# Health Law Alert: The Deadline for Amending Business Associate Agreements is Quickly Approaching

June 23, 2014

A key change from 2013's HITECH "Omnibus" Rule was a requirement that Business Associate Agreements ("BAAs") be modified to reflect the latest revisions to the HIPAA regulations. When the Rule was issued on January 25, 2013, Covered Entities ("CEs") and Business Associates ("BAs") alike were pleased that the Department of Health and Human Services' Office of Civil Rights ("OCR") granted them extra time—until September 22, 2014—to amend existing BAAs to reflect the new requirements. For the majority of CEs that took advantage of this delay and have not replaced their existing BAAs, they now have just three months to get all of their updated BAAs in place.

**The Omnibus Rule**

Among the many changes to HIPAA made under the Omnibus Rule were revisions to BAA provisions. The deadline for compliance with the Omnibus Rule, including the substance of the new provisions that need to be spelled out in BAAs, was September 23, 2013. However, the regulations included a transition period for amending existing BAAs to include the new obligations. Specifically, BAAs that met existing HIPAA requirements and were in effect on January 25, 2013 did not need to be amended right away, so long as the BAA was not modified after March 26, 2013. The deadline for these grandfathered BAAs—the date by which they need to be amended to reflect the new requirements—is September 22, 2014.

Under the Omnibus Rule, BAAs, at a minimum, need to address four issues that may not have been addressed in agreements entered into before January 25, 2013. Further, since many BAAs have been in place since early 2003—and may not have been updated to reflect the changing enforcement attitude around PHI or the enormous growth in the transmission of, and access to, electronic PHI—now may be a good time to think about whether your BAAs have everything you need (or want) them to have.

**So what are the New Requirements?**

As noted above, the deadline for complying with the substance of what is required of BAs under the Omnibus Rule was September 23, 2013. However, the BAAs themselves need to be modified to explicitly address specific obligations from the Omnibus Rule. Specifically, the BAA must provide that the BA will:

***Comply with the HIPAA Security Rule.***

While many BAs have historically promised via contract to comply with the concepts underlying the Security Rule, the Omnibus Rule requires BAs to fully comply with all Security Rule standards. In other words, BAs essentially need to meet the Security Rule standards in the same fashion as a CE. Smaller BAs, or BAs that have historically not paid too much attention to HIPAA, may face challenges in meeting all of the Security Rule requirements. Although the substance of meeting Security Rule requirements has been mandatory for BAs since September 23, 2013, CEs will want to make sure that their BAAs specifically spell out this obligation.

***Ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of the BA agree to comply with the same restrictions required of the BA itself.***

BAAs need to obligate a BA's "subcontractors" to meet the same restrictions and conditions that apply to the BA itself. In addition to making sure the BAA says this specifically, CEs should consider possibly regulating a BA's use of subcontractors. For instance, some CEs may want to forbid the use of subcontractors altogether or require BAs to seek permission from the CE prior to entering into a relationship with a subcontractor. Similarly, a CE may prefer to set limits by specifying permissible or impermissible subcontractors (for example, prohibiting the use of subcontractors located outside of the United States). Another way to regulate the use of subcontractors is to create a template subcontractor agreement and require all BAs to use that template as a condition of doing business with the CE.

***Report any breaches of unsecured PHI to the CE.***

BAAs must require the BA to report any "breaches" of unsecured PHI to the CE. This change reflects CE's obligations to report breaches to consumers, regulators and potentially the media. Given the stakes at issue in HIPAA breaches, however, CEs may want to include more specific provisions to protect their interest in the event of a breach by a BA.

Options for building in extra protection may take many forms. Most obviously, CEs could mandate specific breach reporting timelines. Because the 60-day limit found in the regulations is an outer limit, and not a fallback standard, CEs may want to require BAs to inform them of a breach as soon as possible, such as within a day or two of learning of the breach. Further, some CEs may want to think about requiring BAs to inform them of "potential" breaches. The idea with this approach is that it permits the CE to then control and perform the breach analysis. CEs may also want to think about trying to require BAs to pay the CE's costs in the event of a breach.

***If the BA carries out a CE's obligations under the Privacy Rule, making sure that the BA complies with the Privacy Rule's requirements.***

This provision is intended to reflect the idea that if a BA carries out an activity required under the Privacy Rule, the BA needs to meet the Privacy Rule's obligations in its conduct. For example, if a BA contracts with a CE to carry out a CE's obligations under the Privacy Rule, such as distributing a notice of privacy practices for the CE, the BA needs to comply with the HIPAA requirements that would apply to the CE in the performance of that obligation. Along these same lines, CEs may want to think about what the BAA requires of BAs in terms of keeping track of disclosures the BA makes, so that any future requests from patients for an accounting of disclosures can be met without difficulty. Further, because the HITECH change to HIPAA's accounting of disclosures requirement has not yet been finalized, CEs may also want to think about whether provisions in the BAA on accountings are written in a way that will incorporate future changes mandated by regulation or whether the CE will once again need to amend its BAAs to reflect any future changes.

***What else do people care about?***

The stakes for HIPAA compliance are very high: penalty amounts under HITECH have gone up, OCR has increased its emphasis on enforcement, and a CE can be held vicariously liable for the acts of its BAs. Given these risks, CEs may want to think about whether additional protections should be included in their BAAs. For organizations that chose to take advantage of the Omnibus Rule's transition period, now may be a good time to address other provisions as part of the requirement to update existing agreements by September 22, 2014.

While not required by HIPAA, the following provisions can provide added protections to CEs. The inclusion of the following terms is often a matter of negotiating power between the CE and BA.

- ***Indemnification commitments.***

A CE may want to require its BAs to defend and indemnify the CE for HIPAA violations. While BAs can be held liable by OCR for their own conduct, CEs may still face concurrent responsibility for the conduct of their BAs. The inclusion of an indemnification clause may ultimately turn on the relationship and bargaining power of the parties.

- ***Insurance requirements.***

Obligating the BA to obtain insurance to cover costs arising from data breaches and other HIPAA violations is another way to try and reduce the CE's exposure for HIPAA violations. An increasing number of companies are offering data breach insurance at various levels of coverage.

- ***Access and audit rights as a way to monitor BA compliance.***

Some CEs will include a provision permitting them to have access to and audit the BA's HIPAA practices. The right to audit BA compliance may afford the CE with comfort in terms of how seriously the BA it taking its HIPAA obligations. Larger BAs in particular may push back against CEs who try and include this concept in the BAA.

- ***Fines and other remedies in the event of a breach or unauthorized disclosure of PHI by the BA.***

Some CEs seek to impose penalties for a breach or unauthorized disclosure of PHI by a BA. These clauses can take the form of liquidated damages, specific performance, or other equitable relief.

- ***Other substantive obligations.***

BAAs can be written to address many other substantive obligations imposed on the BA. For instance, the CE may want to specify in detail how the BA will comply with the Privacy Rule's "access" provision, which requires BAs to provide a copy of electronic PHI in a designated record set to the CE, the individual, or the individual's designee. Other substantive Privacy Rule obligations can also be addressed at varying levels of detail.

If you have comments or questions about amending BAAs, please contact Jesse Berg at jesse.berg@lathropgpm.com or 612-632-3374.

**Gray Plant Mooty Health Law Seminar**

HIPAA issues will be addressed at Gray Plant Mooty's 18th annual Health Law Seminar, to be held July 17th at the Depot in Minneapolis. You can find more information about this event and how to register here.