HITECH Act Health Data Security & Breach Update

Cynthia Marcotte Stamer
Partner
Curran Tomko Tarski LLP
2001 Bryan Street, Suite 2050 Dallas, Texas 75201
Direct: 214.270.2402 Mobile: 469.767.8872
CStamer@CTTLegal.com
www.CTTLegal.com
©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
About Cynthia Marcotte Stamer

Curran Tomko and Tarski LLP Health Care & Employment Practice Leader and Partner Cynthia Marcotte Stamer is nationally known for her work, publications and presentations on privacy and security of health and other sensitive information in health and managed care, employment, employee benefits, financial services, education and other contexts. She continuously advises employers, health care providers, health insurers and administrators, health plan sponsors, employee benefit plan fiduciaries, schools, financial services providers, governments and others about privacy and data security, health care, insurance, human resources, technology, and other legal and operational concerns.

Chair of the ABA RPTE Employee Benefit & Other Compensation Committee, Vice President of the North Texas Health Care Compliance Professionals Association, Past Chair of the ABA Health Law Section Managed Care & Insurance Section and the former Board Compliance Chair of the National Kidney Foundation of North Texas, Ms. Stamer has more than 20 years experience advising clients about health and other privacy and security matters for health care providers, health plans and employers.

A popular lecturer and widely published author on privacy and data security and other related health care and health plan matters, Ms. Stamer is the Editor in Chief of the forthcoming 2010 edition of the Information Security Guide to be published by the American Bar Association Information Security Committee in 2010, as well as the author of “Protecting & Using Patient Data In Disease Management: Opportunities, Liabilities And Prescriptions,” “Privacy Invasions of Medical Care-An Emerging Perspective,” “Cybercrime and Identity Theft: Health Information Security Beyond HIPAA,” and a host of other highly regarded publications. Ms. Stamer also publishes and speaks extensively on health and managed care industry privacy, data security and other technology, regulatory and operational risk management matters. Her insights on health care, health insurance, human resources and related matters appear in the Atlantic Information Service, Bureau of National Affairs, World At Work, The Wall Street Journal, Business Insurance, the Dallas Morning News, Managed Healthcare, Health Leaders, and a many other national and local publications. To arrange for training or for additional information about Ms. Stamer, her experience, involvements, programs or publications, see cynthiastamer.com or contact Ms. Stamer at (214) 270.2402 or cstamer@CTTLegal.com.
THE FINE PRINT

This presentation and any materials and/or comments are training and educational in nature only. They do not establish an attorney-client relationship, are not legal advice, and do not serve as a substitute for legal advice. No comment or statement in this presentation or the accompanying materials is to be construed as an admission. The presenter reserves the right to qualify or retract any of these statements at any time. Likewise, the content is not tailored to any particular situation and does not necessarily address all relevant issues or be updated to reflect the current state of law in any particular jurisdiction or circumstance as of the time of the presentation. Parties participating in the presentation or accessing of these materials are urged to engage competent legal council for consultation and representation in light of the specific facts and circumstances presented in their unique circumstance.

Circular 230 Compliance. The following disclaimer is included to ensure that we comply with U.S. Treasury Department Regulations. Any statements contained herein are not intended or written by the writer to be used, and nothing contained herein can be used by you or any other person, for the purpose of (1) avoiding penalties that may be imposed under federal tax law, or (2) promoting, marketing or recommending to another party any tax-related transaction or matter addressed herein.*
HIPAA Privacy & Data Security

- Apply To
  - Heath Care Providers
  - Health Plans
  - Health Care Clearinghouses
  - 2/17/2010 Business Associates
Health Information Technology for Economic and Clinical Health (HITECH) Act

- Part of the Stimulus package known as the American Recovery and Reinvestment Act 2009 (HITECH Act or ARRA)

- HITECH Act Amends HIPAA In Several Respects
HITECH Act Amends HIPAA

- Clarifies that HIPAA’s criminal sanctions apply to employees or other individuals that wrongfully use or access PHI held by a covered entity;
- Increases criminal and civil penalties for HIPAA Privacy Rules violators;
- Allows State Attorneys General to bring civil damages actions;
- Broadens the applicability of the HIPAA’s Privacy Rules and penalties to include business associates;
- Adds specific “breach notice” obligations upon these entities to provide certain notifications in the event the security of Protected Health Information (“PHI”) is breached;
- Modifies certain HIPAA use and disclosure and accounting requirements;
- Prohibits sales of PHI without prior consent;
- Tightens certain other HIPAA restrictions on uses or disclosures;
- Tightens certain HIPAA accounting for disclosure requirements;
- Clarifies the definition of health care operations to exclude certain promotional communications; and
- Expands the Business Associate Agreement requirements
HITECH Act Impending Changes

2/17/2010 Effective Dates
HITECH ACT
Business Associates Subject To Privacy & Security Rules & Related Penalties

- Originally HIPAA provisions and civil and criminal penalties only applied to health care providers, health plans and health care clearinghouses ("covered entities")
- Business associates subject to HIPAA provisions in the same manner as other covered entities
- Civil and criminal sanctions for violations of the Privacy and Security Standards in the same manner that they apply to covered entities that violate such security provision.
HITECH Act
Individual Request To Restrict Access

- CE/BA must honor a request by a subject for a restriction on uses or disclosures of PHI if:
  - Except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and
  - The PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.
  - A covered entity, with respect to the use, disclosure, or request of PHI, must limit the PHI to the extent practicable to the limited data set or, if needed by the covered entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively.
By August 17, 2010, OCR must define “minimum necessary.”

