HINSHAW

Alerts

New HIPAA Requirements for Business Associates and Their Subcontractors

February 1, 2013
Health Law Alert

This Health Law Alert *is the second in a six-part series Hinshaw & Culbertson is publishing detailing the significant changes to HIPAA privacy, security, enforcement, and breach notification rules as part of the Omnibus Final Rule.*

The Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules generally permit a covered entity to disclose protected health information (PHI) to a business associate and to allow a business associate to create, receive, maintain or transmit protected health information on a covered entity's behalf, provided the covered entity obtains satisfactory assurances from the business associate that the business associate will appropriately safeguard the information it receives. This article focuses on the new definition of who is a "business associate" and on new duties and liabilities for business associates and their subcontractors under the omnibus final rule (Final Rule).

Definition of a Business Associate

One significant change in the Final Rule involves changes in the definition of "business associate." HIPAA generally defines a business associate as a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of PHI. The definition includes, by way of example, various functions that a business associate may provide, including claims processing or administration; utilization management; benefit management; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services. The Final Rule adds "patient safety activities" to the list of functions and activities that give rise to a business associate relationship.

In the Final Rule, the U.S. Department of Health and Human Services Office of Civil Rights (OCR) significantly expands the types of persons or entities that qualify as business associates. The Final Rule explicitly expands the definition of "business associate" to include: health information organizations; e-prescribing gateways; other entities that provide data storage or transmission services for covered entities and that require access on a routine basis; and entities that offer a personal health record to individuals on behalf of a covered entity.

Subcontractors. In expanding the scope of the definition of "business associate," OCR has also indicated that a business associate includes a "subcontractor that creates, receives, maintains or transmits protected health information on

Attorneys

Michael A. Dowell

behalf of the business associate." The term "subcontractor" is defined in Section 160.103 of HIPAA as "a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate." Throughout the Final Rule and commentary, OCR states that although the use of the term "subcontractor" suggests that there is a contract in place between the parties, an individual or entity that fits within the definition of a subcontractor will be treated as a subcontractor even if the business associate has failed to enter into a business associate agreement (BAA) with that individual or entity. The obligation to enter into BAAs with subcontractors lies with the business associate subcontracting or delegating its responsibilities and not with the covered entity.

Persons and Entities Who Are Not Business Associates

The definition of a "business associate" now includes a list of activities that specifically fall outside the definition of a "business associate." In the Final Rule, OCR specifically lists the following exceptions to the definition of a business associate:

- A health care provider with respect to disclosures concerning the treatment of the individual;
- A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, as long as the plan and the sponsor comply with the requirements of the privacy rule;
- A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law;
- A covered entity participating in an organized health care arrangement that performs various business associated functions or activities on behalf of such organized health care arrangement; and
- Patient safety organizations.

Application of the HIPAA Security Rule to Business Associates

Section 13401 of the Health Information Technology for Economic and Clinical Health (HITECH) Act provides that the security rule's administrative, physical and technical safeguard requirements, as well as the rule's policies and procedures and documentation requirements, apply to business associates in the same manner as these requirements apply to covered entities, and business associates can be civilly and criminally liable for violations of these provisions. In the final rule, OCR modified the security rule to implement the HITECH Act's provisions extending direct liability for compliance with the security rule to business associates and to business associate subcontractors.

Application of HITECH Privacy Requirements to Business Associates

Under the privacy rule, business associates may use or disclose PHI only in accordance with their BAAs or as required by law. Moreover, a business associate may not use or disclose PHI in a manner prohibited by the privacy rule if done by a covered entity (unless HIPAA specifically permits such use and disclosure for business associates). The commentary to the Final Rule notes that not all of the requirements of the privacy rule apply to business associates. For example, business associates do not need to provide a notice of privacy practices or designate a privacy official. Business associates must obtain "satisfactory assurances" in the form of BAAs from their subcontractor business associates. Lastly, business associates must furnish any information that HHS requires to investigate whether the business associate is in compliance with the regulations.

Liability for Actions of a Business Associates

The HITECH Act imposes direct liability on business associates (including business associate subcontractors) for a specific set of obligations under HIPAA's privacy, security and breach reporting rules. The business associate has to also comply with the contractual obligations imposed under a BAA.

Direct Liability. Business associates are directly liable under HIPAA HITECH rules for the following:

- Compliance with the requirements of the BAA;
- Failure to enter into BAAs with subcontractors that create or receive PHI on their behalf;
- Impermissible uses and disclosures;
- Failure to provide breach notification to the covered entity;

• Failure to provide access to a copy of electronic PHI to either the covered entity, the individual, or the individual's designee (whichever is specified in the BAA);
• Failure to disclose PHI where required by HHS to investigate or determine the business associate's compliance with HIPAA;
• Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request;
• Failure to provide an accounting of disclosures; and
• Failure to comply with the applicable requirements of the security rule.

