New HIPAA Compliance Obligations For Business Associates
Jennifer Rathburn, Katea Ravega, Ilana Spector
Quarles & Brady LLP

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) Omnibus Final Rule (“Final Rule”), released on January 25, 2013, made substantial changes to the obligations and liabilities of business associates and their subcontractors. Business associates are vendors of covered entities which include health care providers, health care plans and health care clearinghouses. As a result of the Final Rule, more entities will be treated as business associates, business associates will have direct liability for violations of HIPAA and business associates will need to update their business associate and subcontractor agreements, as well as their HIPAA policies and procedures.

Expanded Definition of Business Associate

The Final Rule expanded the definition of "business associate" to include not only those who "create, receive, maintain or transmit" protected health information ("PHI"), but also anyone who "maintains" PHI on behalf of a covered entity, as well as subcontractors of business associates who have access to PHI. Essentially, all downstream entities with access to PHI are now covered.

Direct Liability for Business Associates

Prior to the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), which amended HIPAA, business associates were only contractually liable to covered entities under their business associate agreements ("BAAs"). Although it still holds true that business associates may be liable for breaching provisions of their BAAs, the Final Rule also makes business associates directly liable for violations of certain provisions of HIPAA, exposing the business associates to civil and criminal penalties. Business associates are also now subject to audits by the Office for Civil Rights ("OCR").

Business Associate Agreements

The BAA is the required written agreement between a covered entity and the business associate (or a business associate and its subcontractors). The legal requirements will apply to any entity engaged in the activity of a business associate or subcontractor. As a result, an entity may be a business associate regardless of whether there is a BAA in place or not - so it's important to be aware that one cannot avoid being a business associate or subcontractor simply by not signing a BAA.

The Final Rule changed and expanded some of the BAA requirements, for example:
Using appropriate safeguards and complying, where applicable, with the HIPAA Security Rule, with respect to electronic PHI;

Reporting breaches of unsecured PHI to the covered entity if not already updated for HITECH;

Ensuring that any subcontractors that create or receive PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate; and

Complying with the requirements of the HIPAA Privacy Rule to the extent the business associate carries out the obligations of the covered entity.

Business associates should also consider adding some optional language in their model BAAs, such as including sections that detail the express obligations of the covered entity and how business associates may use and disclose PHI, e.g., for de-identification and aggregation purposes. Business associates should also determine their position on whether they are an agent or an independent contractor since liability for their acts may be imputed to the covered entity. In addition, business associates should determine what they are willing to pay in the event the business associate causes a security breach, such as costs associated with notification preparation and postage, call centers, forensic investigations and mitigation efforts. Although business associates are not required to agree to pay for these costs, covered entities are increasingly requesting business associates to do so. Accordingly, business associates need to consider their cost structure and approach for handling security breaches.

The Final Rule also removed the requirement from the prior provisions of HIPAA that covered entities report to the Secretary of Health and Human Services when termination of a BAA is not feasible. Now, business associates are directly liable so any existing provisions on this topic should be revised or removed from the BAA.

In addition, many covered entities are imposing unduly burdensome requirements on their business associates that are beyond what is required by HIPAA, such as audits, notification timeframes that are shorter than the legal requirement, disaster recovery plan requirements, specific encryption requirements, and increased liability for violations of HIPAA. For these reasons, business associates need to understand what HIPAA specifically requires to be in a BAA and evaluate what they are willing to agree to beyond the minimum requirements. As a result, business associates may benefit from seeking legal advice regarding these matters.

Lastly, business associates will need to develop a model business associate subcontract agreement passing on these obligations to their subcontractors.

As discussed in more detail in this Quarles & Brady business update on the BAA compliance deadline, if you entered into a compliant BAA prior to January 25, 2013 and the BAA will not be renewed or modified between March 26, 2013 and September 23, 2013, then you do not need to revise your BAA until the BAA is renewed or modified on or after Sept 23, 2013 or until September 22, 2014, whichever date is earlier. BAAs that automatically renew (also called “evergreen” contracts) also qualify for this extension. If you do not have a BAA in place or your BAA is not compliant with the prior provisions of
HIPAA, then you must enter into a BAA that complies with the Final Rule by September 23, 2013.

Harm Threshold

Although current business associates may be familiar with the security breach notification rules under HITECH, business associates should be aware that the Final Rule changed the risk of harm standard for determining whether a breach has occurred. In general, the Final Rule takes a more objective approach to determining whether a security breach occurred, and this is discussed in more detail in a separate Quarles & Brady business update. In addition, another consideration facing business associates as they negotiate the BAA is whether the business associate or the covered entity determines whether an incident constitutes a "reportable" security breach for which notice is required. Covered entities are now pushing for increased notification and control over the determination of whether a suspected breach constitutes a reportable breach even when such incident occurs to the business associate rather than the covered entity. So be prepared for more negotiation on security breach notification provisions in BAAs.

Next steps

If you are not sure whether you are a business associate, subcontractor, or none of the above, this is the time to find out! There are a few months left to meet the Final Rule's compliance deadline of September 23. We recommend updating existing BAAs and subcontractor agreements and HIPAA policies and procedures to ensure your organization is prepared for an OCR or covered entity audit.