Pre-August 17, 2010, covered entities remain responsible for determining what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.
HITECH Act New Conditions on Health Care Operations/Marketing

CE/BA communication about product or service ≠ health care operations purpose unless:

- Made for one of the following purposes:
  - To describe a health-related product or service (or payment for such product or service) provided by/included in benefit plan of CE making communication, including those about entities participating in provider network; replacement/ enhancements of health plan; and health-related products or services available only to a health plan enrollee that add value to but not part of benefit plan
  - For treatment of the individual; or
  - For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

- Either:
  - The communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication; and
    - Any payment received by such covered entity in exchange for making a communication is reasonable in amount as to be defined by the Regulations;
    - Each of the following conditions apply--
      - The communication is made by the covered entity; and
      - The covered entity making such communication obtains from the recipient of the communication a valid authorization with respect to such communication; or
  - Each of the following conditions apply:
    - The communication is made by a business associate on behalf of the covered entity; and
    - The communication is consistent with the written contract other allowable written arrangement between such business associate and covered entity.
OCR must issue rules providing any written fundraising communication that is a healthcare operation shall provide an opportunity for the recipient of the communications to elect not to receive any further such communication, in a clear and conspicuous manner.
When an individual elects not to receive any further such communication, election revokes authorization previously provided to allow the communications.
Presently CE not required to account for uses & disclosures for treatment, payment or operations purposes.

The HITECH Act requires CE/BA using electronic health records to account for disclosures for treatment, payment and operations purposes during the three years prior to the date on which the accounting is requested.
HITECH Act
CE/BA Using Electronic Health Record Must Provide Individuals Access

- If CE uses/maintains EHR with PHI in an electronic format:
- The individual has right to obtain materials directly or to direct CE to transmit that such copy directly to an entity or person designated by individual, provided that any such choice is clear, conspicuous, and specific; and
- Fee CE may charge to provide copy of such information (or a summary or explanation of such information) in an electronic form can’t exceed CE’s labor costs in responding to the request.
In response to request for an accounting, CE using EHRs must provide an accounting for disclosures of PHI for treatment, payment and by providing either:

- An accounting of the uses and disclosures made by all business associates; or
- A list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address) and a business associate included on a list must provide an accounting of disclosures made by the business associate upon a request made by an individual directly to the business associate for such an accounting.
Effective Date

- Covered entities having an electronic health record as of January 1, 2009, the duty to account for treatment, payment and operations disclosures will apply to disclosures of protected health information from the record after December 31, 2014.

- Covered entities acquiring electronic health records after January 1, 2009 must account for treatment, payment and operations disclosures made by the covered entity from such record on and after the later of:
  - January 1, 2011; or
  - The date that it acquires an electronic health record.

- OCR may delay effective dates up to 2 years.
HITECH Act
Electronic Health Records & Protected Health Information Sale Prohibited

➢ CE/BA shall not directly or indirectly receive remuneration in exchange for any PHI without valid authorization that includes a specification that PHI can be further exchanged for remuneration by the entity receiving protected health information of that individual unless the purpose:
  √ Exchange is for public health activities
  √ For the treatment of the individual, subject to any OCR regulation promulgated to prevent protected health information from inappropriate access, use, or disclosure
HITECH Act
Exceptions To Electronic Health Records &
Protected Health Information Sale Prohibited

- Research and the price charged reflects the costs of preparation and transmittal of the data for such purpose.
- Certain specified health care operations;
- For remuneration that is provided by a covered entity to a business associate for activities involving the exchange of PHI that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement;
- To provide individual with a copy of the individual's protected health information; and
- Purpose otherwise allowed by OCR Regulations as similarly necessary and appropriate as the exceptions provided above.
Where CE allowed to sell, CE/BA must limit the PHI to the extent practicable to the limited data set or, if needed by the CE, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively.
HITECH Act
De-Identified PHI Guidance Required

By February 17, 2010, HHS must issue guidance on how best to implement the requirements for the de-identification of PHI under Privacy Rule § 164.514(b)
HITECH Act

HHS Must

Study definition of ‘psychotherapy notes’ and issue regulations to revise such definition

Report to Congress Annually
HITECH Act Amends HIPAA Penalties

- To specify that any violation by a covered entity is subject either to enforcement and penalties under section 1176 (Civil Penalties) and 1177 (Criminal Penalties) of the Social Security Act
- To provide that the civil penalty of up to $100 per day under Social Security Act § 1176 does not apply where criminal sanctions have been imposed for a violation under criminal penalties provisions of Social Security Act § 1177
HITECH Act Increases HIPAA Civil Penalties

- Requires OCR to formally investigate any complaint of a violation if a preliminary investigation of the facts of the complaint indicate such a possible violation due to willful neglect
- Harmed Individuals To Get Share Of Penalties

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
HITECH Act  Increased HIPAA Civil Monetary Penalties Effective February 17, 2009

- If violator did not & could not by exercising reasonable diligence know violating, a penalty for each such violation of at least $100 for each such violation, except total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $25,000; and $50,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000
- Where the violation due to reasonable cause and not to willful neglect, a penalty for each violation of an amount that is at least $1,000 for each such violation, except that:
  - The total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $100,000 and
  - The amount described in this subparagraph is $50,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000
- Where the violation was due to willful neglect and the violation is timely corrected, a penalty in an amount that is at least $10,000 for each such violation except that the total amount imposed on the person:
  - For all such violations of an identical requirement or prohibition during a calendar year may not exceed $250,000; and
  - Not to exceed $50,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000
- Where the violation is due to willful neglect and is not corrected, a penalty of $50,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000
- In determining the amount of a penalty, HHS Secretary shall base such determination on the nature and extent of the violation and the nature and extent of the harm resulting from such violation.

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Enforcement Through State Attorneys General For Post February 17, 2009 Violations

State Attorney General, may bring a civil action for civil damages of and to enjoin further violations on behalf of residents of the State if:

- It has reason to believe that an interest of one or more of the residents of that State has been or is threatened or adversely affected by any person who violates the Privacy & Security Rules;
- An action to impose a civil money penalty action could be instituted by HHS under the civil monetary provisions of HIPAA
- The State Attorney General gives prior written notice of any action and copy of its complaint to HHS (or if prior notice unfeasible, immediately upon instituting such action. HHS will have the right to intervene in the actions, to be heard on all matters arising therein; and to file petitions for appeal
- If HHS has instituted an action with respect to a specific violation, a State attorney general cannot bring an action against the person with respect to such violation during the pendency of that action.
Enforcement Through State Attorneys General For Post February 17, 2009 Violations

- State Attorney General recoveries may include:
  - Statutory Damages equal to the sum of the number of violations multiplied by 100 up to a maximum of $25,000 per calendar year, reduced as the Court determines appropriate considering the factors HHS may consider in determining the amount of a civil money penalty.
  - If the Attorney Generally is successful, the court in its discretion may award costs plus attorneys fees to the State.

- The power to sue under HIPAA does not prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State.

- Venue over the State Attorney General’s HIPAA enforcement action lies in any district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

- Process may be served in any district in which the defendant is an inhabitant or maintains a physical place of business.

- Provisions effective since February 17, 2009.
Connecticut AG Brings 1st AG HIPAA Suit Against Heath Net

Connecticut Attorney General’s Office

Press Release

January 13, 2010


The suit was filed in the U.S. District Court for the District of Connecticut in Bridgeport.

Blumenthal said that the lawsuit is the first in Connecticut to be filed under HIPAA.

“Today, this lawsuit is historic — involving an unregulated health care provider that has placed the privacy of its patients at risk,” Blumenthal said.

The suit seeks to stop the practices of Heath Net and to force the company to comply with HIPAA.

The lawsuit is the first in Connecticut to be filed under HIPAA.

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
HITECH Act HIPAA Data Breach
Effective September 23, 2009

HIPAA covered entities/business associates required to provide specified notifications within a reasonable time no longer than 60 days after know or should know a post September 23, 2009 breach of unsecured protected health information posing a significant financial, reputational or other risk to the subject of the information
Breach Notice Only Applies to Unsecured Protected Health Information

Covered entities and business associates that implement the specified technologies and methodologies with respect to protected health information are not required to provide notifications in the event of a breach of such information, i.e., the information is not considered “unsecured” in such cases.
Breach Notice Rules vs. Security Rules

- Breach Notice: Impermissible Use of Any PHI In Violation of HIPAA If Results In Actual Significant Risk To Individual

- Security: Failure To Protect, Regardless of Risk, Electronic PHI In Accord With Regulations
“Unsecured Protected Health Information”
Applies To PHI, Not Just EPHI

Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 on the HHS Web site.

45 C.F.R. § 164.402(1)
HITECH Act Breach Guidance

Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information, available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Secured PHI

- Protected health information is rendered unusable, unreadable, or indecipherable to unauthorized use or access as required by HHS

- Guidance originally published on April 17, 2009, and later published in the Federal Register on April 27, 2009 at 74 FR 19006; updated in August 24 guidance

45 C.F.R. § 164.402(1)
“Secured PHI”

Secured if protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

• Encryption

• Destruction

• Limited data set ≠ secured but special rules

45 C.F.R. § 164.402(1)

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Secured PHI Via 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. See, 45 CFR 164.304, definition of “encryption.”

- To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.
Secured PHI Via Encryption

Encryption processes tested by the National Institute of Standards and Technology (NIST) judged to meet this standard are


Secured PHI Via Destruction

The media on which the PHI is stored or recorded 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; Redaction is specifically excluded as a means of data destruction.

- Electronic media have been cleared, purged, or destroyed such that the PHI cannot be retrieved consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization available at http://www.csrc.nist.gov/
“the acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information” not otherwise excluded by Regulations

45 C.F.R. § 164.402

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Compromises The Security Or Privacy Of The Protected Health Information

- Means “poses a significant risk of financial, reputational, or other harm to the individual”
- A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

45 C.F.R. § 164.402(1)
Breach Excludes

- Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such 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 not permitted under subpart E of this part.

- Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

- A disclosure of protected health information where a 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 such information.

45 C.F.R. § 164.402(2)
Following the discovery of a breach of unsecured protected health information, Covered Entity must notify the following of information specified in regulations:

- Individuals
- HHS
- Attorney General In State
- Media
Required Notifications: Big Picture

Regulations specify required contents, methods of delivery and other requirements for providing notice.
Breaches Treated As Discovered

A covered entity shall be deemed to have knowledge of a breach if such 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 of the covered entity (determined in accordance with the federal common law of agency)

45 C.F.R. § 164.404(a)(2)

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Individual Notice

- Generally Required To Individual By 1st Class Mail

- Special Rules For Substitute Notice Under Certain Circumstances
Notification to Media

- If breach involves > 500 residents of a State or jurisdiction, a covered entity must notify prominent media outlets serving the State or jurisdiction without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

45 C.F.R. § 164.406
Notification to HHS Secretary

- Breaches involving 500 or more individual, provide the notification to HHS contemporaneously with the individual notice in manner specified on the HHS Web site.

- Breaches involving less than 500 individuals, maintain a log or other documentation of such breaches and provide the notification to HHS for breaches occurring during the preceding calendar year within 60 days after the end of each calendar year in the manner specified on the HHS Web site.

45 C.F.R. § 164.408

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Notification By Business Associate

- A business associate must notify Covered Entity of breach without unreasonable delay and no later than 60 calendar days after breach following the discovery of a breach of unsecured protected health information. Breaches treated as discovered.

- Breach discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate.

- A business associate 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 other agent of the business associate (determined in accordance with the federal common law of agency).

- **Content of notification** to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach and any other available information that the covered entity is required to include in its individual notification.

45 C.F.R. § 164.410

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
If a law enforcement official states to a covered entity or business associate that a required breach notification, notice, or posting would impede a criminal investigation or cause damage to national security, Covered Entity/Business Associate shall:

- If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

- If statement made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement submitted during that time.

45 C.F.R. § 164.412
Law enforcement official

An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

- Investigate or conduct an official inquiry into a potential violation of law; or
- Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

45 C.F.R. § 164.103
Administrative Requirements

A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart, e.g.:

- Must train all members of its workforce on the policies and procedures and document the provision of this training as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity. This includes a requirement to update training of each member of the covered entity’s workforce whose functions are affected by a material change in the policies or procedures due to change in law within a reasonable period of time after the material change becomes effective.

- Must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures and document all complaints received, and their disposition, if any.

- Must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures and must document the sanctions that are applied, if any.

- Must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.
Administrative Requirements

A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart, e.g.:

- Must refrain from intimidating or retaliatory acts. Under this prohibition, covered entity or business associate may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by the Privacy Rule including the filing of a complaint under this section;

- Must not require individuals to waive their rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

- Must implement policies and procedures with respect to protected health information that are reasonably designed to comply with the standards, implementation specifications, or other requirements of the Privacy rule taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance.

- Must change its policies and procedures as necessary and appropriate to comply with changes in the law by promptly documenting the revised policy or procedure and updating its notice of privacy practices

- Must maintain the required policies and procedures in written or electronic form; for six years from the date of its creation or the date when it last was in effect, whichever is later.

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Burden Of Proof

When a use or disclosure in violation of subpart E occurs, the covered entity or business associate, as applicable, has the burden of demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach.

45 C.F.R. § 164.414(b)

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Breach Notification Analysis In Plan

Conduct & Document Assessment

- Breach of Privacy Rule?
- Unsecured PHI? If no, Privacy Rule Analysis Only
- Compromise Privacy/Security Pose Significant Risk Of Financial, Reputational, or Other Harm To Individual? If no, Privacy Rule but no breach notice obligation

- Document Analysis
- Document Corrective Action
Breach Notification-SOX For CE/BAs

Must Effectively Operationalize HIPAA Compliance Practices, Monitoring & Reporting
HIPAA Protects “Protected Health Information”

- Information relates to:
  - past, present, or future mental or physical condition;
  - the provision of health care; or
  - payment for the provision of health care

- Created by a:
  - Provider
  - Plan
  - Clearinghouse
  - Employer

- Identifies the Individual or creates a reasonable basis to believe that the individual’s identity may be revealed

- Not de-identified or otherwise excluded
Privacy Rule: A covered entity cannot use or disclose protected health information (PHI) except as permitted or required by the final Privacy Standards.

