United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

HIPAA COW Webinar: HIPAA, HITECH and Business Associates

November 11, 2010
12:00-1:30pm (CST)

Sarah Radermacher, JD
Office for Civil Rights
U.S. Department of Heath and Human Services

Disclaimer

The content of this presentation reflects the views of the author. No statement in this presentation should be construed as an official position of the Office for Civil Rights (OCR), or the Department of Health and Human Services (DHHS).

Presentation Topics

- HIPAA and Business Associates Prior to HITECH
  - Statutory Background and Jurisdiction
  - Business Associates and Indirect Accountability
- HITECH and Business Associates
  - Background and Subtitle D
  - OCR Rulemaking Directives
- OCR Proposed Rulemaking
  - Proposed Business Associate Provisions
  - Compliance Date and Transition Period
- Key Business Associates Take-Aways

HIPAA and Business Associates: Prior to HITECH

What is Covered?

- Protected Health Information (PHI):
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium
  - by Covered Entities or their Business Associates
- Not PHI:
  - De-identified information
  - Employment records
  - FERPA records

Who is Covered?

- HIPAA Covered Entities (CEs):
  - Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
  - Health plans
  - Health care clearinghouses
- Business Associate (BA) Relationships

HIPAA and Business Associates: Prior to HITECH

- **§ 160.103 - Definition**
  - A person who performs functions or activities on behalf of, or certain services for, covered entities that involve the use or disclosure of PHI
  - Includes contractors & agents
  - Examples: third party administrators or pharmacy benefit managers for health plans, claims processing or billing companies, transcription companies, and persons who perform legal, actuarial, accounting, management, or administrative services for CEs that require access to PHI

- **§ 164.502(e) – Disclosures to BAs.** Permits disclosures to business associates if the CE obtains satisfactory assurances that the BA will appropriately safeguard the information.

- **§ 164.504(e)(1) – BA Contracts.** Enumerates certain requirements to create contractual BA obligations:
  - Permitted, required disclosures
  - BA obligations (no further use or disclosure; use of appropriate safeguards; reporting; ensuring the same of agents; making information available for access, amendment, accounting, making information available to the Secretary; and termination requirements)
  - Authorized termination

- **Comparable Security Rule provisions are at §§ 164.308(b) and 164.314(a).**

American Recovery and Reinvestment Act of 2009 (ARRA)

Title XIII: Health Information Technology for Economic and Clinical Health Act (HITECH Act)

Subtitle A: Promotion of HIT through the Office of the National Coordinator for HIT (ONC)

Subtitle B: Testing of HIT through the National Institute of Standards and Technology (NIST)

Subtitle C: Grants and Loan Funding for Incentives for the Use of HIT

Subtitle D: Improved Privacy and Security Provisions

The HITECH Act and Business Associates

- Clarifies that any entity that provides data transmission of PHI to a CE and that requires routine access to PHI or that contracts with a CE to provide a PHR is a BA and must have a BA agreement with the CE. See section 13408.
- Applies the HIPAA Security Rule's requirements for administrative, physical, and technical safeguards, policies and procedures, and documentation directly to BAs. See section 13401(a).
- Provides that a BA may use or disclose PHI only if such use or disclosure is in accordance with the HIPAA Privacy Rule's required terms for BA contracts and applies the knowledge of noncompliance requirements to BAs. See section 13404(a).
- Makes the HITECH Act's additional requirements that relate to privacy and security and are made applicable to covered entities also applicable to BAs, and mandates that these requirements be incorporated into the BA contract. See sections 13401(a) and 13404(a).
- Extends HIPAA's civil and criminal penalties to BAs for violations of these provisions. See sections 13401(b) and 13404(c).

NPRM, Business Associates: Definitional Additions

- **Patient Safety Organizations**
- **Health Information Organizations**
- **E-Prescribing Gateways**
- **Others that provide data transmission** of PHI and require access to such PHI on routine basis
- **PHR vendors** that offer a PHR to one or more individuals on behalf of covered entities are BAs (possibly with respect to only some individuals)
- **"Conduits"** that only access PHI on random or infrequent basis to support transport are not BAs

NPRM, Business Associates: Definitional Additions

- **Subcontractors**
  - Would be BAs, if they create, receive, maintain, or transmit PHI on behalf of a BA. Defined at § 160.103.
- **Excepted entities for which BA agreement is not required**
  - Health care provider with respect to treatment disclosures
  - Plan sponsor with respect to group health plan
  - Certain government agencies (performing enrollment and eligibility activities for another agency's government health plan)

