HIPAA Compliance in the Digital Age

HIMSS CENTRAL & SOUTHERN OHIO Chapter

October 18, 2013

Presented By:

Lisa Pierce Reisz

Vorys, Sater, Seymour and Pease LLP

614.464.8353 | lpreisz@vorys.com

"No, it's not a female Hippopotamus, anyone else know?"

Final Omnibus HIPAA Rule is Comprised of Four Final Rules

- Final modifications to the HIPAA Privacy, Security and Enforcement Rules as mandated by HITECH.
- Final rule adopting changes to the HIPAA Enforcement Rule provided by HITECH.
- Final rule on Breach Notification for unsecured PHI under HITECH.
- Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act ("GINA").

Changes to Privacy Rule

- Right to electronic copy of EHR, and right to direct copy to third party.
- Right to restrict disclosures to health plans of treatment/services paid for in cash.
- Marketing communications paid for by third parties require authorization.
  - Limited exception for refill reminders and current prescriptions.
- Easy way to stop fundraising communications.
- Prohibition on sale of PHI without authorization.

Changes to Privacy Rule (cont'd)

- Makes it easier for parents to permit providers to release student immunization records to schools.
- Permits researchers to use a single authorization for more than one purpose, and relaxes the policy on authorization for future research.
- HIPAA protection limited to 50 years after death, and makes access to friends and families easier.
- Required changes to Notices of Privacy Practices, but relaxes distribution requirements for Health Plans.

HIPAA Enforcement Rule Transformed HIPAA Compliance

- HITECH transformed HIPAA compliance from what had been a low priority of CEs and their BAs into an obligation requiring careful attention.
  - Significant increase in civil monetary penalties which could be imposed for HIPAA violations.
  - Increased budget to OCR for HIPAA enforcement efforts.
  - Audits (with budget to conduct them).
  - Granted state AGs enforcement authority over HIPAA violations affecting state residents.
  - Created breach notification and reporting requirements for certain violations.
- HITECH's increased enforcement emphasis has been incorporated into the Final Omnibus HIPAA Rule.

Increased Civil Monetary Penalties

- Pre-HITECH: CMPs were not more than $100.00 per violation, with a maximum of $25,000 for all identical violations during a calendar year.
- Now: CMPs range from $100 to $50,000 per violation, and up to $1,500,000 for identical violations for a calendar year.
- HITECH also restricts the defenses to an alleged violation.

Civil Monetary Penalties

- Civil monetary penalties for HIPAA violations were significantly increased after HITECH (and these increased CMPs have been incorporated into the Final Omnibus HIPAA Rule).

Civil Monetary Penalties for HIPAA Violations:		
Violation Category of Culpability	**Each Violation**	**Annual Maximum for Identical Violations**
Did not know (and would not have known with reasonable diligence)	$100 - $50,000.00	$1,500,000.00
Violation due to reasonable- cause but not willful neglect.	$1,000 - $50,000.00	$1,500,000.00
Willful neglect – but violation corrected	$10,000 - $50,000.00	$1,5000,000.00
Willful neglect – violation NOT corrected	$50,000.00	$1,500,000.00

Factors Impacting Amount of CMPs

- The nature and extent of the violation.
- The nature and extent of the resulting harm.
- Other factors, including prior compliance with the rules and/or the financial condition of the covered entity or business associate at the time of the violation.

Increased Federal Enforcement

- HHS Enforcement:
  - **77,877 HIPAA complaints filed with OCR between April 14, 2003 and January 31, 2013.**
    - 70,800 complaints resolved: through investigation and enforcement (over 18,711); through investigation and finding no violation (8,971); and through closure of cases not eligible for enforcement (43,118).
    - 7,077 complaints currently open.
  - **The compliance issues investigated most are:**
    - Impermissible uses and disclosures of PHI;
    - Lack of safeguards of PHI;
    - Lack of patient access to their PHI;
    - Uses or disclosures of more than the minimum necessary PHI; and
    - Lack of administrative safeguards of ePHI.