Agency Liability. The Final Rule makes covered entities and business associates (as principals) liable for the acts of their business associates that are agents, in accordance with the federal common law of agency. The test for determining if a business associate constitutes an agent of the covered entity is whether the covered entity has the "right or authority to control the business associate's conduct in the course of performing a service on behalf of the covered entity," regardless of the terms of a BAA. For liability to attach to a covered entity for the actions of its business associate, in addition to determining that the business associate is an agent of the covered entity, the business associate must have also been acting within the scope of the agency/principal relationship. This significantly impacts the relationship of covered entities and their business associates, potentially requiring greater monitoring by the covered entity when the business associate is an agent. An analysis of whether a business associate is an agent will be fact specific, taking into account the terms of a BAA as well as the totality of the circumstances involved in the ongoing relationship between the parties.

Modifications to Business Associate Agreement Requirements

Through the Final Rule, OCR modified a number of the specific requirements for BAAs to implement Section 13404 of the HITECH Act. Among other things, OCR has removed the requirement that covered entities report to the U.S. Department of Health and Human Services when a business associate is failing to perform in accordance with its BAA but termination of the agreement is not feasible.

OCR added a new provision at 45 CFR § 164.504(e)(1)(iii), applicable to business associates who engage subcontractors, which provides that a business associate that is aware of noncompliance by its subcontractor must respond to the situation as a covered entity would (i.e., by trying to cure the breach, ending the violation or terminating the contract). The Final Rule also adds a new provision at 45 CFR § 164.504(e)(2)(ii)(H), which specifically provides that when a business associate carries out a covered entity's obligation under the privacy rule, it must comply with the privacy rule requirements that apply to the covered entity in the performance of that function or responsibility.

A new 45 CFR § 164.504(e)(5) has been added, which mandates that the provisions governing BAAs and implementation specifics for arrangements between covered entities and business associates also apply to the arrangements and agreements between business associates and subcontractors. Specifically, the final rule mandates the following requirements for BAAs:

• That the business associate comply, where applicable, with the security rule with respect to electronic PHI.
• That the business associate report breaches of unsecured PHI as required by the breach notification rule.
• That the business associate ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the business associate agree to the same restrictions that apply to the business associate.
• That to the extent the business associate is to carry out the covered entity's obligation under the privacy rule, the business associate comply with the requirements of the privacy rule that apply to the covered entity in the performance of such obligation.

Compliance Deadline

The Final Rule is effective on March 26, 2013; however, OCR has provided transitional relief that allows plans and business associates to continue to operate under their existing BAAs until September 23, 2014, or, if earlier, the date the BAA is renewed or modified. However, to qualify for the transitional relief, the BAA must have been in effect on January 25, 2013, so any BAAs not finalized by that date will need to be amended for the final regulations by September 23, 2013, a whole year earlier.

Covered Entities and Business Associates Should Take the Following Actions to Achieve Compliance

To ensure compliance with the Final Rule, covered entities, business associates and subcontractors will need to take a number of steps promptly, including the following:

- Business associates will need to perform a variety of actions to ensure timely compliance, including:
  - Assess which of their service providers may qualify as subcontractors
  - Perform a risk assessment to identify vulnerabilities or weaknesses in HIPAA compliance;
  - Implement appropriate administrative, physical and technical safeguards to address those vulnerabilities;
  - Develop and implement policies, procedures and forms addressing privacy and security obligations; and
  - Developing a template BAA to use with subcontractors.
- Covered entities should begin assessing their current business associate arrangements to determine whether any changes to their BAAs may be needed in order to comply with the Final Rule.
- Confirm that BAAs are in place where required (including subcontractor arrangements).
- Review and modify existing HIPAA privacy and security policies to comply with the Final Rules, including:
  - Revise breach notification policies to address the new "low probability" standard and required risk assessment factors;
  - Address the expanded access right to permit individuals to receive an electronic copy of their health information;
  - Address the limitations on marketing, fundraising and the sale of PHI;
  - For covered entities, revise restriction request policies and confirm that requests can be granted and implemented properly for individuals who have paid out of pocket and in full; and
  - For health plans, address the limitations on the use of genetic information for underwriting purposes pursuant to the Genetic Information Nondiscrimination Act (GINA).
- Re-train relevant workforce members on their revised privacy, security, and breach notification policies. Emphasis should be placed on training workforce members to identify and report breaches of unsecured PHI in a timely manner.
- Revise notice of privacy practices to include additional statements specified by the Final Rule and redistribute them consistent with the rule. Health plans have separate requirements for redistribution.

How We Can Help

Hinshaw & Culbertson LLP attorneys have extensive experience developing and advising on privacy and information security programs. If you have questions or need assistance in determining how to make the requisite changes to your policies, procedures, and practices in order to come into compliance with the Final Rule, please call Michael A. Dowell or your regular Hinshaw attorney.

Download PDF

This alert has been prepared by Hinshaw & Culbertson LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship.