguards.
- In the event of a breach, likely that covered entities will receive a request from HHS-OCR and/or CMS asking for a description of the incident and details regarding the safeguards that were in place or have been put in place since the breach to protect the privacy and security of PHI.

Avoiding the HITECH Act's Breach Notification Requirement: Securing PHI

Avoiding Breach Notification: Securing Your PHI

- HITECH Act breach notification requirement applies only to the breach of unsecured PHI.
- HITECH Act required HHS to issue guidance specifying technologies and methodologies that would render PHI “unusable, unreadable, or indecipherable” to unauthorized individuals.
- If PHI is rendered “unusable, unreadable, or indecipherable” to unauthorized individuals, it is secure.
- The breach of secure PHI is not subject to the breach notification requirement.
- Avoid having to comply with the breach notification requirement by **SECURING** your PHI.

Avoiding Breach Notification: How to Secure PHI

- HHS issued guidance on April 17, 2009 setting forth an exhaustive list of what technologies and methodologies will render PHI secure.
- Technologies and Methodologies that will render PHI secure:
 1. Encryption.
 2. Destruction.
- Nothing else will render your PHI secure.

Avoiding Breach Notification: Encryption

- EPHI must be encrypted in accordance with 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 a meaning without use of a confidential process or key and such confidential process or key that might enable encryption has not been breached.”

Avoiding Breach Notification: Encryption Safe Harbors

- Valid processes for encryption of stored PHI include those consistent with NIST Special Publication (“SP”) 800-111, *Guide to Storage Encryption Technologies for End User Devices*, including (but not limited to) full disk encryption, volume encryption, virtual disk encryption, and file/folder encryption.
- Valid processes for encrypting PHI during transmission would be those complying with the requirements in Federal Information Processing Standard (“FIPS”) 140-2, including NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security Implementations*, 800-77, *Guide to IPsec VPNs*, or 800-113, *Guide to SSL VPNs*.
- For example, validated processes for symmetric key encryption include the Advanced Encryption Standard (“AES”), Triple-DES, and Skipjack algorithms.

Practically Speaking

- Compliance with NIST/FIPS Standard is not a simple checklist.
 - Each standard specifies means of compliance that may differ in particular situations.
 - Example: full disk encryption may be a valid way to secure data against third parties, but not against unauthorized insiders who share a laptop or computer with authorized users.
 - File/Folder encryption may be better way of ‘securing’ data in that scenario.

Avoiding Breach Notification: Destruction

- To comply with the destruction guidance, the media on which the PHI is stored or recorded must be destroyed in the following ways:
 - Hard copy media (such as paper and film) must be shredded or destroyed in such a way that PHI cannot be read or otherwise reconstructed.
 - Electronic media must be cleared, purged, or destroyed so that the PHI cannot be retrieved, consistent with the NIST SP800-88, *Guidelines for Media Sanitization*.

What to do now?

- Work with your Chief Information Officer or IT/IS Managers to determine whether you currently encrypt or have the capabilities to encrypt PHI.
 - The cost of encryption likely is less expensive than addressing a security breach.
- Review your medical record retention and destruction policies to confirm that data is being destroyed properly.
 - To reduce risk, do not retain medical records longer than necessary.

Changes to the HIPAA Privacy and Security Rules:

Applicability to Business Associates

HIPAA Applies to Business Associates?

- Prior to the HITECH Act
 - Not directly subject to HIPAA.
 - Reasonable Assurances in the form of a BA Agreement.
 - Liability limited to breach of contract.
- HITECH Act expanded the reach of the HIPAA Privacy and Security Rules.
- Effective February 16, 2010.

HIPAA Applies to Business Associates?

- HIPAA Security Rule
 - BAs must comply with the HIPAA Security Rule.
 - Conduct a security risk assessment.
 - Implement administrative, physical and technical safeguards.
 - Have policies and procedures in place to protect the security of PHI.

HIPAA Applies to Business Associates?

- HIPAA Privacy Rule
 - BAs still are NOT required to comply with the HIPAA Privacy Rule.
 - BAs must continue to provide reasonable assurances in the form of a BA agreement.
 - If a BA violates any provision of the BA Agreement, will be subject to the same civil and criminal penalties for HIPAA violations as covered entities.

Practical Effect

- Business associates will need to be revised to incorporate the new HITECH Act requirements.
 - Breach Notification Obligations
 - Compliance with Security Rule
 - New Penalties for Breaches
 - Changes to Individual Rights

Changes to the HIPAA Privacy and Security Rules:

Additional Limitations on the Use and Disclosure of PHI

Additional Limitations: Marketing

- Prior to the HITECH Act
 - Excluded from the definition of marketing are communications:
 1. That describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication;
 2. For treatment of that individual; or
 3. For case management, care coordination or to recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

Additional Limitations: Marketing

- HITECH Act placed limitations on the marketing exception.
- If payment received for making the communications, the communication is marketing, unless:
 1. The communication describes only a drug or biologic currently being prescribed for the individual and the amount of payment received for making the communication (if any) is reasonable in amount;
 2. The communication is made by the covered entity and the covered entity has received a valid HIPAA authorization from the individual to whom it is making the communication; or
 3. The communication is made by a business associate and is consistent with the terms of its business associate agreement with the covered entity.

Additional Limitations: Fundraising

- HHS required to issue a rule that requires all written fundraising communications to provide the recipient with an opportunity to opt out of any future fundraising communications.
- Different from the Privacy Rule, the HITECH Act now requires covered entities to treat an individual's election to opt out of fundraising communications as a revocation of authorization.

Additional Limitations: Minimum Necessary

- Privacy Rule requires covered entities to disclose only the minimum amount of PHI reasonably necessary to accomplish the purpose of the permitted use or disclosure of PHI.
- Criticized as one of the most vague and difficult-to-implement components of the Privacy Rule.
- HITECH Act requires HHS to issue guidance on the minimum necessary standard by August 17, 2010.
- Until HHS guidance issued: Use or disclose a limited data set, *to the extent practicable*, or if necessary, to the minimum necessary to accomplish the intended purpose.
- Just as difficult to implement?

Additional Limitations: Health Care Operations

- House and Senate bills originally required HHS to review the definition of health care operations and eliminate activities that could be conducted with deidentified health information or should require an authorization.
- This provision caused the most angst in the health care industry.
- Provision was NOT included in the final HITECH Act.
- The HITECH Act does not require the Secretary to review and modify the definition of health care operations.

Individual Rights: Accounting for Disclosures

- Privacy Rule currently excepts from the accounting requirement those disclosures of PHI made for purposes of treatment, payment and health care operations.
- HITECH Act eliminates TPO disclosure exception for disclosures made of an EHR.
- 3 Year Reporting Period vs. 6 Year Reporting Period
- Compliance Date:
 - January 1, 2014 - Covered Entities who began using EHRs prior to January 1, 2009.
 - January 1, 2011 - Covered Entities who acquire an EHR after January 1, 2009 (or the date they acquire the EHR thereafter).

Individual Rights: Restrictions on Disclosures

- Privacy Rule currently provides individuals with a right to request a restriction on a covered entity's use or disclosure of PHI for purposes of treatment, payment or health care operations purposes.
- Covered entities have no corresponding obligation to agree to that request.
- HITECH Act imposes a new obligation on covered entities to agree to a requested restriction if the disclosure is to a health plan for purposes of payment or health care operations *and* the PHI relates to a health care item or service for which the health care provider has been paid out of pocket in full.

Changes to the HIPAA Privacy and Security Rules:

Increased Enforcement and Penalties

Individual Rights: Increased Enforcement

- HHS-OCR enforces Privacy Rule; HHS-CMS enforces Security Rule.
- HITECH Act:
 - Requires HHS to formally investigate any complaint of a violation of HIPAA if a preliminary investigation indicates a possible violation due to willful neglect, and to impose civil penalties for these violations.
 - Allows state Attorneys General to bring civil actions in federal court on behalf of state residents if there is reason to believe that the interest of one or more residents has been threatened or adversely affected by a person who violates HIPAA.

Individual Rights: Increased Penalties

- HITECH Act created tiered approach to civil monetary penalties for violations of HIPAA.
 - If the person did not know (and by exercising reasonable due diligence would not have known) that he or she violated the law, the penalty shall be at least \$100 for each violation not to exceed \$25,000 for all such identical violations during a calendar year, but may be no more than \$50,000 for each violation not to exceed \$1.5 million for all such violations of an identical requirement or prohibition during a calendar year.
 - If the violation was due to reasonable cause and not to willful neglect, the penalty shall be at least \$1000 for each violation not to exceed \$100,000 for all such identical violations during a calendar year, but may be no more than \$50,000 for each violation not to exceed \$1.5 million for all such violations of an identical requirement or prohibition during a calendar year.
 - If the violation was due to willful neglect AND the violation was corrected, the penalty shall be at least \$10,000 for each violation not to exceed \$250,000 for all such identical violations during a calendar year, but may be no more than \$50,000 for each violation not to exceed \$1.5 million for all such violations of an identical requirement or prohibition during a calendar year.
 - If the violation was due to willful neglect and was not corrected, the penalty shall be at least \$50,000 for each violation not to exceed \$1.5 million for all such violations of an identical requirement or prohibition during a calendar year.
- **INCREASED PENALTIES IN EFFECT NOW.**

DISCLAIMER

- These materials should not be considered as, or as a substitute for, legal advice and they are not intended to nor do they create an attorney-client relationship. Because the materials included here are general, they may not apply to your individual legal or factual circumstances. You should not take (or refrain from taking) any action based on the information you obtain from these materials without first obtaining professional counsel. The views expressed do not necessarily reflect those of the firm, its lawyers, or clients.

Sonnenschein
SONNENSCHN NATH & ROSENTHAL LLP