Omnibus Rule: HIPAA 2.0 for Law Firms

Introduction
On January 25, 2013, the U.S. Department of Health and Human Services (HHS) issued the much-anticipated “Omnibus Rule” finalizing changes to the HIPAA Privacy, Security, Breach Notification and Enforcement Rules. These changes implement the HITECH Act of 2009 and the Genetic Information Nondiscrimination Act (GINA) of 2008, strengthening security and privacy protections for individual health information. The Omnibus Rule extends significant aspects of HIPAA directly to health care “business associates” (BAs) including many law firms. BAs will be directly liable for compliance with the Security Rule, significant provisions of the Privacy Rule and remain subject to the Breach Notification Rule. The revised regulations authorize HHS to audit BAs, subject them to compliance reviews, impose civil monetary penalties for violations and even make referrals to DOJ for criminal prosecution. The Omnibus Rule takes effect on March 26, 2013 with full compliance generally required by September 23, 2013.

Much has been written about the rule in the month following its publication. This article reviews some noteworthy changes under the Omnibus Rule for law firms acting as HIPAA business associates. After discussing those changes, the article will offer some recommendations to address related loss prevention issues.

Evolving Regulation of HIPAA Business Associates
Under the original regulations, the Privacy and Security rules applied only to HIPAA-defined “covered entities” (CEs) consisting of health plans, health care clearinghouses, and health care providers that perform certain electronic transactions. Regulators recognized that CEs needed to engage third parties (later referred to as “business associates”) to perform functions and services involving the use of PHI. Regulators also recognized that protections for PHI should persist whether PHI resides with a CE or a BA. However, the original HIPAA statute did not authorize HHS to regulate BAs. So, to ensure PHI would remain safe in the hands of BAs, HHS had to regulate BAs indirectly by requiring CEs to obtain written assurance that BAs would handle PHI appropriately. HIPAA specifically requires CEs to execute business associate agreements (BAAs) with BAs that include various provisions set out within the Security and Privacy Rules. Notably, under the original regulations, BAs had only to afford “reasonable and appropriate” protections for PHI; they did not have to protect electronic PHI in accordance with the comprehensive and detailed specifications in the Security Rule. Much of that changed as a result of the HITECH Act.

HITECH Act: Foundation for Change
The American Recovery and Reinvestment Act (ARRA) of 2009 signed into law by President Obama included the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The

HITECH Act was designed to promote the widespread adoption and standardization of health information technology. Recognizing that increased use of healthcare information technology would heighten security and privacy risks, Congress included provisions within the Act to improve HIPAA’s privacy and security protections and enacted the first federal data breach notification requirement. Of even greater significance, Congress fundamentally altered the regulatory landscape for BAs by subjecting them to direct regulation.

**Omnibus Rule: HITECH Act Becomes Reality**

The Omnibus Rule in part implements the HITECH Act mandate to apply provisions of HIPAA directly to BAs. Although HHS has had the authority to enforce such provisions against BAs for several years, the agency agreed not to exercise its enforcement powers against BAs prior to the publication of the Omnibus Rule. That changes after September 23, 2013.

Of significance for law firm-BAs, the Omnibus Rule:

- Applies the HIPAA Security Rule directly to business associates working with electronic PHI (ePHI) just as the Security Rule applies to CEs.
- Applies provisions of the Privacy Rule governing permissible uses and disclosures directly to business associates, including the requirement that uses and disclosures of PHI must be limited to the “minimum necessary” to accomplish an intended purpose.
- Applies civil and criminal penalties for applicable HIPAA violations directly to business associates.
- Retains the requirement covered entities and business associates to enter into business associate contracts that meet the specific requirements set forth in the Security Rule and Privacy Rule.
- Creates a rebuttable presumption that any acquisition, access, use or disclosure of PHI not permitted under the HIPAA Privacy Rule is a breach subject to the Breach Notification Rule unless a covered entity or business associate can demonstrate that “there is a low probability that the [PHI] has been compromised based on a [documented] risk assessment.”
- Expands the definition of BAs to include subcontractors and other types of entities.
- Clarifies that existing BAAs must be updated in accordance with the Omnibus Rule but allows certain agreements to be grandfathered in beyond the initial compliance deadline.
- Applies federal common law of agency and holds CEs/BAs liable (as principals) for the acts of BA-agents. [The Omnibus Rule eliminates the exception to vicarious liability that existed under the original rule for agents that were business associates and had a valid business associate agreement in place.]
- Expands civil monetary penalties with up to $50,000 per individual violation up to a total of 1.5 million dollars per year for violations of a single provision.
- Mandates business associates notify covered entities in the event of a PHI breach suffered by a business associate no later than 60 days following the incident.
- Clarified that downstream subcontractors of business associates are subject to the HIPAA requirements as business associates.
Mandates that business associate agreements be updated in accordance with the Omnibus Rule.

