Protected information

HIPPA and business agreements: what service providers need to know

JULES S. HENSHELL
Of Counsel
Semanoff Ormsby Greenberg & Torchia, LLC

(215) 887-3754
jhenshell@sogtlaw.com

Insights Legal Affairs is brought to you by **Semanoff Ormsby Greenberg & Torchia, LLC**

Anyone who has been to a doctor's office knows that the Health Insurance Portability Act (HIPAA) protects the confidentiality and security of identifiable patient health information (PHI). Yet, many businesses newly marketing services to the health care industry are not aware of the impact of HIPAA on their business.

"The relationship between health care providers and their service providers who handle PHI requires a written business associate agreement (BAA)," says Jules S. Henshell, Of Counsel at Semanoff Ormsby Greenberg & Torchia, LLC.

Smart Business spoke with Henshell about what to consider when signing a HIPAA business associate agreement.

Who is a business associate?

A business associate is any individual or entity that creates, receives, maintains or transmits PHI in the course of performing services on behalf of a HIPAA-covered entity. The HIPAA Omnibus Rule makes business associates of HIPAA-covered entities directly liable for violations of HIPAA and the Health Information Technology Act (HITECH).

What is a business associate agreement?

A business associate agreement is a written agreement, required by HIPAA, between a covered entity and a business associate that describes the rights and responsibilities of each party with respect to the handling of PHI, compliance with HIPAA and implementing regulations known as the HIPAA Omnibus Rule.

How can a company evaluate whether or not a proposed BAA is acceptable?

Certain elements of every BAA are required by law. Other terms are not expressly required. The latter are potentially negotiable. For example, HIPAA does not require that a business associate agree to indemnify a covered entity in the event of breach of PHI, but a covered entity may want such protection. Similarly, HIPAA requires that a business associate agree that the Secretary of Health and Human Services will have access to its books and records. HIPAA does not require that a BAA include such access by a covered entity, but a health care provider may want to audit HIPAA compliance by the business associate.

In addition to review of the terms proposed by the covered entity, the acceptability of a proposed BAA may turn on the following considerations:

1) *Determine if you are a business associate* — Will you be creating, receiving or transmitting PHI in the course of performing services? If the services agreement does not entail handling PHI, there is no reason to sign a BAA.
2) *Consider your ability to comply with the BAA commitments* — Do you have policies, procedures and safeguards for protecting privacy and security of PHI?
3) *Consider your bargaining power to negotiate* — Is the covered entity willing to entertain discussion of the terms of the BAA not required by HIPAA? Contracting officers for large health systems may resist negotiation, but allow for direct discussion between their legal counsel and your lawyer.
4) *Consider whether you will be using a subcontractor to perform* — Do you have a subcontractor agreement to ensure that your subcontractor complies with HIPAA? Does it include timeframes that enable you to meet breach notification deadlines in the proposed BAA?
5) *Consider your risk in the event of security breach of PHI.*

What is at risk if a business associate violates HIPAA rules?

There are substantial civil monetary penalties for each HIPAA violation. Civil monetary payments totaling $22,855,300 were made to the Department of Health and Human Service's Office of Civil Rights (OCR) to resolve HIPAA violations last year. In 2016, OCR also announced its first enforcement action directly against a business associate, Catholic Health Care Services of the Archdiocese of Philadelphia. The resolution agreement imposed a $650,000 monetary payment and a corrective action plan, signaling new focus on enforcement against business associates.

Such focus is likely to continue as OCR identifies business associates through ongoing audits of covered entities. ●