HHS Enforcement Actions

- RiteAid settled with HHS and FTC for $1 million for its failure to protect PHI in disposal of pill bottles and other health information, 6/2010.
- Cignet Health Care fined $4.3 million for failing to provide patients a copy of their own medical records, 2/2011.
- Mass General Hospital paid $1 million settlement and CAP after employee lost paper file containing PHI on subway, 2/2011.
- UCLA Health Systems settles with HHS for $865,000 and commitment to a CAP for employee PHI surfing, 7/2011.
- Blue Cross Blue Shield of Tennessee settled HIPAA violation with HHS for $1.5 million for failing to secure PHI in off-site storage facility, 3/2012.

HHS Enforcement Actions (cont'd)

- Phoenix Cardiac Surgery (physician practice) settled with HHS for $100,000.00 after OCR investigation found failure to implement HIPAA policies and procedures and to safeguard ePHI, 4/2012.
- State of Alaska settles HIPAA violations with HHS for $1.7 million after breach investigation in which OCR determined that Alaska did not have adequate HIPAA policies and procedures in place (i.e. no risk assessment),6/2012.
- Massachusetts Eye and Ear Infirmary paid $1.5 million to HHS for violations of the HIPAA Security Rule including failure to conduct a risk assessment and failure to implement policies related to security of ePHI on mobile devices, 9/2012.
- Hospice of North Idaho settles HIPAA violation for $50,000.00 after breach investigation showed that HONI failed to do a security risk assessment, 1/2013.

Criminal Enforcement Actions
42 U.S.C. § 1302d-6

- To commit a criminal offense under HIPAA a person must "knowingly" and in violation of HIPAA do one of the following:
  - Use or cause to be used a unique health identifier;
  - Obtain individually identifiable health information; or
  - Disclose individually identifiable health information to another person.
- Penalties for Criminal Violations:
  - Fine of $50,000 to $100,000.00.
  - Imprisonment of 1 to 5 years.
- DOJ enforces HIPAA's criminal provisions.
- Few cases have been prosecuted but typically involve theft of PHI for some form of "financial gain" by an employee of a covered entity.
  - ***U.S. v. Gibson*,** No. CR04-0374RSM, 2004 WL2237585 (W.D. Wash. Aug. 19, 2004).

OCR Audits

- HITECH required HHS to provide for periodic audits to ensure HIPAA compliance by CEs and BAs.
- HHS awarded KPMG a $9.2 million contract to conduct HIPAA audits of up to 150 CEs before December 31, 2012.
- OCR began a pilot audit program in November 2011 in which it performed 115 audits of CEs to assess privacy and security compliance. The pilot phase ended in December 2012.
  - The goal of the OCR audit program was analyze the policies and procedures of covered entities to determine areas of risk.
  - Full investigations of covered entities were only undertaken if the audit revealed a serious compliance problem.
- OCR has indicated that audits of both CEs and BAs will continue into the future.

Preliminary Audit Observations

- Policies and procedures.
- Priority HIPAA compliance programs.
- Small providers.
- Larger entities have security challenges.
- Risk Analysis.
- Privacy challenges are widely dispersed with no clear trend by entity type or size.

State Enforcement Actions

- HITECH gave state AGs new HIPAA enforcement powers.
  - June 2011, HHS trained state AGs on HIPAA enforcement.
- Security breach-related legislation has been enacted in 46 states, the District of Columbia, Puerto Rico and the Virgin Islands.

Breach Notification Rule

- Final Omnibus HIPAA Rule significantly changed definition of "Breach."
  - Beginning on September 23, 2013, HITECH's "significant harm" test will be replaced with a more objective test for breach.
  - Expectation is that more data incidents will be reportable breaches under the new breach rule.

Definition of "Breach"

- Replaces "significant harm" test used to determine "breach" with a more objective measure
- Now, any unauthorized acquisition, access, use or disclosure of PHI is **presumed to be a breach,** unless the covered entity or business associate demonstrates a low probability that the PHI has been compromised based on an assessment of the following four risk factors:
  - The nature and extent of the PHI involved, including the types of identifiers;
  - The unauthorized person who used the PHI or to whom it was disclosed;
  - Whether the PHI was actually acquired or viewed; and
  - Extent to which the risk to the PHI has been mitigated.