A few especially noteworthy changes are discussed in more detail below.

**Expanded Definition of Business Associates & New Requirements**

The Omnibus Rule expands the definition of a “business associate” to include all entities that create, receive, maintain, or transmit PHI on behalf of a covered entity or business associate. HHS explicitly applies that definition to include entities that store PHI (electronic or paper) on behalf of CEs/BAs and even if the entity does not view the PHI. The Omnibus Rule also specifically adds each of the following to the definition of BAs: (1) subcontractors (see below); (2) patient safety organizations; (3) health information organizations; (4) e-prescribing gateways; and (5) vendors of personal health records that provide services on behalf of a covered entity.

Under the Omnibus Rule, a subcontractor is a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate. When a subcontractor creates, receives, maintains, or transmits PHI on behalf of the BA, the subcontractor itself becomes a BA and must then comply with applicable provisions of HIPAA. This holds equally for subcontractors of subcontractors all the way down the chain. Notably, BA and subcontractor liability for HIPAA violations arises immediately “when a [BA or subcontractor] creates, receives, maintains, or transmits protected health information on behalf of a covered entity or business associate and otherwise meets the definition of a business associate” even absent a business associate agreement. So, it will be important to anticipate situations where a BA relationship is likely to arise to ensure compliance.

BAs will need much more robust HIPAA compliance program to address the extensive set of requirements to which they will be held. Those working with PHI in electronic form must meet the numerous standards and implementation specifications set out in the Security Rule in addition to maintaining comprehensive written policies and procedures. BAs must also enter into written BAAs with their subcontractors and ensure that their BAAs contain the specific provisions required by the HIPAA Privacy and Security Rules. Without those agreements in place, any disclosure of PHI by a BA to a subcontractor would be impermissible under the Privacy Rule and would separately give rise to multiple violations under the Security Rule.

The Omnibus Rule subjects BAs to direct liability for impermissible uses or discloses under the applicable BAA or under the Privacy Rule. It also extends the “minimum necessary” standard directly to BAs and their subcontractors: When using, disclosing or requesting PHI, BAs must “make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.” BAs and subcontractors will need to develop, adopt and enforce internal policies accordingly.

In summary, the Omnibus Rule subjects BAs to direct liability for the following:

- Impermissible uses and disclosures under the Privacy Rule or BAA;
- Failure to provide breach notification as required;
• Failure to provide access to a copy of electronic PHI to either the covered entity, the individual, or the individual’s designee;
• Failure to disclose PHI where required by HHS to investigate or determine the business associate’s compliance with HIPAA;
• Failure to provide an accounting of disclosures; and
• Failure to comply with the requirements of the Security Rule.

Loss Prevention Recommendations

Identifying Matters Subject to HIPAA
Under HIPAA, a business associate relationship arises when a firm provides legal services to a covered entity or a business associate and the provision of the service “involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity” to the firm. In an article for the Michigan Bar Journal, health care attorney Suzanne Nolan offers the following advice to help lawyers in other practice groups identify matters that make the firm a business associate:

When representing a [covered entity or] business associate, an attorney will need to determine if his or her representation of the client involves use of or access to PHI. If it does, then the attorney must enter into a business associate agreement with the client and otherwise comply with HIPAA.

Attorneys also should be mindful of when they are apt to encounter PHI during the course of representing a client. Attorneys tend to think of themselves as not being subject to HIPAA except when working with health insurance claims, billing information, or information directly describing a patient’s health condition or treatment. However, because the definition of PHI is fairly broad, attorneys are apt to handle PHI when they (1) represent a covered entity or a business associate in enforcing a restrictive covenant against an employee who is soliciting patients of the covered entity or who has disclosed patient data to a new employer, (2) provide representation in the sale or purchase of a covered entity or business associate and have access to a patient list or a detailed list of accounts receivable, or (3) represent a covered entity or business associate in audits or governmental investigations.

BAAs with Clients
Firm policy should ensure that attorneys entering into BAAs on behalf of the firm have expertise in HIPAA, state data privacy laws and the applicable rules of professional conduct. Negotiating an agreement in which the firm and client have potentially adverse interests must be handled carefully and in accordance with the rules of professional conduct. Special care should be taken with existing clients, many of whom will need to negotiate new BAAs to comply with the Omnibus Rule. Firms should advise such clients to seek independent representation for these negotiations.
CEs increasingly seek to include indemnification provisions in their BAAs. Law firms should be cautious about entering into a BAA with an indemnification provision in favor of the client as such provisions can impact coverage under the firm’s LPL policy.