Security Rule: Covered entities receiving, maintaining or transmitting electronic PHI must safeguard data against improper use, access, disclosure or destruction.

Privacy Rights: Covered entities must honor specified individual HIPAA Privacy rights.

Privacy Officer & Compliance Plan Requirements.

Breach Notice Rules For Post 9/22/09 Breaches of Unsecured PHI.
CE/Workforce Can’t Use, Access Or Disclose PHI Except As Permitted Or Required By The Final Rule Exception As:

- √ Treatment, Payment, & Operations
- √ In An Emergency;
- √ For Law Enforcement Purposes;
- √ For Public Health Activities;
- √ To Report Abuse, Neglect, Or Domestic Violence
- √ Individual Involved In Treatment

- √ To provide information to coroners, funeral directors, etc;
- √ For cadaveric organ, eye, or tissue donation purposes; and
- √ Research or marketing purposes subject to conditions
- √ For use by business associates
Privacy Standard Mandates

Exceptions Only Allow Use/Disclosure Only If CE Meets Requirements:

- √ Allowed By Privacy Rule
- √ Adopt Written Privacy Practices Allowing
- √ Discloses In Privacy Notice
- √ Restricts To Minimum Necessary Except For Treatment, Payment, Operations, To Individual Or Authorized
- √ Verification
- √ Accounting & Other Individual Rights
- √ Documentation and Record Retention
- √ Meets All Other Applicable Restrictions For Exception

©2009-2010 Cynthia Marcotte Stamer.  All rights reserved.
Privacy Rule Mandates

Covered Entity Must:

- Have Complaint Process
- Investigate All Complaints, Apply Appropriate Sanctions Against Violators, And Document Complaints, Investigation, Sanctions And Corrective Actions
- Mitigate, To The Extent Practicable, Any Harmful Effect Of Wrongful Use Or Disclosure Known To Covered Entity
- Honor Individual HIPAA Rights
- Keep Required Records For 6 Years
- Prohibit/Not Retaliate
HIPAA PHI Use/Disclosure Permitted

- To provide information to coroners, funeral directors, etc.;
- Research purposes;
- For organ, eye, or tissue donation purposes; and
- Judicial/administrative procedure;
- Law enforcement purposes;
- Specialized government functions;
- Worker’s compensation;
- For use by business associates with BA Agreement.
Verification Requirements

- Prior to disclosure as permitted by the regulations, the covered entity must verify the identity of the person requesting the health information and the authority of the person to have access to it unless the identity or authority of the person is known to the entity.

- For example, to identify a public official, a covered entity may rely on a badge or other official credentials, the use of government letterhead, etc.
Notice Requirements

- An individual has a right to adequate notice of the uses and disclosures of health information that may be made by the covered entity and of the individual’s rights regarding health information and the covered entity’s duties.

- The regulations contain specific requirements regarding the content of this notice and when it must be given.

- If the entity has a web site, the notice must be on the web site.
Minimum Necessary Standard

When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity generally must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
Disclosure of De-Identified Health Information

- De-identified health information may be disclosed and the HIPAA regulations do not apply if the code or other means of record identification is not disclosed.

- Re-identified information may only be disclosed in accordance with the HIPPA regulations.
Privacy Standards

Individual Rights

- Right To Notice Of Privacy Practices
- Right To Request Added Restrictions
- Right To Request Confidential Communications
- Right To Access PHI
- Right To Amend PHI
- Right To An Accounting Of PHI Certain Disclosures

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Privacy Official

CE must

- Designate Privacy Official To Develop/Implement/Enforce/
- Maintain Disclosure/Use Policies And Procedures
- Credentials
- Authority
- Up The Ladder Access
HIPAA Security Rules

- Require Covered Entities To Establish & Administer Safeguards To Protect Electronic Protected Health Information
HIPAA Security Rules

- CEs Must Comply With Security Standards For Protection of Electronic Protected Health Information:
  - To safeguard the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained or transmitted by or on behalf of CE in accordance with the Security Standards
  - To protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information; To protected against any reasonably anticipated uses or disclosures of electronic protected health information
  - To ensure compliance with the Security Standards by members of its workforce.

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
HIPAA Security Rules

- 18 Security Standards Covering
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
HIPAA Security Rules
Required vs. Addressable

13 “Required” Implementation Specifications - CE Must Always Meet

22 “Addressable” Implementation Specifications – CE Must:

- Assess if whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity’s electronic protected health information
- If the “addressable” implementation specification determined reasonable and appropriate, implement the specification
- If “addressable” implementation specification determined not reasonable and appropriate, CE must document why it is not implementing the specification and implement an equivalent alternative measure if reasonable and appropriate

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
HIPAA Security Rules
Required vs. Addressable

- CEs Often Rely Upon Consultant/Vendor Reps Of Compliance Without Assessing Adequacy
- CEs Often Don’t Have Needed Documentation Of Evaluation, Analysis, And Basis For Determination About Addressable Implementation Specifications
- Determination Ongoing Process, Must Reassess Continually

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Security Standards
Administrative Safeguards

- Documented Audit and Compliance
  Decision-making Required By Security Regulations
- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness & Training
- Security Incident Procedures
Contingency Plan including
- Data Backup Plan (Required)
- Disaster Recovery Plan (Required):
- Emergency Mode Operation Plan (Required)
- Testing And Revision Procedures (Addressable)
- Applications And Data Criticality Analysis (Addressable)

Periodical Ongoing Evaluation

Business Associate Contracts And Other Arrangements
Security Standards
Physical Safeguards

- Facility Access Controls
- Workstation Use
- Workstation Use
- Decide and Media Controls Use, Access & Disposal
- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security
Security Standards
Organizational Requirements

- Business Associate Agreements
- Policies and Procedures Documentation Requirements
- Workforce Management
- Operational Compliance, Oversight & Enforcement

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
CEs/Business Associates/Service Providers/Employers/Workforce Members must be prepared to defend their dealings with PHI and EPHI With Documented Compliance
HIPAA PRIVACY & SECURITY
RULE VIOLATION RISK RISING

- Criminal Convictions
- Civil Settlement
- Rising Enforcement Statistics
- Civil Litigation
- Licensing Consequences
- Credentialing Consequences
- Workforce Disputes
- Patient & Public Trust
- Other
“Companies Say Security Breach Could Destroy Their Business”

- The study, called Datagate, is based on a survey of more than 1,400 IT professionals at companies with at least 250 employees in the United States, the United Kingdom, France, Germany, and Australia
  - 33% — a major data-loss incident involving accidental or malicious distribution of confidential data could put them out of business
  - 60% — experienced a data breach in the past year but only 6% could say with certainty that they had not experienced one in the previous two years
  - 61% — data leakage is the doing of insiders, and 23% said those leaks are malicious
  - 46% — don't debrief or monitor employees after they give notice that they are leaving the company
  - 23% — able to estimate the total annual cost of data leakage, putting the figure at $1.82 million
  - A data breach that exposed personal information would cost companies an average of $268,000 to inform their customers -- even if the lost data is never used

Source: online article, Sharon Gaudin, April 24, 2007 (11:50 AM EDT)
http://www.techweb.com/wire/199201085
Connecticut AG Brings 1st AG HIPAA Suit Against Heath Net
First criminal sentence imposed for HIPAA Privacy Violation

Clinic employee pled guilty in August, 2004 to criminal violation of HIPAA by using misappropriated charge card and other patient information to purchase items for his personal benefit

Sentence 16 months in prison + required to pay at least $15,000 in restitution, including reimbursing victim for the time and money he spent trying to clear his name
HIPAA Criminal Prosecutions & Convictions

Fernando Ferrer, Jr./Isis Machado

- Theft of personal data of more than 1,100 patients of the Cleveland Clinic and use to submit more than $7 million in fraudulent Medicare claims results in January 24, 2007 conviction of Ferrer for:
  - 5 counts of aggravated identity theft
  - 1 count of computer fraud
  - 1 count of wrongful disclosure of individually identifiable health information under HIPAA
  - 1 count of conspiring to defraud the United States

- The misappropriated information included patients' names, birth dates, Social Security numbers, Medicare identification numbers and addresses

- Information provided to him by a former Cleveland Clinic employee, Isis Machado who was Ferrer's cousin

- Machado, who pled guilty on January 12, 2007 and testified against Ferrer at trial.

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
HIPAA Criminal Prosecutions & Convictions

Andrea Smith

- 25-year old Trumann, Arkansas licensed practical nurse sentenced December 3, 2008 to two years probation and 100 hours of community service for accessing and disclosing a patient’s health information for personal gain

- Plead guilty in first HIPAA privacy breach criminal prosecution brought in Arkansas

- Faced up to 10 years in Federal prison, fines of up to $250,000, or both after pleading guilty to wrongful disclosure of individually identifiable health information (“PHI”) for personal gain and malicious harm in violation of HIPAA Privacy Standards

- Arkansas Board of Nursing to consider discipline in February, 2009-2010 hearing

- US District Judge Susan Weber Wright advised Smith during the sentencing she should spend her community service hours educating others on the consequences of violating the Health Insurance Portability and Accountability Act”
In Miami-Dade County, federal felony charges are pending against Jacquettia L. Brown, 29, and Tear Renee Barbary, 25, prosecution on for offenses relating to the theft of patient profile records from Palmetto General Hospital to further a fraud scheme. According to the Indictment, Brown, a medical records employee of Palmetto General Hospital, took records containing personal profile information of Palmetto General Hospital patients. Defendant Brown and Barbary then used the stolen personal information to further a credit card fraud conspiracy. The patient profile records that Brown stole included personal identifying information, such as patients’ names, birthdates, Social Security numbers, addresses, driver’s license numbers, and next of kin contacts. Brown used the stolen identifying information to obtain patients’ credit card account numbers. She gave patient profile records and credit card account numbers to Barbary, who used the information to make unauthorized credit card purchases. When law enforcement officials disrupted the scheme, Brown was in possession of 41 patient profile records and Barbary was in possession of six patient profile records.
Three Arkansas health care workers could be sentenced to up to 1 year in prison, a fine of not more than $50,000, or both after pleading guilty in July, 2009-2010 to misdemeanor violations of the health information privacy provisions of HIPAA for accessing a patient’s record without any legitimate purpose.