Exceptions to Definition of Breach

- Not every impermissible acquisition, access, use or disclosure of PHI constitutes a "Breach" under HIPAA.
  - The unauthorized acquisition or access to **secured** PHI does not constitute a breach: **ENCRYPT, ENCRYPT, ENCRYPT!!**
  - Exceptions to Definition of Breach:
    - Unintentional acquisition.
    - Inadvertent disclosure.
    - Recipient would not have been able to retain information.

Breach Notification Requirements

HITECH breach notification rule adopted without change:

- Breaches involving **fewer than 500 people**
  - Written notification by first class mail to the individual at their last known address.
  - Annual submission of a log to the Secretary of HHS documenting such breaches during the year involved.
- Breaches involving **500 or more people**
  - Written notification by first class mail to the individual at their last known address.
  - Notification to prominent media outlets serving a state or jurisdiction of a breach involving more than 500 residents of the state or jurisdiction.
  - Immediate notification to the Secretary of HHS.
  - Posting on HHS website – the "HHS Wall of Shame."

Timing of Breach Notification

- **Covered Entity:**
  - If a Breach has occurred, a CE must provide notice to the affected individuals **without unreasonable delay** and in no event later than 60 days from the date of discovery.

Timing of Breach Notification (cont'd)

- **Business Associate:**
  - BA, following discovery of a breach, must notify the CE of such breach **without unreasonable delay** and in no case later than 60 days following the discovery of the breach.
    - If a BA is acting as an agent of a CE, then BA's discovery of the breach will be imputed to CE (which means the 60-day clock runs at the time the BA discovers the breach).
    - If the BA is not an agent of the CE, then the CE must provide notice based on the time the BA notifies the covered entity of the breach (a new 60-day clock starts).

Causes of Breach

- ***Human error and process mistakes, not technology, are the biggest causes of HIPAA violations.***
- Top 3 Causes of Breach:
    1. Lost or stolen laptops, removable devices (flash drives), mobile devices, and documents (46%).
    2. Employee mistake or unintentional actions (42%).
    3. Third-party errors (42%).

-- Ponemon Institute (2012)

Causes of Breach (cont'd)

- **Process failures include:**
  1. Failure to encrypt PHI.
  2. Failure to establish adequate password protections.
  3. Failure to adequately train employees on HIPAA policies and procedures.
  4. Failure to consistently discipline employees for HIPAA violations.

Breach Statistics

- There are currently 556 entities listed on the HHS "Wall of Shame."
- Healthcare industry loses $7 Billion a year due to HIPAA data breaches.
- The average economic impact of a data breach has increased by $400,000.00 to a total of $2.4 million since 2012 with an average cost of $471 per patient record.
- 94% of healthcare organizations have had at least one data breach in the last two years.

Breach Statistics (cont'd)

- Average number of lost or stolen records per breach is 2,769.
- 48% of all data breaches in 2012 involved medical records.
- 18% of healthcare organizations say medical identity theft was a result of a data breach.
- Annual security risk assessments are conducted by less than half of all health care providers.

-- Ponemon Institute (2012)

Lessons Learned From Data Breaches

- Encrypt all data on portable devices.
- Improve physical security. Do not give employees unfettered access to all spaces in which data, records and devices are stored.
- Limit online access to data. Not everyone needs access to everything. Re-evaluate job descriptions and tailor data access to those reasonably necessary for employees to perform their duties. Terminate access for all former employees. Discipline employees who access patient data without need.
- Ask patients to update their information regularly to eliminate billing and information release errors.

Lessons Learned From Data Breaches (cont'd)

- Properly destroy data on recycled and retired technology.
- Properly destroy patient paper records that are beyond statutory retention periods.
- Update HIPAA policies and procedures to reflect actual operations of organization.
- Train and re-train employees on HIPAA compliance.
- Consider procuring cyber insurance.

Cyber Insurance

- Considerations Before Making the Purchase:
  - Assess your organization's risks for a data breach
  - Understand your current insurance coverage
  - Evaluate policy options and coverages carefully. Policies should cover the costs of:
    - Notification letters to patients
    - Credit monitoring
    - Computer expert forensic investigation
    - Regulatory defense and penalties
    - Website media content liability
    - Crisis management and public relations
    - Defense costs

Cyber Insurance (cont'd)

- Considerations before making the purchase: (cont'd)
  - Perform a risk assessment (could speed up underwriting and lower premiums).
  - Work with a knowledgeable broker.
  - Take advantage of value-added services.
  - Get preferred vendors approved before policy is bound.

GINA Provisions

- Requires "genetic information" be treated as PHI.
- Prohibits health plans from using/disclosing genetic information for underwriting purposes.

"Normally, I'd discuss your condition with these first-year residents, but because of confidentiality restrictions, all I can really tell them is that you're a shoo-in for an invasive procedure."

Business Associates

- Definition of "Business Associate" expanded:
  - Includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities.
  - Includes entities that merely store PHI (BAs may now "create, receive, maintain, or transmit PHI")
  - Downstream subcontractors of BAs are now defined as BAs.
  - Patient safety activities have been added to the list of functions that may cause an organization to be deemed a BA.
  - Conduit exception is narrow and intended to only exclude courier services and their electronic equivalents; data storage services that store PHI are considered BAs.
- Whether an entity is considered a BA is based on the nature of their activities.
- **The outcome cannot be avoided by simply foregoing a contract!**

Business Associates (cont'd)

Various HIPAA provisions now expressly apply to BA and their subcontractors:

- All applicable provisions of the Security Rule. BAs are now directly liable for Security Rule violations (as well as breach of contract liability).
- The use and disclosure limitations of the Privacy Rule including the minimum necessary principle and, if applicable, de-identification standards. BAs are now directly liable for Privacy Rule violations (as well as breach of contract liability).
- The requirement to provide a copy of ePHI to a covered entity, the individual or the individual's designee
- The requirement to maintain an accounting of disclosures
- The obligation to cooperate with HHS during an investigation or compliance review.

Business Associates (cont'd)

As of September 23, 2013, BAs and their subcontractors must comply with HIPAA requirements:

- Adoption and implementation of dozens of documented HIPAA policies and procedures.
- Implementation of Security Rule technical requirements.
  - Conducting a security risk analysis
  - Developing mitigation plan
  - Producing a contingency plan
  - Encryption of ePHI
  - Preparing systems to log and monitor user activity
- Compliance requires training workforce on HIPAA compliance program

Business Associate Agreements

CEs should be reviewing and updating all business associate agreements:

- Enhanced BA compliance obligations
- Breach response and reporting obligations
  - Timing
  - Responsibility designation
  - Cost of reporting obligations
- Indemnification provisions
  - Breach notification costs
  - Credit monitoring and other mitigation costs
  - Defense costs
  - CMPs
- Insurance coverage.

Federal agency law will play an important part in defining the relationship between CEs and BAs. CEs are directly liable for their BAs if they constitute agents.

State Law and 42 CFR Part 2

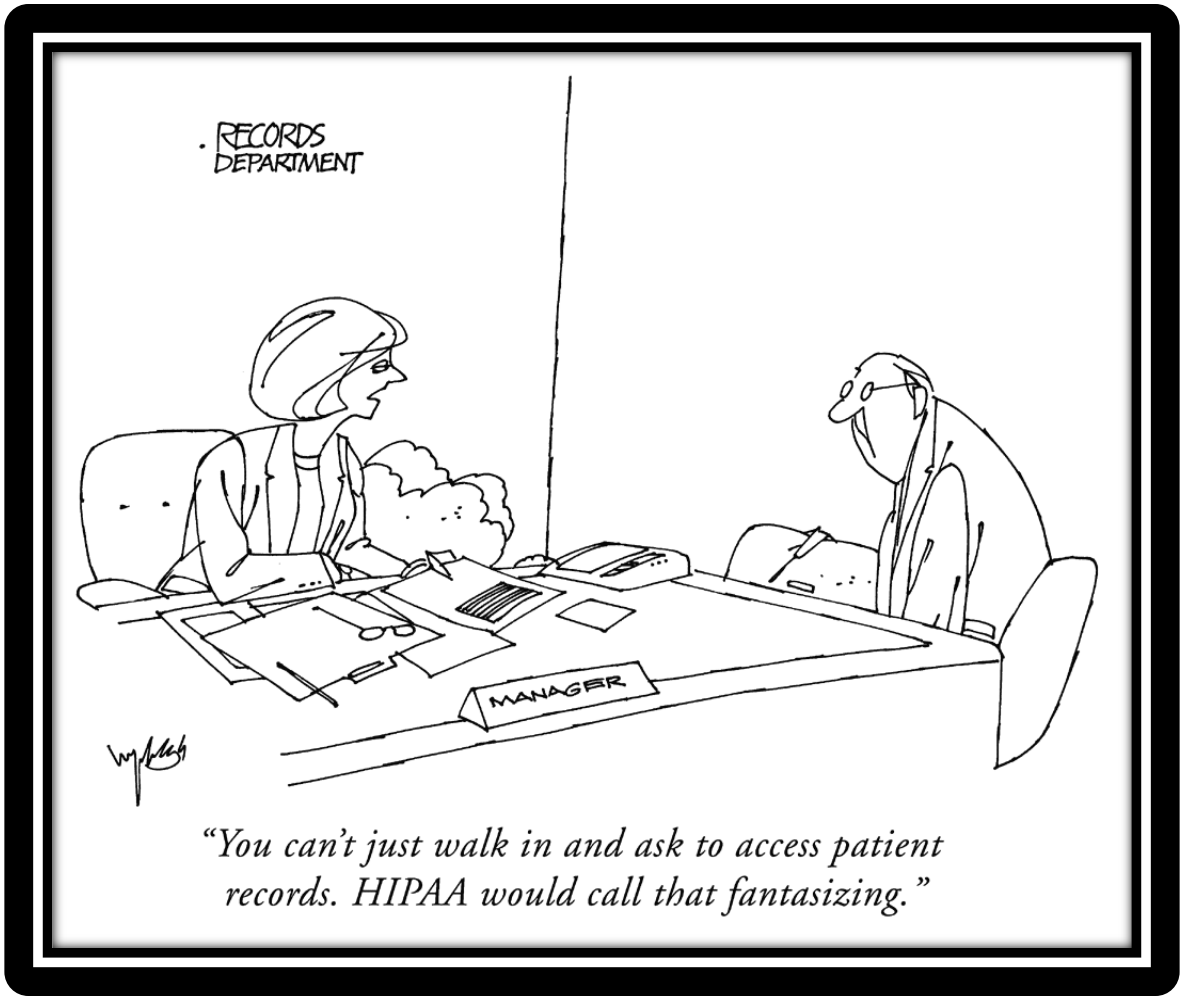
- HIPAA is a Floor
- Additional federal and state laws also govern confidentiality of drug and alcohol treatment records and behavioral health and mental health records.
- "More stringent" is standard to determine preemption; i.e., which law controls.
- "More stringent" = greater privacy protection and/or greater rights to individuals regarding protected health information.

Judicial and Administrative Proceedings

- Subpoenas
- Satisfactory assurances
- Court orders
  - Mental health information
  - Substance abuse information

Compliance Dates

- January 25, 2013 – Publication in Federal Register
- March 26, 2013 – Effective Date
- September 23, 2013 – Compliance Date
- September 22, 2014 – Conform existing BA contracts



"You can't just walk in and ask to access patient records. HIPAA would call that fantasizing."

Key Issues to Address

- Keeping a risk assessment up-to-date.
- Development/Update of HIPAA policies and procedures.
- Review and update of business associate agreements to include breach notification provisions, indemnification provisions, insurance requirements.
- Update of NPPs.
- Update breach response plan to include new test for determining whether you have a reportable breach.
- Encryption policies.
- Employee training and discipline.

QUESTIONS