The firm should retain a copy of all BAAs centrally. Designating a central repository for BAAs is useful for at least two reasons. First, all attorneys and support staff working with PHI should be required to review the disclosure and usage restrictions in the applicable BAA prior to obtaining access. BAAs now have direct liability for any impermissible uses or disclosures, which makes it vital for those working with PHI to understand the applicable restrictions. Second, firms will need to retain a copy of the BAA in accordance with HIPAA’s retention requirements. Storing the BAA in a central repository will facilitate appropriate record retention and ensure the BAA is readily accessible when needed.

Review Insurance Coverage for Losses Related to HIPAA

LPL policies vary with respect to coverage for losses under HIPAA. Some policies specifically exclude regulatory penalties from the scope of professional services. Other policies include some level of coverage. Firms obligated to comply with HIPAA as business associates should review existing coverage and consider supplementing it.

Conclusion

Between the federal government’s commitment to aggressive enforcement, HIPAA’s harsh penalty scheme, and the importance of compliance for clients, law firm management should take the publication of the Omnibus Rule as an occasion to assess the firm’s compliance with HIPAA. Loss prevention partners, general counsel and risk professionals should determine whether the firm has HIPAA compliance obligations and where applicable take steps to bring the firm into full compliance. Achieving compliance will be a non-trivial endeavor for many firms, especially when health care attorneys within affected firms have ample demands on their time as clients struggle to understand the 563-page Omnibus Rule. Firms should consider starting their compliance efforts sooner rather than later and in any event well in advance of the September 23 deadline.

4 The Security Rule applies only to PHI in electronic form (ePHI). The Privacy Rule applies to PHI in all forms.
5 See Omnibus Rule, supra note 1, at 5,586.
7 There is one exception. Officially, HHS has been enforcing the interim final Breach Notification Rule against BAs.
8 See Omnibus Rule, supra note 1, at 5,641.
9 See Omnibus Rule, supra note 1, at 5,571.
10 45 C.F.R. § 160.103 (as amended).
11 See Omnibus Rule, supra note 1, at 5,571.
12 See id. at 5,598. Law firms that receive PHI from CE/BA-clients would be liable for violations of HIPAA even absent a BAA.
13 For ongoing violations of the HIPAA Security and Privacy Rules, each day may count as a separate violation for purposes of calculating civil monetary penalties. Assume the impermissible disclosure described amounts to a violation of four provisions of HIPAA. At up to $50K/provision each day, the potential penalties very quickly add up. Law firms should be careful to ensure that any subcontractors to whom PHI is disclosed have first signed BAAs with the firm. See Omnibus Rule, supra note 1, at 5,691.
14 See 45 C.F.R. § 164.502 (as amended)
15 See 45 C.F.R. § 160.103 (as amended).

About the Author: Matt Wolf, Principal at Carlson & Wolf

Matt Wolf (B.A., UC Berkeley; J.D. UC Berkeley Law) has 15 years of experience in information technology and security. He focuses on the intersection between the law and information security and privacy, routinely advising clients on state and federal regulations in these areas. He spent the first decade of his career as a Microsoft consultant working on emerging security and policy issues within the company’s MSN division, responsible for delivering online services to millions of Microsoft customers worldwide. In that capacity Mr. Wolf worked with technical, executive, and legal teams, helping to foster a collaborative approach to information security and privacy issues. After earning his J.D. from UC Berkeley School of Law, he accepted a position as a Scholar in Residence and explored issues in ethics, political theory and constitutional law. In addition to his academic pursuits, Mr. Wolf directed an information security assessment program to evaluate healthcare and other high-risk data environments. He now works as an information security and privacy consultant to the legal industry as a principal at Carlson & Wolf. Mr. Wolf is a member of the California Bar.

Carlson & Wolf is an information security and privacy consulting firm serving the legal industry. They provide their law firm clients with comprehensive information risk management and security services to address both strategic and tactical needs.

Their offerings include:

Services

Strategic

• Information Governance Evaluations
• Security Program Planning
• Information Risk Management Consulting
• Awareness & Education Program Design

Tactical

• Core Security Awareness Training Courses (CLE eligible)
• Custom Security Awareness Training Courses
• Client Audit Preparation / Response
• Technical Security Assessments
• Compliance Reviews