Recent Changes to HIPAA Privacy Rule
2013 Omnibus Final Rule

Dennis Kennedy 859-426-2118
Dressman Benzinger LaVelle psc
dkennedy@dbllaw.com
What's the effect of most HIPAA presentations?

HIPAA-nosis
Multiple Choice Question: What does HIPAA really stand for?

A. Health Industry Paying all Attorneys Act

B. Healthy Income Protection for Attorneys Act

C. Huge Increase in Paperwork and Aggravation Act

D. All of the above
HIPAA Omnibus

- Earlier this year, HHS released its mega-final rule amending the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("Omnibus").

- It is effective as of March 26, 2013, and most provisions require compliance by September 23, 2013.
HIPAA Omnibus

This presentation will highlight the most notable changes to the HIPAA Privacy Rule.
Business Associates

- Expanded Definition
- Increased liability
- Revisions necessary to Business Associate Agreement
Expanded definition of “Business Associate”

- Includes health information organizations, E-prescribing gateway, or other entities that provide data transmission services to a Covered Entity and that requires access to PHI on a routine basis;

- A person that offers personal health records to individuals; and

- A subcontractor of a business associate.
Increased Liability for Business Associates

- Business Associates are now **directly liable** for compliance with certain HIPAA Privacy Rule requirements.
- Subcontractors are now “directly liable” for complying with Privacy & Security Rules.
A business associate may be **directly liable** for violations of the Privacy Rule for:

- Uses and disclosures of PHI in violation of the Privacy Rule;
- Failing to provide breach notification to the covered entity;
- Failing to disclose PHI to comply with an individual’s request for PHI;
- Failing to provide an accounting of disclosures; and
- Failing to make reasonable efforts to limit uses/disclosures of PHI to the minimum necessary to accomplish the intended purpose.
BAA Requirements

- Require compliance with the Security Rule obligations for electronic PHI;
- Report breaches of unsecured PHI to the covered entity;
- Comply with the Privacy Rule;
- If business associate subcontracts, enter into BAA with subcontractor;
- Draft new BAA unless grandfathered.
VICARIOUS LIABILITY?

- The Omnibus Rule also applies HIPAA’s civil and criminal penalties directly to business associates.
- If a contractor violates HIPAA, the HHS will rely on the federal common law of agency to determine whether to impose penalties on the contracting party such as the covered entity.
Marketing

- Communication about a product or service;
- Authorization generally required;
- Definition of marketing revised to include communications for which the covered entity receives remuneration directly or indirectly;
- Face-to-face exception still applicable; and
- New exception for refill reminders if remuneration is tied to cost.
Sale of PHI

- Prohibited without authorization;
- Defined broadly to include all disclosures for which the covered entity receives remuneration directly or indirectly;
- Several exceptions:
  - Sale or merger
  - Research
  - Public health activities
Fundraising

- General Rule: a covered entity may use or disclose PHI to a business associate or institutionally-related foundation for fundraising purposes.
- However, the PHI could only be:
  - Demographic information; and
  - Dates of service
Fundraising

- Demographic information now includes:
  - Name
  - Address
  - Age
  - Gender
  - DOB

- Additional information can now be used:
  - Department or service
  - Treating physician
Fundraising – New Rule

- Notification to the individual (Is it in the NPP?);
- Ability to opt out;
- Opting out must not be burdensome; and
- When you opt out it applies across the board.
Patient Rights

Right of Access

- Generally must provide access to individual in the form and format requested;
- This now applies to records maintained electronically;
- If not producible in the format requested, then must agree on proper format;
- Time limit to respond has been reduced for records stored off-site – down from 60 days to 30 days but may request 30-day extension.
Patient Rights

Right to Request Restrictions

- Generally an individual has a right to restrict use or disclosure of PHI;
- CE was not required to agree;

New Rule

- If individual pays for services in full out-of-pocket and restricts disclosure from being made to health plan, CE must honor.
Patient Rights

- The final rule requires modifications to, and redistribution of, a covered entity’s NPPs:
  - Health plans must include in their NPPs that they cannot use or disclose an individual's genetic information for underwriting purposes.
  - These health plans must re-issue their NPPs with the updated information.
Patient Rights – Notice of Privacy Practices

- NPPs must include a statement that any use or disclosure of PHI will be made only with written authorization of the individual;
- List categories of uses and disclosures requiring authorization;
- Include fundraising
- Include right to request restriction if paid out-of-pocket;
- Inform individual of right to receive notice of breach;
Omnibus’ final rule modifies the individual authorization and other requirements for disclosure of child immunization proof to schools.

The rule permits a covered entity to disclose proof of immunization to a school where the law requires the school to have such information and parent agrees.

Written authorization is no longer required to permit this disclosure – must still document conversation.
Decedents

- New rule allows family members or others who were involved in the care of the decedent to access the decedent's PHI.
- Requires covered entities to comply with HIPAA for 50 years following the decedent's death.
  - After that time, an individual's individually identifiable health information is no longer PHI.
- Covered entities may still disclose PHI of decedents for research purposes.
Breach Notification

General Rule:

- Must notify individual of a breach of unsecured PH.I
Breach Notification

Breach:

- The acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of the PHI.
Breach Notification

Previously:

- “Compromises the security or privacy of PHI” meant that the breach posed a significant threat of harm to the individual.

New rule:

- This has been eliminated – can no longer use to determine if a breach occurred.
Breach Notification – New Standard

- An impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach unless there is a low probability that the PHI has been compromised based on a risk assessment;
  - Note: “compromised” is no longer defined – can not use old meaning.
Breach Notification – Risk Assessment

- Risk assessment must include the following factors:
  - The nature and extent of the PHI involved;
  - The unauthorized person who received/used the PHI;
  - Whether the PHI was actually acquired or viewed; and
  - The extent to which the risk to the PHI has been mitigated.
What disease do you get from too much HIPAA?

HIPAA-titis
Thank you

Questions?