Pursuant to plea agreements with the United States, Holland, Miller and Griffin pleaded guilty to a misdemeanor a violation of the health information privacy provisions of HIPAA based on their accessing a patient’s record without any legitimate purpose. Each faces a maximum penalty of 1 year imprisonment, a fine of not more than $50,000, or both. A sentencing date has not yet been set, but is expected within the next few weeks.
Dr. Holland, Medical Director of Select Specialty Hospital, located on the 6 floor of the St. Vincent Infirmary Medical Center (SVIMC), admitted that after watching news reports on television, he logged on to the SVIMC patient records from his computer at home and accessed a patient’s files to determine if the news reports were accurate. He admitted he accessed the file because he was curious even though he had had HIPAA training and understood he was violating HIPAA when he accessed the file. SVIMC suspended Dr. Holland’s privileges for two weeks and required him to complete online HIPAA training.
Sarah Elizabeth Miller, formerly an account representative at SVIMC, Sherwood Campus, was responsible for checking patients in and out of the clinic and for processing patient billing. In order to perform her duties, she had access to the SVIMC patient records program which includes all locations, not just that of the Sherwood clinic. Miller admitted that on October 20 and 21, 2008, she accessed a patient’s files approximately 12 times out of curiosity. She admitted that she accessed the records without any legitimate purpose. Records show that Miller was trained on HIPAA privacy laws by SVIMC. SVIMC fired Miller from her position.
Candida Griffin was the emergency room unit coordinator at SVIMC. Her responsibilities were to order patient tests, perform data entry into electronic patient files for patients and perform other secretarial functions in the emergency room. Griffin admitted that on October 20, 2008, she was told by the charge nurse to set-up an alias for a particular patient admitted to the emergency room. On October 21, 2008, after the patient had been moved to ICU, Griffin admitted that she became curious about the patient’s status and accessed the medical chart to find out if the patient was still living. Although Griffin did not inform anyone about accessing the chart, hospital records show that the patient’s records were accessed three times that day by Ms. Griffin. SVIMC records show that Griffin was trained on HIPAA privacy laws. SVIMC fired Griffin from her position.
$2.25 Million CVS HIPAA Settlement

CVS Pays $2.25 Million To Resolve Privacy & Security Rule Violation
HIPAA Administrative Penalties & Settlements

- Provident First “Resolution Agreement” Announced July 18, 2008
- $100,000 Resolution Payment
- Detailed Corrective Action Plan
- Settles Administrative Sanctions From 2005 & 2006 PHI Privacy Breach From Laptop/Data Loss
- CMS Views As Template
- Other Resolution Agreement Negotiations Under Way/Expected
Other Federal Criminal Code Data Security & Identity Theft Laws Require Data Protection

- 18 U.S. C. § 1028. Identity Theft And Assumption Deterrence Act
- 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Examples Of Other Federal Laws Requiring/Recommending Business/Government Protect Personal Information Include:

- 18 U.S. C. § 1028 - Identity Theft And Assumption Deterrence Act
- Electronic Discovery Rules
- FACTA
- Sarbanes-Oxley
- Graham Leech
- Fair Credit Reporting Act/FACTA
- Securities
States With Personal Data Breach Notification Laws

Source: The University of Georgia
Athens, GA 30602

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
State Common Law Claims, e.g.

- Negligence
- Invasion of Privacy
- Intentional Infliction of Emotional Distress
- Breach of Contract
- Deceptive Trade Practices
- Other
Companies/Computers Don’t Break The Law, People Do
Effective Compliance Requires Effective People Management…
Internal & External

Patients & Family
Workforce
Business Associates
Employer & Payers
Other Covered Entities
Government
Site Vendors
Media
Hallway Walkers & Bathroom PIs
Others
The Process is Often as Important as the Result

- Documented Policy of Compliance
- Good Decision-making
- Documentation of Decision-making
- Rapid Response When Disaster Strikes
“This project is extremely important, but it has no budget, no guidelines, no support staff and it’s due tomorrow morning. At last, here’s your chance to really impress everyone!”

EFFECTIVE PREVENTION & CLEAN UP REQUIRES PROVIDE ADEQUATE RESOURCES
Compliance Operationalization
Effectiveness Formula

Path Your PHI
Capture Your Compliance Efforts & Analysis
Adopt Required Policies
Understand Your Organization’s Many Hats, Requirements & Concerns
Privacy, Security, Data Breach, FACTA, State Law, Ethical & Other Requirements
Anticipate Why/How Can/Is Accessed
Train/Require Compliance/Reporting Noncompliance
Anticipate & Monitor/Audit Possible Sources of Breach
Understand/Manage Others Hats, Requirements & Concerns Timely, Documented
Investigation When Breach/Other Noncompliance Suspected
Understand Relationship Between Rules & Operations
Have/Practice/Train on Disaster Plan

+Constant Quality Improvement

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
MEETING THE HIPAA MISSION
REQUIRES

- Establish Compliant Policy
- Train Workforce
- Legally & Effectively Obtain, Use & Safeguard Necessary Personal & Other Sensitive Data
- Make PHI Confidential Information Protected As Trade Secret
- Require HIPAA Data Charting As Part of Operations
- Monitor/Require Timely Notice of Breach & Other HIPAA Noncompliance
- Manage Data Requests & Disclosure To Promote Desired Individual & Organizational Response/Cooperation
- Systemize PHI Safeguards On Hiring, Periodically & At Exit
- FCRA Consents, Privacy Disclaimers Broadly Written To Support Investigations
- Timely Investigate Possible Noncompliance
- Give Notice of Breach & Take Other Required Corrective Action
- Document Compliance Efforts
- Whistleblower & Other HR Compliance
- Crisis Response
- Manage Public Image

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Privacy Risk-Management Program Planning

- Consider Attorney-Client Privilege Before Starting
- Legal & Operational Inventory To Define Minimum Requirements
- Audit Policies, Procedures and Practices
- Assess Compliance Status and Risks
- Design and Document Tailored Risk-management Program
- Document Decisions
Privacy Risk-Management Program Planning

- Implement Risk-Management Program
- Oversee Compliance
- Consistently Enforce Standards Through Appropriate Disciplinary Mechanisms
- When Detect Violation, Respond Appropriately Including Appropriate Compliance Plan Adjustments To Minimize Future Risks
- Responsibility To Monitor Compliance To Specific High Level Person, Not To Individuals That Maintain Programs
- Communicate and Conduct Training Tailored To Ensure Effectiveness
- Establish/Communicate Compliance Standards and Procedures Reasonably Capable of Being Followed
- Oversight & Enforcement
- Continuous Quality Improvement

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Have A Disaster Recovery Plan

“Remember son, if at first you don’t succeed, make it look like someone else’s fault then sue them.”
Have A Disaster Recovery Plan...
A 2nd Look & the CE/BA Relationship

“Remember son, if at first you don’t succeed, make it look like someone else’s fault then sue them.”

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
OCR added to its Compliance and Enforcement Web Site on May 9.

Located at: www.hhs.gov/ocr/privacy/enforcement/data/html

Shows:
- Enforcement Statistics
- Charts showing state-specific case investigation results;
- Calendar-year enforcement-results graphs and charts;
- A Calendar-year graph showing complaint receipts;
- Yearly variation in the issues in cases resolved through corrective action.
PRIVACY RISK-MANAGEMENT PROGRAM PLANNING
WHAT DO YOU NEED PEOPLE TO DO?

- Operational requirements to control/monitor access and usage
- Laws and regulations requiring/recommending control/monitor access & usage
- Contractual/external relations requiring/recommending control/monitor access & usage
- Documented oversight, enforcement and correction
- Incorporate Data Breach & Security Processes In Overall Scheme

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Who Do You Need To Do It?

- People To Be Granted Access With Documentation For Rationale and Scope
- Permitted Access and Usage
- Required Credentials For Maintaining Access & Usage
- Operational requirements to control/monitor access and usage
- Training Safeguards
- Oversight
- Monitoring & Redress of Attempted & Actual Violations
- Termination of Access
- Documentation
Monitoring Suspicious Behavior, Access
FTC Misrepresentation Enforcement

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Protect What You Collect - Restrict Access

SAFEGUARD

Sensitive Information

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
Use & Disclose Cautiously

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
The Dogbert Phone Method

Follow these steps to get rid of callers who want information.

1. No matter what they ask, just give them the information you have right in front of you.

   I've got some good information on the days of the week...

2. If the caller protests, make them restate the question in as many forms as possible.

   How would the Hopi Indians phrase that?

3. Act like the caller's question makes no sense whatsoever.

   Are you talking pig Latin? What do all of those words mean?

Continued...
CONTINUED: THE DOGBERT PHONE METHOD

4. Pause twenty seconds and pretend you've forgotten the entire conversation.

Hello, have you been helped?

5. Now put the caller on hold and disconnect after ten minutes.

Oops!

6. If they call back, scan the obituaries and refer the caller to the recently deceased.

Boy, I hope nothing ever happens to ol' Ben... because he's the only one who can answer your question.

7. If the pest calls you again, slip into a foreign accent and start over at step one.

Ya, vee got zum days of ze veek right here, by yimminy!
The world is a scary place at times…
Privacy Matters

©1938 PARKER BROTHERS, INC.

©2009-2010 Cynthia Marcotte Stamer. All rights reserved.
The HIPAA Help Desk
Compliance is a Goal, Not a Destination

Thank You & Good Luck On Your Journey