Tick Tock, Strikes the HIPAA-HITECH Clock: Time Is Running Out To Update Your Business Associate Agreements

Compliance with the revised Health Insurance Portability and Accountability Act ("HIPAA") is mandatory for covered entities and their business associates beginning September 23, 2013. Given the growing universe of vendors and contractors that service the healthcare industry and require access to patient information, HIPAA compliance is becoming increasingly more challenging. Chief among these tasks is ensuring that all business associate agreements meet HIPAA's updated requirements.

Background

On January 17, 2013, the U.S. Department of Health & Human Services ("HHS") released final, omnibus regulations ("Final Rule") amending HIPAA in accordance with the HITECH Act of 2009.

Under HIPAA's *Privacy Rule* (then and now), a covered entity — which term includes health plans, healthcare clearinghouses, and health care providers — may not use or disclose protected health information ("PHI") unless as permitted or required by the Rule, or as authorized in writing by the individual affected.

Similarly, HIPAA's *Security Rule* is designed to safeguard the confidentiality, integrity, and availability of electronic PHI. The Security Rule sets forth detailed administrative, physical, and technical standards to ensure that, among other matters, only those who are authorized to have access to electronic PHI will have access.

The Final Rule makes significant changes to the privacy and security obligations of covered entities and their business associates with respect to patients' PHI, most notably by making business associates now directly liable for compliance with HIPAA's Security Rule. Covered entities and business associates are required to come into full compliance with the Final Rule by Sept. 23, 2013.

What is a "Business Associate"?

A business associate ("BA") is a person or organization that performs certain functions or activities that involve the use or disclosure of PII on behalf of, or provides services to, a covered entity. Traditionally, BAs included accountants, auditors, third-party administrators, billing providers, claims processors, copying services, pharmacy benefits managers, quality assurance or utilization review consultants, and transcriptionists.

The Final Rule expands the definition of a "business associate" to include any person who creates, receives, maintains or transmits PHI on behalf of a covered entity, and specifically extends to a subcontractor of the BA that handles PHI, and to all downstream vendors with access to PHI as well. In particular, if a BA delegates a function, service, or activity to a subcontractor that involves disclosing PHI to the subcontractor, then that subcontractor is also a BA, even if the subcontractor does not have a directed relationship with the covered entity.

As further clarified by the Final Rule, only those service providers who are providing mere courier services, whether digital or hard copy, (such as the U.S. Postal Service or internet service providers ("ISP"s)) are excluded from being classified as BAs. In contrast, an entity that maintains PHI on behalf of a covered entity (such as a data storage or cloud computing company) is a BA, even if the entity does not actually view the PHI.

The Obligations of a Business Associate

Under the Final Rule, BAs are now directly liable for compliance with the HIPAA Security Rule (and most of the Privacy Rule), requiring them to implement appropriate administrative and security safeguards. Business associate agreements ("BAA"s) should be revised to obligate BAs to:

- Comply with all of the Security Rule's administrative, physical and technical safeguards.
- If the BA is to carry out the covered entity's obligations under the Privacy Rule (*e.g.*, the provision of Notices of Privacy Practices), comply with the Privacy Rule's requirements in the same manner as those requirements apply to the covered entity.
- Limit the use or disclosure of PHI only to those reasons or purposes identified in the BAA.
- Report breaches of unsecured PHI to the covered entity.
- Provide electronic access of PHI directly to individuals or their designees, or to the covered entity (which may then provide the access to the individuals or their designees).
- Provide PHI when required by HHS to facilitate investigation of the business associate, and to otherwise cooperate with the HHS in its investigation of privacy complaints.
- Provide an accounting of disclosures to the covered entity in order to allow it to comply with its accounting of disclosures obligations to an individual.

- Address the expanded rights of individuals to restrict disclosures of PHI that pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket and in full.

- Update their Breach Notification Policies and Procedures to address the new breach standards. (Under the Final Rule, rather than weighing the potential harm to the individual to determine if notification is required (under the so-called "significant risk of harm" test), a breach will be *presumed* (and, hence, notification will be required) whenever an impermissible use or disclosure of PHI occurs, unless the covered entity or BA, as applicable, demonstrates a "low probability" of risk that the information was actually compromised based upon a statutorily proscribed four-part risk-assessment, or unless one of the three narrow exceptions to the definition of "breach" applies.)

- Evaluate the overall probability as to whether PHI has been compromised by considering, and documenting, the following factors: (a) the nature and extent of the PHI involved; (b) the unauthorized person who used the PHI or to whom the disclosure was made; (c) whether the PHI actually was acquired or viewed; and (d) the extent to which the risk to the PHI has been mitigated.

- Obtain satisfactory assurances (in the form of a written BAA) from any subcontractor that creates, receives, maintains, or transmits electronic PHI on behalf of the BA that the subcontractor agrees to the same restrictions and conditions that apply to the BA with respect to such information.

In general, providers must enter into new BAAs or modify existing BAAs by September 23, 2013. However, existing BAAs that (i) were entered into on or before January 25, 2013; (ii) meet the requirements that were applicable prior to the promulgation of the Final Rule; and (iii) were not modified between March 26, 2013 and September 23, 2013, do not have to be revised to incorporate the new requirements until September 23, 2014. That said, parties must comply with the new HIPAA/HITECH provisions regardless of whether their BAAs have been updated – something to seriously consider when deciding whether to revise your BAA sooner rather than later.

Compliance failures now carry steeper penalties – up to $50,000.00 per violation (capped at $1,500,000.00 per year, but only for *identical* violations). Further, under the Final Rule, penalties may be assessed even if the covered entity or BA did not

know about, or by exercising reasonable due diligence would not have known about, the violation.

It should also be emphasized that the Final Rule no longer shields a covered entity from liability simply because it has a valid BAA in place. Even with a valid BAA in place, covered entities and BAs are liable for the acts of their agents, including workforce members and subcontractors, acting within the scope of the agency.

Given the increased penalties and the significant changes in the liability landscape, covered entities should carefully review, and update as needed, their BAAs in conjunction with their overall HIPAA compliance programs.

If you have any questions about this article, please contact:

Robert McHale, Esq.
R | McHale Law
9 West Broadway, Suite 422
Boston, MA 02127
Tel. 617.306.2183
Email: robert.mchale@rmchale.com