United States Department of Health & Human Services
Office of the Secretary
Office for Civil Rights (OCR)

HIPAA/HITECH Omnibus Final Rule Requirements for Business Associates Changes to the Breach Notification Rule

HIPAA Security Assurance Conference

May 22, 2013

Kathleen Kenney, JD
Health Information Privacy Specialist
David Holtzman, JD, CIPP/G
Senior Health Information Technology and Privacy Specialist

Omnibus Components

- **HITECH Privacy & Security**
  - Business associates (BA)
  - Marketing & Fundraising
  - Sale of protected health information (PHI)
  - Right to request restrictions
  - Electronic access
- **HITECH Breach Notification**
- **HITECH Enforcement**
- **GINA Privacy**
- **Other Modifications**
  - Research
  - Notice of privacy practices (NPP)
  - Decedents
  - Student immunizations

Important Dates

- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
- Transition Period to Conform BA Contracts – Up to September 22, 2014, for Qualifying Contracts

Definition of Breach

- 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 mitigated

Definition of Breach

- Exceptions for inadvertent, harmless mistakes remain
- Exception for limited data sets without dates of birth & zip codes removed

Breach Notification

- Makes permanent the notification and other provisions of the 2009 interim final rule (IFR), with only minor changes/clarifications
  - E.g., clarifies that notification to Secretary of smaller breaches to occur within 60 days of end of calendar year in which breaches were *discovered* (versus *occurred*)

Business Associates

- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule; directly liable for violations
- BAs must comply with the use or disclosure limitations expressed in BA contract and those in the Privacy Rule; directly liable for violations
- BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities
- Subcontractors of BA are now defined as BAs
  - BA liability flows to all subcontractors

Business Associate Liability

- Direct liability
  - Impermissible uses and disclosures (including more than minimum necessary)
  - Failure to comply with Security Rule
  - Failure to provide breach notification
  - Failure to provide e-access as provided in BA contract
  - Failure to disclose PHI to HHS for compliance and enforcement
- Contractual liability for requirements of the BA contract

Business Associates: Conduits

- The Final Rule provides important clarification about the status of “conduits” as business associates.
- A conduit, whether of paper or electronic PHI, only provides transmission services, including any temporary storage of PHI incidental to the transmission service.
- Service provider is a business associate if the data is maintained in the performance of its function
  - Even if the agreement with the covered entity does not contemplate any access or access only on a random or incidental basis.
  - The test is persistence of custody, not the degree (if any) of access.

Business Associates: Downstream Contractors

- Downstream entities that work at the direction of or on behalf of a business associate and handle PHI are required to comply with the applicable Privacy and Security Rule provisions, just like the “primary” business associate and are subject to the same liability for failure to do so.
- This does not require the covered entity to have a contract with the subcontractor; that obligation remains on each business associate.

Business Associates: Transition Provisions

- The Final Rule grandfathers certain business associate agreements to September 23, 2014
- The business associate agreement must have been in existence prior to the publication of the Final Rule (January 25, 2013), have complied with HIPAA prior to the publication date and not be renewed or modified during the grandfather period.
- An automatic renewal, under a so-called evergreen clause, does not constitute a renewal or modification for purposes of the availability of the grandfather period.

For More Information

www.hhs.gov/ocr/privacy/