Published on *The National Law Review* https://natlawreview.com

HIPAA Omnibus Final Rule: Highlights for Business Associates

Article By:

Christopher T. Collins

Caitlin C. Podbielski

The omnibus final rule, published on January 25, 2013, finalizes changes to the privacy, security and enforcement rules[1] promulgated under the Health Insurance Portability and Accountability Act of 1996 (the statute and rules together, HIPAA), which affect business associates in two primary ways. First, the final rule significantly broadens the definition of business associate, effectively bringing many new organizations under the authority of HIPAA. Second, the final rule clarifies which requirements and liabilities pertain to business associates as a result of changes enacted by the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

Expanded Definition of Business Associate

Under the final rule, the definition of business associate includes the following categories of organizations:

1. **Subcontractors**

   The final rule expanded the definition of business associate to include all subcontractors of business associates that create, receive, maintain or transmit protected health information (PHI) on behalf of business associates. The reach of this designation will apply to subcontractors irrespective of how far downstream the subcontractor is, contractually, from the covered entity. Each subcontractor, as a business associate under the new definition, will be directly liable for its own compliance with the provisions of the privacy and security rules applicable to business associates.

2. **Entities Providing Data Transmission Services**

   The final rule stated that any organization that provides a covered entity with data transmission services involving PHI and that requires access on a routine basis to such PHI will be considered a business associate, including but not limited to health information organizations and e-prescribing gateways. There is a narrow exception provided under the

final rule for entities that act as “mere conduits for the transportation of PHI” but do not access the PHI other than on a random or infrequent basis, such as Internet service providers (ISPs) and telecommunications companies.

3. **Document and Data Storage Organizations**

   The definition of business associate was expanded to include entities that “maintain” PHI. Organizations that maintain PHI, such as document and/or data storage companies, are considered business associates of covered entities, regardless of whether the entity actually accesses the PHI maintained for a covered entity.

4. **Personal Health Record Vendors**

   Vendors that provide and manage personal health records on behalf of covered entities are business associates under the final rule; however, those vendors that offer the personal health record directly to the individual and not on behalf of the covered entity will not be considered business associates.

5. **Financial Institutions Lending to the Health Care Industry**

   The preamble to the final rule clarified the circumstances under which a banking or financial institution may become a business associate. The mere act of providing payment processing activities for covered entities will not render a financial institution a business associate. However, performing functions above and beyond the mere processing of remittance advice, such as accessing accounts receivable documentation that contains PHI in connection with the provision of working capital financing to a health care provider, may qualify the institution as a business associate. Accordingly, a lender with access to PHI within the covered entity’s accounts receivable will likely be considered a business associate.

New Requirements and Liabilities for Business Associates under the Final Rule

Historically, business associates were not directly subject to liability under HIPAA but, instead, were only contractually liable to their covered entities pursuant to the terms of the business associate agreements. The final rule codifies which provisions of the privacy and security rules apply to business associates as prescribed by the HITECH Act. Notably, the HITECH Act statutorily imposed direct liability on business associates for failure to comply with HIPAA. Business associates may face civil monetary penalties, and in some cases criminal penalties, for failure to comply or for the failure of their agents, including subcontractors, to comply with the following obligations:

- Meeting all requirements of the security rule, including administering administrative, physical and technical safeguards, such as:
    - Conducting risk analyses;
    - Designating a security official;
    - Implementing required security policies and procedures;
    - Implementing technical security measures and facility access controls;
    - Conducting security awareness and training programs for all staff, including

management; and
    - Adopting a contingency plan.
- Adhering to the following privacy rule obligations:
    - Limiting uses or disclosures of PHI to only those (i) provided for within their business associate agreement or (ii) permitted or required under HIPAA;
    - Limiting permissible disclosures or requests for disclosures of PHI to the minimum necessary;
    - Providing an accounting of disclosures;
    - Providing access to its covered entity or to the individual who is the subject of the PHI to PHI kept in a designated record set;
    - Providing PHI to the U.S. Department of Health and Human Services (HHS) to demonstrate compliance during investigations; and
    - Entering into business associate agreements with subcontractors that comply with the provisions governing business associate agreements between covered entities and business associates.
- Maintaining compliance records and submitting reports to HHS when HHS requires such disclosures to determine whether a covered entity or business associate is complying with HIPAA.
- Providing a breach notification to its covered entity upon discovering a privacy or security "breach," as defined under HIPAA, and performing a risk assessment, in accordance with the final rule, when determining whether a breach has occurred.

Deadlines for Compliance

1. **Generally**
   Business associates are required to comply with the final rule by September 23, 2013. However, at least one state's attorney general has already brought an enforcement action against a business associate under the HITECH Act[2], and the final rule does not preclude such enforcement action prior to the compliance date.
2. **Extra Year for Grandfathered Business Associate Agreements**
   Business associate agreements and agreements between business associates and subcontractors entered into prior to January 25, 2013 that (i) are not renewed or modified between March 26, 2013 and September 23, 2013 and (ii) met the requirements of the privacy rule prior to the promulgation of the final rule shall be granted grandfathered status and deemed to continue in compliance until September 22, 2014 or the date the contract is renewed or modified, whichever occurs first.

Review and Revision of Business Associate Agreements

At this time, covered entities and business associates alike should reassess which of their vendors are now business associates or subcontractors under the new final rule. To the extent an existing vendor is recharacterized as a business associate or subcontractor under the final rule, a business associate agreement will need to be put in place before September 23, 2013.

Additionally, covered entities, business associates and subcontractors should review all existing business associate agreements to ensure compliance with the final rule and make amendments or enter into new agreements as required.

Further Information

In subsequent bulletins, we will discuss in more detail the following concepts mentioned above: (1) new requirements for business associate agreements with subcontractors; (2) agency liability that covered entities may have for their business associates' actions and all downstream subcontractors' actions, and that business associates may now have for their subcontractors' actions; (3) changes to the enforcement rule; and (4) the revised definition of "breach" and the expanded notification requirements associated therewith.

[1] 45 C.F.R. parts 160 and 164, subparts A and E; 45 C.F.R. parts 160 and 164, subparts A and C; and 45 C.F.R. parts 160, subparts C through E, respectively.

[2] The first enforcement action against a business associate was brought by the Minnesota Attorney General and settled in July of 2012. Press Release, Minnesota Attorney General Lori Swanson, Attorney General Swanson Says Accretive Will Cease Operations in the State of Minnesota under Settlement of Federal Lawsuit (Jul. 31, 2012), *available at* http://www.ag.state.mn.us/Consumer/PressRelease/07312012AccretiveCeaseOperations.asp. (stated that Accretive was required to cease operations in the State of Minnesota for six years under the settlement agreement for *State of Minnesota v. Accretive Health, Inc.*, Civil File No. 12145 RHK/JJK (D. Minn. 2012)).

National Law Review, Volume III, Number 54