Changes to the HIPAA Privacy Rule

**Business Associates**

164.502(a)(4) - Extends direct liability for compliance with the Privacy Rule to business associates under the Privacy Rule for impermissible uses and disclosures.

164.502(b) - A business associate is directly liable for failing to make reasonable efforts to limit protected health information to the minimum necessary.

164.502(e)(1)(ii) - Business associates are directly liable for failing to enter into business associate agreements with subcontractors that create or receive protected health information on their behalf.

Notice of Privacy Practices

164.520(b)(1)(iii)(E) - Requires covered entities to include in their NPP statements of:
- most uses and disclosures of psychotherapy notes (where applicable).
- uses and disclosures of PHI for marketing purposes and disclosures that constitute a sale of PHI require authorization.
- uses and disclosures not described in the notice will be made only with authorization from the individual.

164.520(b)(1)(v)(a) - Requires covered entities to include in their notice of privacy practice a statement of the right of affected individuals to be notified following a breach of unsecured protected health information.

Student Immunizations

164.512(b)(1) - Permits covered entities to disclose proof of immunization to schools where State or other law requires the school to have such information prior to admitting the student. Written authorization will no longer be required to permit immunization disclosure, but covered entities will still be required to obtain agreement, which may be oral, from a parent, guardian or from the individual, if legally able to consent.

Hybrid Entities

164.105(a)(2)(iii)(C) - The covered entity itself, and not merely the health care component, remains responsible for complying with business associate arrangements and other organizational requirements. Requires that the health care component of a hybrid entity include all business associate functions within the entity.

Subcontractors

164.308(b)(1), 164.308(b)(2) - Covered entities do not have to sign a contract with a business associate that is a subcontractor; rather, it is the business associate that must execute a contract.

164.314 - Requires business associate agreements between business associates and subcontractors to conform to the requirements of the Security Rule.

Changes to the HIPAA Security Rule

**Hybrid Entities**

164.532(d), 164.532(e) - Allows covered entities (and business associates and business associate subcontractors) to continue to operate under certain existing contracts for up to one year beyond the compliance date of the revisions to the Rules (September 22, 2014).

**Notice of Privacy Practices**

164.520(b)(1)(ii)(E) - Requires covered entities to include in their NPP statements of:
- most uses and disclosures of psychotherapy notes (where applicable).
- uses and disclosures of PHI for marketing purposes and disclosures that constitute a sale of PHI require authorization.
- uses and disclosures not described in the notice will be made only with authorization from the individual.

**Subcontractors**

164.520(b)(1)(v)(a) - Requires covered entities to include in their notice of privacy practice a statement of the right of affected individuals to be notified following a breach of unsecured protected health information.

Changes to the HIPAA Breach Notification Rule

**Harm Standard Removed**

New standard:
- **Impermissible use/disclosure of (unsecured) PHI presumed to require notification, unless CE/BA can demonstrate low probability that PHI has been compromised based on a risk assessment of at least:**
  - Nature & extent of PHI involved.
  - Who received/accessed the information.
  - Potential that PHI was actually acquired or viewed.
  - Extent to which risk to the data has been mitigate.

5 Factors in Determining Penalty

1. The nature and extent of the violation.
   - a) Time period during which the violation(s) occurred.
   - b) The number of individuals affected.

2. The nature and extent of the harm resulting from the violation.
   - a) Reputational harm.

3. The history of prior compliance with the administrative simplification provision, including violations by the covered entity or business associate.
   - a) Indications of noncompliance.

4. The financial condition of the covered entity or business associate.

5. Such other matters as justice may require.

Public Health is Not Immune

Alaska DHHS settled a HIPAA Security Rule case for $1,700,000 in June 2012

- OCR’s investigation followed a breach report submitted by Alaska DHHS as required by the HITECH Act.
- The report indicated that a USB hard drive possibly containing ePHI was stolen from the vehicle of a DHHS employee.
- Over the course of the investigation, OCR found that DHHS did not have adequate policies and procedures in place to safeguard ePHI.
- DHHS had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule.
- $1,700,000 fine was under the old, less stringent penalty rules ($100 per violation, maximum of $25,000 for identical violation).