MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Employee Benefits Alert: Stimulus Bill Expands HIPAA Privacy and Security Rules to Business Associates

Impact on Group Health Plans, Benefits Brokers/Consultants, and Third-Party Administrators

2/20/2009

The "administrative simplification" requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") impose privacy and security standards, among others, on "covered entities" (*i.e.*, health plans, most health-care providers, and health-care clearinghouses). These rules are generally burdensome and complex, and, as a result, covered entities often look to outside vendors/service providers to assist in them in their day-to-day operations. Recognizing this to be the case, the final HIPAA privacy and security regulations require covered entities to enter into contracts with their vendors and service providers (or "business associates" in the parlance of the HIPAA final privacy and security rules) obligating them to safeguard "Protected Health Information" (PHI) (in the case of the privacy rule) and "electronic Protected Health Information" (ePHI) (in the case of the security rule). The precise nature of the obligations imposed on business associates under the privacy and security rules was left vague, however, and many business associates were content to simply sign a business associate agreement and do little more.

The American Recovery and Reinvestment Act of 2009 (the "Act") contains a series of provisions aimed at strengthening and extending the basic HIPAA privacy and security protections. Among other things, the Act tightens the rules relating to the minimum necessary disclosures of PHI, imposes additional notice requirements in the case of security breaches, and grants new enforcement powers to the states. Additionally, it extends certain, key substantive privacy and security provisions to business associates.

Group health plans routinely look to benefits brokers and consultants, third-party administrators, and other vendors to assist with plan maintenance and operation. This is especially true of self-funded plans and larger, fully insured programs that are experience-rated. The Act's provisions as they apply to business associates will raise the compliance bar for these and other entities. Service providers to group health plans will need to revisit their HIPAA compliance programs with an eye toward complying with these rules. This client alert describes the provisions of the Act that affect business associates generally.

Background

When it enacted HIPAA, Congress chose to regulate *only* covered entities, a term that includes neither employers nor business associates of covered entities. Under the basic HIPAA standards, PHI and ePHI can generally only be shared among covered entities. This presented the regulators with something of a conundrum: orderly administration of group health plans requires employers and their business associates to have access to all sorts of HIPAA-protected medical information, but access would be barred under the basic regulatory scheme absent some special rule or exemption. The solution was to require contracts with business associates with certain "business associate" covenants.

The Privacy Rule

Compliance with the privacy rule requires varying levels of employer involvement, depending on whether the group health plan is self-funded or fully insured.

Self-funded Plans

Since someone must act on behalf of the self-funded plan, the plan's workforce typically consists of persons who work for the employer. While it might be possible to outsource the plan's covered functions in their entirety to an administrative services-only (ASO) provider, this is rare—at least in part because the ASO provider would need to be a plan fiduciary for ERISA purposes.

Fully Insured Plans

In the case of fully insured plans, the level of compliance depends on the extent to which the plan sponsor needs or wants access to PHI. Fully insured group health plans are exempt from the bulk of the privacy rule's compliance burdens if they receive no PHI, or if they receive only "summary health information" and only for the purpose of obtaining premium bids for providing health insurance coverage to the group health plan or modifying, amending, or terminating the group health plan.

Security Rule

The security rule focuses on such things as unauthorized network access, breaches of network firewalls, hackers, computer viruses, and compromised passwords, all of which could compromise or disrupt the flow of ePHI. The security rule is intended to protect ePHI against careless or malicious individuals who may inadvertently or intentionally exploit system vulnerabilities and misuse sensitive medical data. While the privacy rules determine who should have access to medical records, the security provisions establish the manner in which medical records must be protected from inappropriate access. The security rule requires covered entities to:

- ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits;
- protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the rule; and
- ensure compliance with the rule by its workforce.

The final security rule establishes a series of security "standards" covering administrative, physical, and technical safeguards that, according to the U.S. Department of Health and Human Services ("HHS"), are based on "generally accepted security procedures." The term "standard" for purposes of the final security rule means a baseline security requirement. For some but not all of these standards, the rule also prescribes "implementation features." An implementation feature explains how to go about satisfying the standard. The implementation specifications are further classified as "required" or "addressable." While the covered entity must adopt those that are required, it can choose alternative ways to comply with those that are addressable, or it can choose not to comply so long as (in each case) the reason for the alternative or noncompliance is reasonable and documented. The implementation specifications of the security awareness and training standard, for example, are addressable. This means that they need not be followed to the letter if there is a good reason to deviate.

The Business Associate Requirement

A "business associate" is a person or entity that "assists a covered entity with a function or activity that involves the use or disclosure of individually identifiable health information" (a "covered function"). The crux of the business associate relationship is that the business associate performs or assists in the performance of a function or activity that involves the use or disclosure of PHI. An obvious example is that of a self-funded group health plan that chooses to outsource its claims processing and other administrative services. Some service providers, such as janitorial services, may have incidental access to PHI but they may not perform or assist with the performance of a covered function, or the services that they provide may not involve or require the use or disclosure of PHI. Such a service provider is not a business associate, even though it might technically have access to PHI in the course of performing its duties. Such access is permitted so long as the covered entity has adopted reasonable safeguards as otherwise required by the privacy rule. In this instance, a reasonable safeguard might include a confidentiality clause in the contract with the non-business associate service provider.

Both the final privacy rule and the final security rule include business associate covenant requirements.

The final privacy rule requires that the group health plan obtain "satisfactory assurances" from its business associate that the business associate will safeguard the PHI it receives or creates on behalf of the health plan. The satisfactory assurances must be set out in a written contract or other agreement that includes:

- a description of the permitted and required uses of PHI by the business associate;
- a prohibition against the business associate using or disclosing the PHI for any purpose other than as permitted or required by the agreement or as required by law; and
- a requirement that the business associate implement appropriate safeguards to prevent unauthorized uses or disclosures of PHI.

Before the Act, the privacy rule said nothing about how a business associate should go about satisfying these requirements. In contrast, the business associate compliance standards under the security rule were a little easier to discern. The business associate was required to implement administrative, physical, and technical safeguards that "reasonably and appropriately protect the confidentiality, integrity and availability of the ePHI it creates, receives, maintains or transmits." It was also required to ensure that its agents, including subcontractors, do likewise. This has generally been interpreted to mean that, at a minimum, a business associate that expects to handle ePHI in connection with the performance of business associate functions on behalf of a covered-entity client had to conduct a risk assessment and adopt, document, and monitor applicable safeguards.

The Act

The Act modifies the substance of the HIPAA privacy rules as they apply to business associates in three important respects:

- business associates are now subject to the substantive provisions of the HIPAA privacy and security rules generally in the same manner and to the same extent as covered entities;

  NOTE: According to the the Conference Committee Report accompanying the Act, the Act "would apply the HIPAA Privacy Rule, the additional privacy requirements, and the civil and criminal penalties for violating those standards to business associates *in the same manner as they apply to the providers and health plans for whom they are working*"[1] (emphasis added). But the Act does not do this. It instead (i) codifies the business associate contact requirement (which was previously a purely regulatory provision), (ii) requires business associates to comply with the privacy requirements added by the Act, and (iii) imposes an obligation on business associates to cure breaches by the counter-party covered entity. This apparent disconnect could be addressed in regulations.

- business associates are now subject to civil and criminal penalties for violation of these rules; and
- the Secretary of the Department of Health and Human Services is required to conduct periodic compliance audits of business associates as well as covered entities.

The Act adds a series of notice requirements that apply to both covered entities and business associates where there has been a use or disclosure of "unsecured protected health information." "Unsecured protected health information" means PHI that is not secured through the use of a technology or methodology approved by HHS. Specifically, a business associate that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information" is required to notify the covered entity of the breach within 60 days of discovery. Where contact information is deficient or out of date, and where ten or more individuals are affected, HHS may require that notice be posted on the covered entity's website, or even published in major print or broadcast media, and include a toll-free phone number. Where 500 or more individuals are affected, public notice is mandated.

The Act also includes new standards that apply to the "minimum necessary" requirements, health-care operations standards, limited data sets, accounting for disclosures of PHI, and marketing, among others. These changes apply to both covered entities and business associates.

Compliance Steps

Simply put, the Act raises the HIPAA compliance bar for covered entities and significantly raises the HIPAA compliance bar for business associates.

Group health plans that are subject to HIPAA will need to revisit their HIPAA privacy and security efforts to comply with the new rules. As a practical matter, however, most group health plans tend to rely heavily on their outside advisors (a/k/a business associates). As a consequence, there will be increased pressure to ensure that up-to-date business associate agreements are in place and that business associates are fully compliant.

For their part, business associates will, in many instances, need to ramp up their compliance efforts in connection with both privacy and security. With respect to the privacy rule, this will apparently require written policies and procedures, workforce training and discipline, and periodic compliance reviews, among other things. For purposes of the security rule, it will entail the adoption of physical, administrative, and technical safeguards, and the adoption of security policies and procedures.

Endnotes

[1] H.R. Rep. No. 111-16, at 493 (2009) (Conf. Rep.).

For assistance in this area, please contact one of the attorneys listed below or any member of your Mintz Levin client service team.

BOSTON

Alden Bianchi
(617) 348-3057
AJBianchi@mintz.com

Tom Greene
(617) 348-1886
TMGreene@mintz.com

Addy Press
(617) 348-1659
ACPress@mintz.com

Patricia Moran
(617) 348-3085
PAMoran@mintz.com

NEW YORK

David R. Lagasse
(212) 692-6743
DRLagasse@mintz.com

Gregory R. Bennett
(212) 692-6842
GBennett@mintz.com

Jessica Catlow
(212) 692-6843
JCatlow@mintz.com
