February 7, 2013

The Granade Law Firm

Dedicated to Counseling the Health Care Industry regarding Privacy and Security Laws

HIPAA Alert #1: Business Associates

The new HIPAA Final Rule was promulgated by the U.S. Department of Health and Human Services (HHS) on January 25, 2013. While the Final Rule brings tremendous change to the HIPAA privacy and security regulations, this alert – the first in a series – focuses on the ways in which the Final Rule will impact business associates. Please note, if your organization is a covered entity, you should consider whether your organization owns and/or operates any entities that may be considered business associates.

THE 30,000 FOOT VIEW: THE NEW RULE'S IMPACT ON BUSINESS ASSOCIATES

1. The definition of "Business Associate" (BA) has been significantly revised, and is now more expansive than the previous definition. Rather than being limited to entities that "use or disclose" PHI on behalf of a covered entity, BAs now include any organization that "creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA]…." (45 C.F.R. 164.103)
2. Although entities do not have to enter into BAAs with organizations that are purely "conduits" of PHI, such as UPS and the USPS, this exception has been narrowed. HHS makes clear that record storage companies and other services that involve the maintenance of PHI for covered entities (e.g., hosting an electronic health record in the cloud) are BAs, regardless of whether these vendors actually view the PHI. (78 Fed. Reg. at 5572)
3. Any "Subcontractor" (i.e., downstream entity from a business associate) that creates, receives, maintains or transmits PHI on behalf of a covered entity or business associate **is considered a business associate**, or BA. (45 CFR 160.103)
4. Business Associate Agreements should be updated and revised to include new HIPAA Final Rule requirements. Optional provisions, such as indemnification, data breach insurance, and/or reimbursement of notification expenses should be discussed with counsel.

COMPLIANCE DEADLINES:

1. The publication date of the Final Rule was January 25, the effective date is March 26, and the compliance deadline (with the exception of pre-existing BAAs needing amendment) is September 23. Please note, the civil monetary penalties provisions were effective as of the enactment of the HITECH Act of 2009.
2. BAs must move quickly to achieve compliance with the applicable HIPAA provisions prior to the Final Rule's compliance deadline of September 23, 2013. See below, "Security Standards" and "Privacy Standards."
3. Regarding business associate agreements (BAAs), HHS provides an extended compliance deadline of one additional year to enter into BAAs that comply with the Final Rule *but only if* the BAA in question was in existence prior to the issuance of the Final Rule on January 25 of this year.

SECURITY STANDARDS:

1. Business associates must comply with the HIPAA Security Standards in order to "ensure the confidentiality, integrity, and availability of all ePHI the covered entity or BA creates, receives, maintains or transmits." (45 CFR 164.306). <u>In sum, BAs must now comply with HIPAA's Security Standards as if they were covered entities</u>.
2. BAs must adopt written policies and procedures (P&Ps) and other documentation required by the HIPAA Security Standards. (45 CFR 164.316)
3. BAs must appoint a Security Official. We strongly recommend the appointment of a Privacy Official as well. The position may be shared, particularly in smaller organizations.
4. BAs must conduct (if they have not yet done so) a risk assessment to determine risks and vulnerabilities to ePHI.
5. Following the risk assessment, a responsive risk management plan must be prepared, and the BA must ensure it has implemented appropriate administrative, technical and physical safeguards.
6. NOTE: The importance of conducting a robust risk assessment of your information systems is critical, and must be followed by a thorough risk management plan that is periodically updated. The HHS Office for Civil

Rights (OCR) investigations triggered by the report of a data breach typically result in OCR closely reviewing not only the written P&Ps in place to safeguard PHI, but also the results of the entity's risk assessment and resulting risk management plan. All P&Ps, assessments, plans, etc., must be documented in writing and maintained for at least six years following the last effective date of the particular document.

PRIVACY STANDARDS:

1. BAs must comply with certain of the HIPAA Privacy Standards, as described below.
2. BAs must use and disclose PHI in accordance with both its BAA and the Privacy Standards.
3. BAs must allow individuals (and/or the covered entity) to access PHI in accordance with HIPAA's individual rights provisions. This includes, for instance, providing an electronic copy of ePHI to the individual and/or the covered entity. (e.g., 45 CFR 164.502, 164.524)
4. BAs must comply with HIPAA's "minimum necessary" standard, which requires entities to use and disclose only the minimum PHI necessary to accomplish the purpose behind the use or disclosure.
5. BAs must enter into BAAs when appropriate; even if the upstream BA or covered entity fails to initiate negotiation of a BAA, a BA will be held liable if no BAA is in place.
6. Regarding compliance with other provisions of the Privacy Standards, HHS states that BAs remain "contractually liable for all other Privacy Rule obligations that are included in their contracts…." (78 Fed. Reg. at 5592)

