Bloomberg BNA

BNA's
Health Law Reporter™

Do I Need New HIPAA Business Associate Agreements?

By Kirk J. Nahra

Now that the HIPAA omnibus regulation has been published, companies across the health care industry and an enormous range of service providers are struggling to meet the challenges presented by these new rules by the Sept. 23 compliance date. Some of these obligations present new challenges in interpreting what the rules mean (e.g., the new marketing and sale restrictions). Other provisions require new analysis in situations arising in the future (e.g, the breach notification provisions). Business associates in general need to evaluate how best to comply with the detailed and onerous HIPAA Security Rule.

The question surrounding new business associate agreements presents a mixture of compliance obligations, risk management and business opportunity, from the perspective of both covered entities and business associates. Business associate agreements have been around since the beginning of the HIPAA era. Because HHS had no authority to regulate anyone other than covered entities, the regulators created the idea of a business associate agreement to impose contractual obligations on the wide range of service providers to the health care industry. This was, at the time, a genius idea, to provide reasonably effective privacy protections beyond the authority provided by Congress. It imposed at least a contractual structure on the privacy and security of health care information far beyond the core requirements for covered entities. HHS did not properly appreciate, however, the time and money that would be spent negotiating hundreds of thousands of business associate agreements across the country.

Fast forward to HITECH. Now, HHS has authority to regulate business associates directly, as of the compliance date in September. Under the new rules, business associates will need to comply with many of the provisions of the HIPAA Privacy Rule, all of the HIPAA Security Rule and the HIPAA Breach Notification provisions. So, what about the need for updated business associate agreements themselves?

At a minimum, HHS clearly stated that business associate agreements still are required. Their justification for this is, frankly, limited, and not particularly persuasive. But, these agreements still are required even though the bulk of these documents (and all of the ''required'' elements) now will simply reiterate compliance requirements applicable by law for the business associates.

So, even though there is limited rationale for these agreements, do covered entities need to have new business associate agreements in place to meet the new requirements? And do business associates want new agreements or not? While it is possible that some existing agreements will meet all relevant standards, and there is no explicit statement from HHS (as there was with privacy notices) that new business associate agreements are required, most covered entities will find both that they will need to make changes to their agreements to deal with these new changes AND that it is desirable to have new agreements that reflect these changes. (Business associates also may find reasons to want new

Kirk J. Nahra is a partner with Wiley Rein LLP, in Washington. He chairs the firm's Privacy Practice and co-chairs the Health Care practice. He assists a wide range of companies in meeting their obligations under the HIPAA rules and a wide range of other privacy and security laws across the country and internationally. He can be reached at (202) 719-7335 or knahra@wileyrein.com. The information contained in this article is not intended to constitute legal advice.

 ISSN 1064-2137

agreements). Despite some confusion, it seems clear that the obligation to implement business associate agreements continues to rest with the covered entity (and that business associates now have specific legal obligations whether there is a business associate agreement in place or not)

In addressing these questions, keep in mind the following points.

What are you trying to accomplish with your business associate agreements?

There are three main purposes for business associate agreements—compliance, education/information, and contract enforceability. These are not the same. An agreement that says ''we agree to follow all applicable law'' may be compliant, but will not tell the business associate what they actually need to do. Do you (if you are a covered entity) want to assume that your business associates know what to do? Remember, some of the actions of the business associate can be attributed to you, whether it is because they are an ''agent'' under the new rules or because they have a security breach of some kind that affects your patients or members.

When did you last change your agreements?

The ''new'' omnibus regulation imposes new obligations. It is important to think about the measuring stick, however. Are you comparing this regulation to (1) the original HIPAA Rules from 2003; (2) the changes made by the HITECH law in 2009 (which many people acted upon even though they were not actually in effect); or (3) the proposed regulation from July 2010? It is important to evaluate what your starting point is. Each of these time periods has a different impact on whether the current documents are effective and appropriate, or not.

Similarly, while HHS has included some significant time extensions for revising existing agreements, covered entities and business associates should be cautious about relying on these additional time periods too much. For example, if a covered entity did not revise its agreements at the time of the HITECH law, many of these agreements may be close to a decade old. I would discourage relying on agreements that are this old, even if you are given some flexibility as a formal compliance matter on revising these documents.

How consistent are your agreements?

Another variable for any covered entity or business associate is the consistency of the current agreements. Do they all fit the same template (unlikely)? How similar are they? Are they mainly ''your'' template, or the other party's? And over what course of time did you enter into these agreements? Each variable again will affect the likelihood that changes are necessary or appropriate.

What have you said about breach notification?

The new changes to the breach notification requirement represent one of the most important new elements of the omnibus regulation. Keep in mind that, if you are a covered entity, it is your problem if your business associate has a breach, even though your business associate now has an independent legal obligation to meet the various HIPAA requirements. How do your agreements address breach reporting? Do you simply mirror the words of the regulation? What kind of investigation or assessment do you want your business associate to do before notifying you? Or do you have additional elements relating to what should be reported, when, and who bears the cost burdens?

Do you have all of the required elements?

Many BA agreements will have most of the required elements. But will all of them be there? For example, certain new provisions relating to the minimum necessary standards are unlikely to be included in ''standard'' business associate agreements executed before the omnibus regulation. Is it worth making a change to hundreds or thousands of agreements just to modify minor contract terms?

Are there other elements that are important to add?

Beyond these required elements, are there other contact terms that you want to ensure are included in these agreements? For covered entities, do you want to include details or provisions related to de-identification, data aggregation, sales and marketing? For business associates, if you need to engage in any of these activities, the new regulation makes clear that a failure to include these elements means that they cannot be performed by a business associate.

Conclusion

The decision on whether to enter into new business associate agreements (and on what time frame) is a complicated one. Obviously, both business associates and covered entities wish to minimize the time and effort spent on renegotiating these agreements. HHS did the health care industry no favors by continuing the obligation to maintain these agreements, and then making various changes to the details of what should be included. This is a tedious, time consuming process. Nonetheless, ensuring the effectiveness of these agreements, both for compliance purposes and for the effective operation of health care businesses and protection of personal information, is a significant commitment. It is critical to ensure that these documents cover appropriate territory and adequately and effectively ensure that the agreements operate in the way intended. There is a tendency to make these agreements ''one size fits all,'' and that tendency should be managed appropriately. There clearly are benefits to consistency, but there also are significant differences among both covered entities and business associates. Because there is so much data flow of PHI between these entities, the management of this data requires constant attention, and ensuring an appropriate business associate agreement program is not only a compliance requirement but also an important best practice throughout the health care industry.

  HLR ISSN 1064-2137