SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

The Health Information Technology for Economic and Clinical Health Act (HITECH) and Electronic Protected Health Information

David M. Mack, JD, MPH

Today's Discussion

- Breaches in the Health Care Industry
- New Laws and Guidance
- HIPAA Breach Notification Requirements
- Connecticut Breach Notification Requirements
- Other Applicable HITECH Issues
  - Business Associates
  - Accounting
  - Access
  - Enforcement and Penalties
  - Upcoming HIPAA Issues

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Breaches in the Health Care Industry

- August 2008 - Providence Health & Services (Seattle, WA) paid the Department of Health and Human Services (HHS) $100,000 to settle allegations of HIPAA violations and was required to adopt a Corrective Action plan, which, for three years, requires that Providence submit copies of its written policies and procedures to HHS for approval
  - Computer back-up disks and tapes containing unencrypted electronic protected health information (PHI) were stolen from the unattended car of a Providence employee. Additionally, several laptops were stolen from Providence employees over the course of seven months
  - The back-up disks and tapes and laptops contained the PHI of over 386,000 patients

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Breaches in the Health Care Industry

- March 2009 – A laptop containing PHI was stolen from an outside vendor of Moses-Cone Hospital (Greensboro, NC). The Hospital provided the outside vendor the laptop, which was password protected but not encrypted, to review patient data
  - The PHI of over 14,000 patients may have been compromised
  - The Hospital waited months before informing patients

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

New Laws and Guidance

- The Stimulus Bill
  - The Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009
- Other Guidance
  - FTC Health Breach Notification Final Rule, 74 Fed. Reg. 42962 (August 25, 2009)
  - HHS Breach Notification for Unsecured Protected Health Information, Interim Final Rule, 74 Fed. Reg. 42740 (August 24, 2009)
  - HHS Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, 74 Fed. Reg. 19006 (April 27, 2009)

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notification of Breach

- Notification is required if there is a "breach"
- Breach is the acquisition, access, use, or disclosure of PHI, other than as permitted by HIPAA, which compromises the security or privacy of the PHI

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Determining If There Has Been a "Breach"

- Step 1: Did the incident involve PHI?
- Step 2: Was there an acquisition, access, use or disclosure of PHI not permitted by the HIPAA Privacy Rule (e.g. unauthorized or impermissible)?
- Step 3: Does an exception or safe harbor apply?
- Step 4: Did that use or disclosure compromise the security or privacy of the PHI?

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Step 1: PHI

- Must be an incident involving PHI
- PHI is individually identifiable health information that is transmitted or maintained in electronic media or in any other form or medium
- PHI does not include:
  - Certain educational records
  - Employment records
  - De-identified information

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Step 2: Unauthorized or Impermissible

- Must be not permitted by the HIPAA Privacy Rule
- Typically, this does not include:
  - Use or disclosure incident to a permitted use or disclosure despite reasonable safeguards
  - Violations of administrative requirements (e.g. lack of policy or training)
  - Violations of the HIPAA Security Rule

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Step 3: Exceptions

Notification is not required if the breach fits into one of the following three exceptions:

- Unintentional Acts by Workforce Member (e.g. employee, volunteer, trainee, or other person under direct control of the covered entity)
  - in good faith,
  - within scope of employment or engagement, and
  - no further acquisition, access, use, or disclosure not permitted by the HIPAA Privacy Rule
- Inadvertent Disclosures by the Workforce Member
  - from one authorized workforce member to another at the covered entity (or business associate) or within an Organized Health Care Arrangement in which the covered entity participates, and
  - no further acquisition, access, use or disclosure not permitted by the HIPAA Privacy Rule
- PHI Not Retained
  - disclosed to an unauthorized person, and
  - good faith belief that the PHI was not able to be retained by the unauthorized person

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Step 3: Safe Harbor

- Notification is only required for breach of unsecured PHI
- PHI must be unreadable, unusable, or indecipherable to unauthorized individuals to fall outside of the definition of "unsecured"
- The only two methods for securing PHI to avoid notification are encryption and destruction. Although the encryption and destruction practices are not required, they are strongly recommended given the cost and impact of sending out breach notifications
- Firewalls and access controls are reasonable and appropriate safeguards, but are not sufficient to avoid notification
- De-identified is not considered PHI. Redaction alone may not be sufficient. Use de-identified to the extent practicable