DATA BREACHES:

1. HHS revised the definition of "Breach." Rather than using a "risk threshold" involving a determination of whether there was a risk of significant financial, reputational or other harm to an individual, HHS now requires the covered entity or BA (following an impermissible use or disclosure of PHI) to "assess the probability that the [PHI] has been compromised based upon a risk assessment that considers at least the following factors:
    a. Nature and extent of PHI involved, including the types of identifiers and likelihood of re-identification;
    b. The unauthorized person who used the PHI or to whom the disclosure was made;
    c. Whether the PHI was actually acquired or viewed; and
    d. The extent to which the risk to the PHI has been mitigated." (78 Fed. Reg. at 5642)
2. If an evaluation of the factors above fails to demonstrate that there is a low probability that the PHI in question has been compromised, then breach notification is required.
3. The burden of proof has shifted in data breach cases under HIPAA. As stated by HHS, the impermissible use of disclosure of PHI is "presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised." (78 Fed. Reg. at 5641)

CONTRACTING:

1. Each agreement in a business associate chain must be <u>at least as stringent</u> or more stringent as the agreement above with respect to the permissible uses and disclosures.
2. Increased danger of creating unintentional agency relationships – Through the examples provided in its comments to the Final Rule, HHS broadly expanded the dangers associated with creating an agency relationship between those entities contracting out services to business associates. A covered entity or BA may unintentionally create an agency relationship, subjecting the contracting entity to ***direct liability for the actions of the business associate***, by including in a BAA any requirements that allow the contracting entity to designate how a BA acts <u>during</u> the course of the agreement. When amending your BAA to bring it into compliance with the new HIPAA Final Rule, review with counsel whether the terms and conditions might unintentionally create an agency relationship.
3. HHS makes it clear that the parties – the CE and BA, or BA and Subcontractor – may add additional provisions to their BAAs, such as indemnification or reimbursement for costs/expenses related to a data breach.
4. NOTE: Indemnification and/or reimbursement provisions, as well as cyber liability/data breach insurance, should be considered with legal counsel's involvement.

ENFORCEMENT AND PENALTIES:

1. Anyone may file a complaint with HHS against a **business associate** (not just covered entities) for failure to comply with the HIPAA privacy/security regulations. (45 CFR 160.306)

2. OCR may initiate an audit or "compliance review" against a business associate to determine HIPAA compliance, regardless of whether a complaint has been received. (45 CFR 160.308)
3. BAs must maintain the same "paperwork" – written P&Ps and other documentation – required by HIPAA as do covered entities. (45 CFR 160.310)
4. BAs must comply with requests of OCR, such as responding to investigative demands and subpoenas. (45 CFR 160.310)
5. BAs may not retaliate against anyone that files a complaint about the BA. (45 CFR 160.316)
6. BAs must have downstream BAAs with their Subcontractors.
7. Most importantly, BAs (including downstream Subcontractors) are subject to the same civil monetary penalties (CMPs) as covered entities if the BA violates HIPAA. (45 CFR 160.400 *et seq*.)
8. The following chart outlines the levels of CMPs that became effective immediately upon enactment of HITECH. This penalty structure was adopted by the HIPAA Final Rule:

Violation category 42 U.S.C. §1320d-5, amended by the HITECH Act and 45 C.F.R. §160.404	**Range of Penalty HHS May Impose for each Violation (Min. to Max.)**	**All violations of an identical provision, per calendar year**
Did not know	$100 - 50,000	$1,500,000
Reasonable cause[1]	$1,000 - 50,000	$1,500,000
Willful neglect (Corrected within 30 days)	$10,000 - 50,000	$1,500,000
Willful neglect (**Not** corrected within 30 days)	$50,000	$1,500,000

Since many of these requirements are new to most business associates, we hope this brief outline has helped highlight HHS' emphasis on business associates' obligations to maintain the privacy and security of protected health information. Covered entities have had over a decade to come into compliance with most HIPAA requirements; business associates, however, must move quickly to achieve compliance with the applicable HIPAA provisions.

Please let us know how we can assist your company with its compliance activities.

THE GRANADE LAW FIRM, LLC
1266 West Paces Ferry Road, Suite 204
Atlanta, Georgia 30327
(678) 705-2507

PHYLLIS F. GRANADE
pgranade@granadelaw.com

AJAY R. VYAS
avyas@granadelaw.com

[1] The Final Rule also revised the proposed definition of "reasonable cause." 45 C.F.R. §160.401 now defines "reasonable cause" to mean "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect."