HITECH and HIPAA:
Highlights for Health Departments

Aimee Wall
UNC School of Government

When Congress enacted sweeping legislation in February designed to stimulate the nation's economy, it incorporated several provisions that have a direct impact on privacy practices of many health care providers, including local health departments.[1] Below is a brief summary of many of the key provisions of the new legislation. This summary is not intended to provide a comprehensive analysis of the new law but rather a quick snapshot of the major changes.

- **Breaches by covered entities and business associates**: The new law requires covered entities (CE) and business associates (BA)[2] to make certain notifications in the event a breach of PHI occurs. On August 24, 2009, DHHS issued interim final regulations[3] that implement these new breach notification requirements.[4] The regulations went into effect September 23, 2009, but DHHS does not plan to impose any sanctions based upon the new requirements until February 22, 2010.[5]

    - ***Breach defined***: The definition of the term "breach" is key to understanding these new notification requirements. A breach is the acquisition, access, use, or disclosure of protected health information [PHI] in a manner not permitted [by the HIPAA Privacy Regulation] which compromises the security or privacy of the PHI.
        - ***Risk of harm threshold:*** The breach must pose a significant risk of financial, reputational, or other harm to the individual.
        - ***Exceptions***: The term "breach" does not include
            - Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or a BA if the acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure not permitted by the HIPAA Privacy Regulation.

---

[1] Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5). Full text of the legislation can be found online from the Library of Congress at http://thomas.loc.gov/.

[2] The term "covered entity" refers to entities required to comply with the HIPAA Privacy and Security Regulations. A "business associate" is, in short, an entity that uses identifiable health information to perform functions or activities on behalf of a covered entity. 45 C.F.R. 160.103.

[3] 74 Fed. Reg. 42740-42770 (Aug. 24, 2009).

[4] The HIPAA Privacy and Security Regulations can be found in 45 C.F.R. Parts 160, 162 and 164. Full text of the regulations is available online from the DHHS Office of Civil Rights at http://www.hhs.gov/ocr/hipaa.

[5] 74 Fed. Reg. 42756-57 ("…we will use our enforcement discretion to not impose sanctions for failures to provide the required notifications for breaches that are discovered before…February 22, 2010. During this initial time period…we expect covered entities to comply with this subpart and will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance.").

- Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA if the information is not further used or disclosed in a manner prohibited by the HIPAA Privacy Regulation.
- A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- ***Notification limited to breaches of "unsecured PHI":*** The notification requirements apply only when the PHI used or disclosed was "unsecured." PHI is considered "unsecured" if it is not secured using a technology or methodology specified by guidance issued by the U.S. Department of Health and Human Services (DHHS). The guidance was issued in draft form on April 17, 2009 and was amended to address concerns raised by public comments.[6] In short, the guidance describes technologies and methodologies that render PHI "unusable, unreadable, or indecipherable to unauthorized individuals – with a primary focus on (1) encryption and (2) destruction of storage media.

- ***Discovery of a breach:*** In general, a breach is treated as discovered as of the first day on which such breach is known to the CE, or, *by exercising reasonable diligence would have been known to the CE.*

- ***CE notifications required:*** If a CE discovers a breach, various notifications may be required.
  - ***Individual***: Upon discovery of a breach of unsecured PHI, the CE must notify each individual whose PHI has been or is reasonably believed by the CE to have been, accessed, acquired, used, or disclosed. The notification must take place "without unreasonable delay" (no more than 60 calendar days). The regulation outlines the content required in the notice and guidelines for appropriate methods of notification.
  - ***Media***: Upon discovery of a breach of unsecured PHI involving more than 500 residents of a State or jurisdiction, the CE must notify prominent media outlets serving the State or jurisdiction. The notification must take place "without unreasonable delay" (no more than 60 calendar days).
  - ***DHHS***: The CE must notify DHHS of all breaches of unsecured PHI. For larger scale breaches (>500), the notification must occur at the same time the individual is notified. For smaller scale breaches (<500), the CE must provide an annual log or accounting of breaches to DHHS not later than 60 days after the end of the calendar year.

- ***BA notifications required***: If a BA discovers a breach, it must notify the CE "without unreasonable delay" (no more than 60 calendar days).

[6] The current version of the guidance is available online at http://www.hhs.gov/ocr/privacy/ or can be found at 74 Fed. Reg. 42742-43.

- ***Law enforcement delay***: Law enforcement officials may direct a CE to delay a required notification if the officials believe that it would impede a criminal investigation or cause damage to national security.

- **Breaches by non-covered entities**: There are certain types of entities that are not governed by the HIPAA regulations but collect consumer health information in the form of "personal health records." According to the new law, a "personal health record" is "an electronic record of individually identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or for the individual." The law outlines breach notification requirements for these types of entities and directs the Federal Trade Commission (FTC) to adopt implementing regulations, which it did on August 25, 2009.[7] Vendors of personal health records must notify individuals and the FTC when there has been a breach of information from a personal health record maintained or offered by the vendor. Other notification requirements apply as well. Both the FTC and DHHS regulations emphasize that they do not overlap. In other words, an entity that is subject to the DHHS regulations (such as a local health department) is not subject to the FTC regulations.

- **Business associates**

  - ***Direct enforcement authority***: When the HIPAA Privacy and Security Regulations were initially drafted, DHHS's enforcement authority was limited to "covered entities" (CEs). Recognizing that a CE may need to share PHI with other organizations, DHHS created the concept of "business associates" (BAs) in the HIPAA regulations. A BA is basically an entity that needs to have health information in order to do work on behalf of the CE (such as a billing agency). Some BAs are covered entities but many are not. For those that are not CEs, DHHS lacked the authority to *directly* require BA compliance with the HIPAA Privacy and Security Rules, but it *indirectly* require compliance because BAs need to enter into agreements or contracts with CEs agreeing that they will comply with many of the regulatory requirements. Under the new law, many of the provisions of the HIPAA Privacy and Security Regulations now apply *directly* to business associates (BAs) in the same manner that they apply to CEs.
    - ***Security***: The provisions that BAs must comply with include 164.308 (administrative safeguards), 164.310 (technical safeguards), 164.312 (physical safeguards), 164.316 (policies and procedures and documentation).
    - ***Privacy***: If a BA uses or discloses PHI in violation of its agreement or the Privacy Regulation, it can now be subject to civil and criminal enforcement in the same manner as a covered entity.

  - ***BA contracts required***: Each organization that provides data transmission of PHI to a CE or its BA and that requires access on a routine basis to PHI is required to have a BA agreement.

[7] 74 Fed. Reg. 42,962-82 (adding new 16 C.F.R. Part 318).

- **Enforcement**

    - ***Use of civil monetary penalties (CMPs):*** CMPs collected through enforcement of the HIPAA privacy regulation must now be transferred to DHHS for the purpose of funding HIPAA enforcement. DHHS must establish a methodology for distributing a percentage of CMPs collected to the individual(s) harmed by a violation.

    - ***Enforcement by states***: When the HIPAA Privacy and Security Regulations, the federal government was the exclusive avenue available for enforcement. The new legislation authorizes the state attorneys' general to bring a civil action to enforce the HIPAA Privacy Regulation in order to (1) enjoin further violations or (2) obtain damages for individuals harmed (calculated pursuant to a statutory formula).

- **Individual rights**

    - ***Requested restrictions*****:** The Privacy Regulation allows a person to request restrictions on the disclosure of information for treatment, payment and health care operations. Previously, covered entities were not required to agree to such requests. The new legislation *requires* a CE to comply with requests if (1) the request relates to disclosures to a health plan for the purposes of payment or health care operations and (2) the provider has been paid in full out of pocket for the health care item or service.

    - ***Accounting of disclosures*****:** Under the HIPAA Privacy Regulation, an individual has a right to request and receive an accounting of disclosures made by a CE during the previous six years. The regulation identifies several exceptions, most notably excepting disclosures made for treatment, payment and health care operations (TPO). The new legislation directs DHHS to revise the regulation to require that if a CE maintains electronic health records, the CE must be able to account for TPO disclosures for three years. It allows the CE to impose a reasonable fee for providing such an accounting. The effective date for the new requirement will vary depending upon when the entity acquires an electronic health record.

    - ***Access:*** Under the HIPAA Privacy Regulation, individuals have the right to request and obtain a copy of PHI maintained by a covered entity, subject to some exceptions. Under the new law, an entity that uses or maintains electronic health records must allow the individual to have access to his or her PHI in an electronic format. The fee charged must not be greater than the entity's labor costs involved in responding to the request.

- **Other DHHS directives:** The new law directs DHHS to do the following:
    - Amend the definition of "psychotherapy notes" in 45 CFR 164.501 to include "test data that is related to direct responses, scores, items, forms protocols, manuals, or other materials that are part of a mental health evaluation, as determined by the mental health professional providing treatment or evaluation."
    - Implement a public education initiative and have regional office staff available to help covered entities, business associates and the public.

- Issue annual guidance on "the most effective and appropriate technical safeguards" for implementing HIPAA's security requirements
- Issue guidance about the minimum necessary provisions.
- Review and evaluate the definition of health care operations. If appropriate, it must revise the definition by regulation to eliminate activities that should be done with de-identified information or with patient authorization.
- Issue guidance on how to best implement the de-identification requirements in the HIPAA Privacy Regulation.
- Provide for periodic audits to ensure that covered entities and business associates are complying with the requirements of the HIPAA Privacy Regulation.

Acronym Refresher

ARRA: American Recovery and Reinvestment Act (aka Stimulus Bill)
BA: Business Associate
CE: Covered Entity
CFR: Code of Federal Regulations
CMP: Civil Monetary Penalties
DHHS: U.S. Department of Health and Human Services
FTC: Federal Trade Commission
HIPAA: Health Insurance Portability and Accountability Act of 1996
HITECH: Health Information Technology for Economic and Clinical Health Act (part of the Stimulus Bill)
OCR: DHHS Office of Civil Rights
PHI: Protected Health Information
TPO: Treatment, Payment and Health Care Operations