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Step 3: Safe Harbor

Encryption

- Rendering electronic PHI unusable, unreadable, or indecipherable to unauthorized persons. The use of an algorithm to encrypt data into a form with low probability of having meaning without a confidential key. The success of encryption depends on the strength of the algorithm and the security of the decryption key
- Data at rest-See NIST Special Publication 800-111; Data in motion-See Federal Information Processing Standards 140-2 and NIST Special Publications 800-52, 800-77, 800-113, or others which are Federal Information Processing Standards 140-2 validated
- Keep encrypted key on a separate device or at a different location from the data the key encrypts or decrypts

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Step 3: Safe Harbor

- Destruction
  - For paper records, film and other media, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed. Redaction is not sufficient
  - For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding) such that PHI cannot be retrieved. See, NIST Special Publication 800-88, Guidelines for Media Sanitization
- Falling within the safe harbor does not necessarily eliminate obligations under state law or a covered entity's obligation to mitigate damages

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Step 4: Risk Assessment

- Only considered a breach when "poses a significant risk of financial, reputational, or other harm to the individual"
- Requires covered entities and business associates to conduct and document a "risk assessment"
- Consider the risk that the individual can be identified and then the risk of harm to the individual

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Step 4: Risk Assessment

- Must consider several factors, including:
  - Who used the PHI or to whom it was disclosed (e.g. another covered entity may be less risky)
  - Any mitigating factors (e.g. confidentiality agreement, return prior to access)
  - Type and amount of PHI involved (e.g. names only may be low risk, unless sensitive; risk of identity theft)

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Step 4: Risk Assessment Involving Limited Data Sets

- Use or disclosure of PHI in a limited data set may be a breach and requires a risk assessment
- A limited data set is PHI that excludes certain direct identifiers of the individual or of relatives, employers, or household members of the individual (e.g. names, telephone numbers, or Social Security numbers)
- Data Use Agreement required and impermissible use or disclosure by third party recipient who is not a covered entity or business associate does not require notification
- The use or disclosure of a limited data set from which all 16 direct identifiers, birth date, and zip code have been removed does not constitute a breach

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Documentation

- Must document to demonstrate that no breach notification was required (e.g. risk assessment or exception)
- Documentation Requirements
  - The factors the entity considered during the assessment
  - The basis for the conclusion
  - Must maintain the documentation and make it available to HHS upon request

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notification of Breach

- Notice
  - To the patient,
  - To the covered entity by business associate,
  - To the media, or
  - To the Secretary
- Effective September 23, 2009
- See State law for additional notice requirements

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Timing of Notices

- Discovery of Breach
  - A breach is treated as discovered by a covered entity as of the first day the breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity and not when risk assessment is completed
  - Knowledge of a business associate or workforce member (i.e. employee, volunteer, trainee, but not the person committing the breach) is imputed to the covered entity
  - Need reasonable systems to identify a breach
- Timing of Notification
  - All notifications must be made "without unreasonable delay" and in no case later than 60 calendar days after discovery of the breach
  - In some cases, it may be unreasonable to wait until the 60th day to provide notification (e.g. individual needs to protect self from harm)
  - Notice must be delayed if law enforcement provides a written statement that notice would impede a criminal investigation or cause damage to national security for the period of time specified in the statement

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notice to the Patient

- Previously, no requirement under HIPAA to notify a patient of a breach
- Now, any breach requires the covered entity to notify each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of the breach

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notice to the Patient

- Content of the Notification
  - Plain language
  - Brief description of what happened, including the date of breach and the date of discovery
  - Description of the types of unsecured PHI involved
  - Steps individuals should take to protect themselves from potential harm
  - Brief description of steps being taken in response to the breach
  - Contact information

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notice to the Patient

- Methods of Notification
  - Notice by first-class mail or email, if specified as a preference by the individual
  - In the event more urgent notice is deemed necessary by the covered entity, telephone or other contact may be appropriate, in addition to written notice
  - Permitted to provide information in steps as information becomes available
  - Special Cases
    - Deceased Individual: notice to next of kin or personal representative
    - Minor or Individual Lacking Legal Capacity: notice to parent or personal representative

