akerman

Practice Update

HIPAA Omnibus Final Rule Imposes New Obligations on Business Associates

February 12, 2013

By Elizabeth F. Hodge

On January 25, 2013, the Department of Health and Human Services/Office for Civil Rights (HHS/OCR) published in the Federal Register (78 Fed. Reg. 5566) the long-awaited final rule titled Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules (Omnibus Final Rule). The rule becomes effective March 26, 2013 and compliance is required by September 23, 2013.

One of the purposes of the final rule is to strengthen the privacy and security protections for protected health information (PHI) of patients that is maintained in electronic formats. To achieve that goal and plug what was perceived as a gap in the existing HIPAA regulations, the omnibus final rule imposes direct liability on business associates and their subcontractors for violations of the HIPAA Security Rule (which applies to PHI in electronic formats) and for uses and disclosures of any PHI in violation of the HIPAA Privacy Rule.

Expanded Definition of "Business Associate"
The final rule expands the definition of who is a Business Associate to include:

Related People

Elizabeth F. Hodge

Related Work

Data Privacy and Security
Healthcare

Related Offices

Tampa

1. Health information organizations, e-prescribing gateways, or other persons that provide data transmission services with respect to PHI to a covered entity and that requires routine access to such PHI,
2. Persons offering a personal health record on behalf of a covered entity, and
3. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.

HHS also revised the definition of "Business Associate" to make clear that it applies to entities that "maintain" PHI for a covered entity. In the commentary, HHS states that data storage companies that maintain PHI on behalf of covered entities (whether in digital or hard copy form) are business associates, regardless of whether the company actually views the information it holds. There is still a narrow exception for those businesses that are conduits, but the commentary makes clear that this category only applies to "mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services."

Increased Liability for Business Associates and Subcontractors

Business Associates and their subcontractors are now directly liable for violations of the HIPAA Security Rule and for uses and disclosures of PHI in violation of the HIPAA Privacy Rule. A covered entity is liable, in accordance with the Federal common law of agency, for civil monetary penalties based on the act or omission of any of its agents, including its business associates, acting within the scope of the agency. Similarly, a Business Associate is liable for civil monetary penalties for violations based on the act or omission of any agent of the Business Associate, including subcontractors, acting within the scope of the agency.

Business Associates – and subcontractors—also now have these additional responsibilities under the new omnibus final rule:

1. Keep records and submit compliance reports to HHS when HHS requires such disclosure to determine whether a covered entity or business associate is complying with HIPAA,
2. Disclose PHI as needed by a covered entity to respond to an individual's request for an electronic copy of his or her PHI,
3. Notify the covered entity of a breach of unsecured PHI,
4. Make reasonable efforts to limit use and disclosure of PHI and requests for PHI to the minimum necessary,
5. Provide an accounting of disclosures, and
6. Enter into business associate agreements with subcontractors that comply with the HIPAA Privacy and Security Rules.

Despite requests from commenters for additional time to comply with the omnibus final rule, all affected parties must meet the September 23, 2013 compliance date. It is likely that many downstream subcontractors have not been following the evolution of the HIPAA Privacy and Security Rules and so may be unaware of the September 23, 2013 requirement.

Revisions to Business Associate Agreement Requirements

Business Associate Agreements (BAA) between covered entities and business associates must now require that the Business Associate comply with the Security Rule requirements and report to covered entities breaches of unsecured PHI. If a business subcontracts any its activities involving PHI, the Business Associate must enter into a BAA with its subcontractor(s). Achieving compliance with the final rule will require more cooperation among the various participants in the chain than was needed in

the past. Each BAA in the business associate chain must be as stringent or more stringent than the agreement above with respect to the permissible uses and disclosures, i.e., a subcontractor cannot use or disclose PHI in a manner that the business associate cannot. The covered entity is not required to have a direct BAA with subcontractors; that is the responsibility of the Business Associate.

Subject to certain limitations, the final rule grandfathers existing BAAs until September 22, 2014 to allow covered entities and Business Associates time to revise the agreements. However, covered entities and Business Associates are still required to comply with new rules regarding uses and disclosures of PHI beginning on the September 23, 2013 compliance date.

Next Steps

Covered entities must determine if they share PHI with any of the types of entities that have now been deemed to be Business Associates, including cloud vendors and other data storage companies. If a Covered Entity discovers such relationships, it must then execute BAAs with those identified entities. Covered entities must also review their existing BAAs for compliance with the new requirements for such agreements. Business Associates will need to identify which of their subcontractors create, receive, maintain or transmit PHI on behalf of the Business Associate and enter into appropriate BAAs with those companies. Given the increased liability imposed by the omnibus final rule, all participants in a given BAA chain should review the legal risks related to PHI, including compliance and contracting strategies.

---

without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.