NPRM, Business Associates: Security Rule

- **Inserted references, as appropriate, throughout the Security Rule**
- **Modifications to § 164.308(b) (BA contracts & other arrangements):**
  - Removed exceptions and included them into the definition of BA.
  - BAs must obtain satisfactory assurances from subcontractor(s)
  - CEs liable as BAs when actions as BA violate satisfactory assurances
  - Additional reference to requirement for documentation of satisfactory assurances regarding those that BAs obtain from subcontractor(s)
- **Modifications to § 164.314 (organizational requirements):**
  - BA contracts must require BAs to comply with applicable provisions of the Security Rule
  - BA contracts must require BAs to report any security incident to CEs, including breaches of unsecured PHI as required at **§ 164.410.**
  - Removed certain provisions already addressed by the Privacy Rule
  - Organizational requirements apply to contracts or other arrangements between BAs and subcontractors

NPRM, Business Associates: and Privacy Rule Uses and Disclosures

- **Modifications to § 164.502(a) (general rules):**
  - Limits BA uses and disclosures to those permitted or required by the HIPAA Rules
  - Clarifies other subparagraphs (1) and (2) only apply to CEs
  - Adds provisions to address BAs' permitted/required uses and disclosures
    - (4) Business Associates: Permitted uses and disclosures.
      - If failure to enter into such BA agreement; and
      - General prohibition from BA's use or disclosure of PHI in manner that would violate the Privacy Rule, if done by the CE
    - (5) Business Associates: Required uses and disclosures. Liability for failure to:
      - Furnish any information the Secretary requires to investigate whether the BA is in compliance with the regulations
      - Provide individuals with electronic access to the requested PHI it maintains electronically, as necessary to satisfy a CEs obligations under § 164.524(c)(2)(ii) and (3)(ii)

NPRM, Business Associates: and Privacy Rule Uses and Disclosures

- **Modifications to § 164.502(b) (minimum necessary):** Requires that BAs, like CEs, limit the PHI they use, disclose, or request to the minimum necessary standard

- **Modifications to § 164.502(e): Disclosures to BAs**
  - Exceptions moved to definition of BA
  - BA may disclose PHI to a BA subcontractor, and allow the subcontractor to create or receive PHI on its behalf, if it obtains satisfactory assurances that the subcontractor will appropriately safeguard the information

NPRM, Business Associates:
Privacy Rule Business Associate Contracts

- Removal of required reporting to the Secretary when termination of a BA contract is not feasible.
- BA that is aware of noncompliance by its BA subcontractor must respond to the situation in the same manner
- Certain modifications to BA contract requirements:
  - Security Rule compliance, where applicable
  - Report breaches per the Breach Notification Rule
  - Ensure that BA subcontractors agree to the same restrictions and conditions that apply to the BA

NPRM, Business Associates:
Privacy Rule Business Associate Contracts

- To the extent BA to is to carry out CE's obligation under the Privacy Rule, it must comply with requirements that apply to the CE in the performance of such obligation
- Include references to the Security Rule in § 164.504(e)(3) (Other Arrangements)
- New § 164.504(e)(5) applies BA contract requirements to BAs and their BA subcontractors
- Removal of reference to "subcontractors" in §§ 164.504(f)(2)(ii)(B) and 164.514(e)(4)(ii)(C)(4)

NPRM, Business Associates: Enforcement Rule

- Direct BA liability recognized by insertion of the term "BA," where applicable, following references to "CE" in Subparts C and D

- Added language to recognize that CEs (and BAs) are liable for actions of BAs acting as agents within the scope of agency

NPRM, Business Associates: Compliance Date & Transition Period

- Covered entities and BAs will have 240 days from publication of final rule to comply
  - Rule will become effective 60 days after publication
  - Additional 180-day compliance period

- Covered entities and BAs will have up to one year after compliance date to revise BA agreements
  - BAs must comply with other applicable provisions of Privacy and Security Rules during this transition period

NPRM, Business Associates: Key NPRM Take-Aways

- A Final Rule is forthcoming
- An entity would be a BA if it meets the definition
- BAs would be directly liable for noncompliance of certain provisions of the HIPAA Rules:
  - Security Rule compliance
  - Impermissible uses and disclosures under Privacy Rule
    - BA uses/disclosures must comply with those permitted or required by the Privacy, Security and Enforcement Rules, as well as the BA agreement
    - BAs must obtain satisfactory assurances from subcontractors
    - BAs must take reasonable steps in response to impermissible pattern or practice of subcontractor
    - CEs (and BAs) are liable for the actions of BAs acting as agents within the scope of agency
  - Failure to disclose to Secretary or provide e-access
- Other Privacy Rule related obligations would be contractual
- BAs that have not done so already, would need to take steps to enhance their security procedures and ensure that privacy protections are in place to prevent impermissible uses and disclosures of PHI under their control
- Sample business associate contract language is forthcoming

NPRM, Business Associates: Comments

- Published July 14, 2010 (75 Fed. Reg. 40868)
- Comments were due on September 13, 2010
- Roughly 300 comments submitted
- Well over 200 addressed the BA provisions

More Information

- http://www.hhs.gov/ocr/privacy
- Fact sheets
- OCR's enforcement program
- Security Rule
- Breach Notification Rule
- Patient Safety Rule
- Genetic Information Nondiscrimination Act
- Recent HITECH Act Rulemaking & Activities