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notice to the Patient

- Substitute Notice Reasonably Calculated to Reach the Individual
  - Required when the covered entity lacks sufficient contact information (not including next of kin or the representative of a deceased individual) or a notice is returned as undeliverable
  - Fewer than 10 individuals
    - Can provide notice by telephone or other means reasonably calculated to reach the individuals
  - 10 or more individuals
    - Conspicuous posting on covered entity's website for 90 days or in major print and broadcast media in areas where the individuals affected by the breach likely reside
- Collect alternative contacts and request permission to email

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notice to the Covered Entity

- In the event a business associate discovers a breach of PHI, it must report the breach to the covered entity
- Discovery of Breach
  - A breach is treated as discovered by a business associate as of the first day the breach is known to the business associate or any employee, officer, or agent of the business associate, or by exercising reasonable diligence would have been known to the business associate or any employee, officer, or agent
- Timing of Notification
  - All notifications must be made "without unreasonable delay" and in no case later than 60 calendar days after discovery of the breach
  - Should provide shorter time frame in Business Associate Agreement in order to ensure time for investigation, risk assessment, and notification

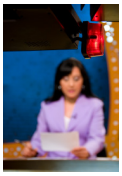
SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notice to the Covered Entity

- Content of Notification
  - Identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, breached
  - Business associate has an obligation to inform covered entity of any newly available facts, even after the initial notification

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notice to the Media



- For breaches involving PHI of more than 500 individuals of any one state or jurisdiction, the covered entity must also notify "prominent media outlets" in that state or jurisdiction
- Notice must be made "without unreasonable delay" and in no case later than 60 calendar days after discovery of the breach
- Same content as for an individual notice, but often in the form of a press release

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notice to the Media

- Determining if notice is required:
  - Example: Covered entity discovers a breach of 1000 individuals. 400 live in Connecticut and 600 live in Massachusetts. Notice to the media is required only in Massachusetts
- Consider the number of individuals in each state, the location of the individuals, and the types of media available

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notice to the Secretary

- For breaches involving the PHI of more than 500 individuals, the covered entity must notify the Secretary of HHS
  - Does not take into account particular states
  - Must be sent concurrently with the notice to individuals
  - HHS will post information on its website

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notice to the Secretary

- For breaches involving the PHI of less than 500 individuals, the covered entity must:
  - Maintain a log or other documentation of such breaches, and
  - Submit such log or documentation annually to the Secretary
- Annual submission must be made no later than 60 days after the end of the calendar year, in a manner to be specified on the HHS website. For calendar year 2009, the covered entity is only required to submit information to the Secretary for breaches occurring on or after September 23, 2009

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notification of Breach

- Notification Rules if Not Regulated by HIPAA
  - The Federal Trade Commission (FTC) is implementing breach notification requirements
  - Applies to three types of entities:
    - Vendors of Personal Health Records (PHR),
    - PHR Related Entities, and
    - Third-Party Service Providers
  - Similar to notification rules under HIPAA

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notification of Breach

- What if an entity is considered *both* a HIPAA covered entity or business associate and one of the three FTC regulated entities?
  - Entity is subject only to the HIPAA regulations

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notification of Breach

- Connecticut Law
  - In the event of a "breach of security" of "personal information," the entity that owns the information must disclose the breach of security to Connecticut residents whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through such breach

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notification of Breach

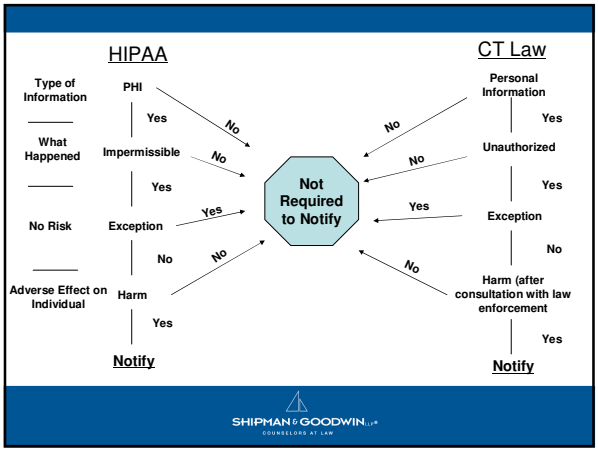
- "Breach of security" in Connecticut
  - Unauthorized access to or acquisition of electronic files, media, databases or computerized data containing *personal information* when access to the personal information has not been secured by encryption
  - *Personal information* is an individual's first name or first initial and last name in combination with any one or more of
    - social security number,
    - driver's license number,
    - state identification card number, or
    - account number, credit or debit card number in combination with any required security code, access code or password
- Laws of other states may also apply

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Notification of Breach

- Connecticut Exception: disclosure is not required if, after completion of an investigation and consultation with law enforcement, the breach will not likely result in harm

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW



SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Other Applicable HITECH Issues

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Application of HIPAA to Business Associates

- HIPAA has traditionally regulated only certain covered entities and not business associates directly
- HITECH directly applies HIPAA's security and privacy rules to all business associates, meaning business associates must now implement all of the administrative, physical and technical safeguards required by HIPAA for a covered entity and have policies, procedures and documentation to establish its compliance
- Violation of the privacy and security rules will subject the business associate to the same civil and criminal penalties as would apply to a covered entity who violated the same provisions
- Business Associates now include organizations that provide data transmission (HIEO, RHIO, e-prescribing gateway, vendor of personal health records)
- Covered Entities need to update Business Associate Agreements

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Expansion of Accounting Rule

- Must account for all disclosures of PHI maintained in an electronic health record (EHR) for treatment, payment, and health care operations for 3 years from the date of the disclosure
- Must provide an accounting of such disclosures upon request

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Expansion of Accounting Rule

- If a covered entity receives a request for an accounting, it has two options:
  - Provide an accounting of disclosures by the covered entity and business associates, or
  - Provide a list of business associates for the individual to contact directly for an accounting of disclosures. If contacted, the business associate must provide the accounting
- Effective January 1, 2011 if EHR acquired after January 1, 2009
- Effective January 1, 2014 if EHR acquired before January 1, 2009

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Access to PHI in Electronic Format

- Individuals now have a right to receive an electronic copy of their electronic PHI
- A covered entity may charge a fee for access, limited to the lesser of:
  - Labor costs, or
  - Any applicable State law
- Effective February 17, 2010

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Enforcement and Penalties

- Expanded enforcement and increased penalties
- State attorney general action
  - May file civil actions or injunctions to enforce HIPAA
  - May recover damages, costs and attorneys' fees up to $100 per violation up to $25,000 per type of violation
- Still no private right of action, but an individual harmed by a breach may receive a percentage of penalties collected

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Enforcement and Penalties

- Strengthened OCR Enforcement
  - Mandatory investigations and fines for willful neglect complaints
  - Mandated periodic audits of covered entities and business associates
  - Penalties from enforcement fund future OCR enforcement

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Enforcement and Penalties

- Increased Penalties
  - Effective immediately, increased civil penalties from the previous high of $25,000 to a new high of **$1,500,000** depending on the type of violation
  - Corrective action without a penalty is allowed if person does not know (and by exercising reasonable diligence would not have known) of the violation

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Enforcement and Penalties

- **Increased Tiered Civil 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
  - 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
  - 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
  - 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

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Enforcement and Penalties

- Expanded Application of Criminal Penalties:
  - Criminal penalties of fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining with the intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm
  - Criminal penalties now also apply to:
    - *business associates*, and
    - *individuals* who without authorization obtain or disclose, whether or not they are employees of the covered entity

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Upcoming HIPAA Issues Identified by HITECH

- HHS reports to Congress on breach data, complaints
- HHS guidance on de-identifying PHI, minimum necessary and psychotherapy notes
- HHS and FTC study regarding application of HIPAA to non-covered entities
- Comptroller General report to Congress on best practices related to treatment disclosures
- GAO report on impact of HIPAA on insurance premiums, health care costs, adoption of EHR, medical errors and quality improvement

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW

Shipman & Goodwin LLP Contact Information:

David Mack
(860) 251-5058
dmack@goodwin.com

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW