Changes to HIPAA Privacy and Security Rules

STEPHEN P. POSTALAKIS
BLAUGRUND, HERBERT AND MARTIN
300 WEST WILSON BRIDGE ROAD, SUITE 100
WORTHINGTON, OHIO 43085
SPP@BHMLAW.COM

PERSONNEL COUNCIL
FRANKLIN COUNTY BOARD OF DD
SEPTEMBER 22, 2009

Why these changes apply:

- County Boards of DD are considered "covered entities" under HIPAA as both Health Plans and Health Care Providers.
  - County Boards may also function as "business associates" under HIPAA.
- Generally, providers are "covered entities" because they are Health Care Providers.
- COG's, when contracting to perform services on behalf of a County Board, are acting as "business associates."

Definition of Breach

- Notification obligations only apply to breaches of unsecured PHI.
  - Unsecured PHI is PHI that is not secured with a technology that renders it unusable, unreadable, or indecipherable to unauthorized persons (i.e., encrypted; redaction is not sufficient)

Definition of Breach: Breaches involving Privacy Rule violations

- Breach is: unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI.
- Breach could be oral, written, or in electronic form.
- If breach is unauthorized but consistent with existing HIPAA regulations, no reportable breach has occurred.

Definition of Breach: Breaches involving significant risk of harm

- Once it is determined that the disclosure was impermissible under the HIPAA Privacy or Security Rule, a second harm threshold must be met:
  - The breach must pose a significant risk of financial, reputational, or other harm to the individual.
  - Only then is the notification requirement triggered.
  - A use or disclosure of protected health information that does not include identifiers, date of birth, and zip code does not compromise the security or privacy of the PHI.

How do you know if the breach poses a risk of **significant** harm?

- Covered entities must perform a risk assessment. Relevant factors are:
  - Type and amount of information involved.
  - Whether the covered entity took immediate steps to reduce risk of harm.
  - Who impermissibly used information, or to whom it was disclosed.
  - Whether it was returned to the covered entity prior to being used for an improper purpose.

Risk Assessments

- Covered entities carry the burden of proof to show why they did not report a disclosure.
- Accordingly, all risk assessments should be documented in the event the failure to report be challenged.

Exceptions to definition of breach

- Unintentional Access in Good Faith
- Inadvertent disclosure within a Covered Entity
- Person to who PHI is disclosed is not able to retain information

Unintentional Access in Good Faith

- Unintentional access or use of PHI
- By a workforce member acting under authority of the covered entity/business associate
- Done in good faith
- Within the scope of employment
- Does not result in further use or disclosure not permitted by HIPAA

Inadvertent disclosure within a Covered Entity

- Disclosure made inadvertently by a person authorized to access PHI to another person within the covered entity who is authorized to access PHI
- Information received as a result of such disclosure is not further used or disclosed in an impermissible manner

Person to whom PHI disclosed not able to retain information

- Person to whom PHI is disclosed would not reasonably have been able to retain the information.
- Requires good faith belief on part of disclosing individual that the unauthorized recipient is unable to retain information.

Timing of Notice to Affected Individuals

- Covered entities that have a security breach of PHI are required to provide written notification to each individual affected and Secretary of Health and Human Services (HHS):
  - Without unreasonable delay and no later than 60 calendar days following discovery of the breach.
  - Business associates of a covered entity must report a breach to the covered entity within same time frame

Form and Content of Notice

- Written notice:
  - By written communication, first class mail, to the individual.
  - Next of kin or personal representative, if deceased.
- Substitute notice: involves insufficient or out-of-date contact information
  - If the number affected is fewer than 10 people: alternative form of written notice, telephone, or other means.

Form and Content of Notice

- If number affected is greater than 10 people, substitute notice shall:
  - Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
  - Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

Form and Content of Notice

- Additional notice in urgent situations:
  - In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured PHI, the covered entity may provide information to individuals by telephone or other means, as appropriate, including written notice by first class mail

Form and Content of Notice cont'd.

- For breaches affecting 500 people or more, covered entity must:
  - Notify prominent media outlets serving the State or jurisdiction
  - Notify HHS in a manner specified by its website, at same time as notice of breach
- For breaches affecting less than 500, covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification to HHS for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

Form and Content of Notice cont'd

- General Provisions for Notice:
  - Brief description of what happened, including date of the breach and the date of the discovery of the breach, if known;
  - Description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

Form and Content of Notice cont'd

- General Provisions for Notice:
  - Any steps individuals should take to protect themselves from potential harm resulting from the breach;
  - Brief description of what covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
  - Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address

Effective Date

- Rules go into effect September 23, 2009
  - HHS says it will use its enforcement discretion not to impose penalties until February 23, 2010
  - Covered entities nevertheless need to comply with new security breach rules

Restriction Request Rules

- Currently, HIPAA allows individuals to request that certain PHI not be used by the covered entity.
- Covered entities are generally allowed to decline all such requests.
- As amended by ARRA, covered entities must comply with restriction requests where disclosure is:
  - To a health plan carrying out payment or health care operations (administrative, not treatment); **and**
  - The PHI pertains only to a health care item or service for which the health care provider has been paid in full.

Electronic Health Records

- ARRA creates new category called electronic health records ("EHR")
  - Electronic record of health-related information on an individual.
  - Disclosure accounting requirements for EHR are greater than that of PHI
  - Under new rules, covered entities must track disclosures of EHR for treatment, payment or healthcare operations.
    - To be developed by rule

Electronic Health Records Cont'd

- Covered entities cannot receive remuneration in exchange for PHI or EHR unless consent is given by individual whose information is being disclosed
- Individual has the right to obtain a copy of PHI in electronic format if the covered entity maintains an EHR of that information.
  - To accommodate portability of records

Changes to Civil Monetary Penalties

	Current Law	As amended
Penalty when could not know of violation	$100/$25,000	$100/$25,000 to $50,000/$1,500,000
Penalty for each violation (if for "reasonable cause, not willful neglect")	$100/$25,000	$1,000/$1000 to $50,000/$1,500,000
Penalty for willful neglect		$10,000/$250,000 to $50,000/$1,500,000
Penalty for willful neglect and not corrected		$50,000/$1,500.000 to no specified maximum

Enforcement of civil and monetary penalties

- State attorney generals now authorized to bring HIPAA enforcement actions against covered entities that violate HIPAA privacy or security rules
- HHS will conduct more frequent "periodic audits" to ensure compliance.
- Increased penalties went into effect immediately on signing of the act, February 2009.
- ARRA requires HHS to create a regulation that authorizes individuals affected by a HIPAA violation to receive a percentage of any civil or monetary penalty or settlement collected for the violation.