LOCKE LORD® QUICKStudy
Health Care Practice
August 29, 2014

Update Your "Grandfathered" HIPAA Business Associate Agreements by September 23

By: Tammy Ward Woffenden and Lane Wood

In January 2013, the Department of Health and Human Services (HHS) published its "Final Rule" implementing provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which significantly modified and expanded requirements under the Security and Privacy Rules of the Health Insurance Portability and Accountability Act (HIPAA). The Final Rule included changes to Business Associate Agreements (BAAs) and required that such agreements—whether between a Covered Entity and its Business Associate or a Business Associate and its subcontractor—place the following additional obligations on the Business Associate:

- Comply with the HIPAA Security Rule;
- Agree to execute BAAs with downstream subcontractors (who are also considered Business Associates under the Final Rule);
- Report breaches of unsecured Protected Health Information (PHI) to the Covered Entity; and
- If the Business Associate carries out an obligation of the Covered Entity, comply with any HIPAA rule applicable to such obligation.

BAAs that were in compliance with the HIPAA Privacy Rule prior to January 25, 2013, were "grandfathered" and have been permitted to remain in place through September 22, 2014 if the BAAs were not updated prior to this date. However, by September 23, 2014, all BAAs must be updated to include the additional requirements created by the Final Rule. BAAs that do not specifically include these provisions but require "compliance with all applicable laws" do not sufficiently reflect the new requirements and will be out of compliance after the compliance deadline. Covered Entities and Business Associates should review all business relationships that involve the transfer, creation or maintenance of PHI to ensure that all required BAAs are updated prior to September 23, 2014.

In addition to meeting the upcoming September 23rd deadline, Covered Entities and Business Associates should have already completed the following measures to satisfy changes to the Final Rule:

- New BAAs put into place after January 25, 2013 should comply with the Final Rule.
- Any modifications and renewals, unless automatic, to BAAs following the Final Rule's March 26, 2013 effective date should comply with the Final Rule. This includes "grandfathered" BAAs that were modified or renewed.

- Covered Entities must implement BAAs with all Business Associates, including those new entities that the Final Rule designated as falling within the definition of Business Associate. These include Health Information Organizations, E-Prescribing Gateways, and Vendors of Personal Health Records. The Final Rule also clarified that certain entities that offer data storage services (including cloud service providers) are Business Associates, even if the entity does not view stored PHI or only does so on a random or infrequent basis.
- Business Associates must implement BAAs with subcontractors that create, receive, maintain, or transmit PHI on behalf of a BA and its Covered Entity. These subcontractors, which also qualify as Business Associates under HIPAA, must obtain BAAs from their own downstream contractors, despite how far "down the chain" the subcontractor provides services.

If you have any questions regarding these requirements, please contact a member of the health care practice group of Locke Lord. Our health care attorneys have the experience to assist you with HIPAA and HITECH compliance.

For more information on the matters discussed in this *Locke Lord QuickStudy*, please contact the authors:

Tammy Ward Woffenden | 512-305-4776 | twoffenden@lockelord.com
Lane Wood | 214-740-8513 | lwood@lockelord.com