A Timely Analysis of Legal Developments

ASAP®

February 5, 2013

What Do Employers Really Need to Know About the New HIPAA/HITECH Omnibus Final Rule?

By Philip Gordon

The Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act Omnibus Rule, published in the *Federal Register* January 25, 2013, makes many changes to the HIPAA Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule, with substantial impact on employers. While these changes do not alter the fundamental structure of HIPAA compliance, employers still face a relatively lengthy "to do" list to comply with all of the new requirements. Perhaps, even more importantly, once the revised regulations go into effect, employers will confront much higher enforcement risk and significantly increased exposure to six- and seven-figure civil monetary penalties.

HIPAA Compliance for Employers Will Change in the Details, Not the Fundamentals

Employers that sponsor one or more self-insured, HIPAA-covered group health plans—group health, dental, vision, pharmacy benefits, long-term care, health care reimbursement flexible spending accounts, or employee assistance programs—are required to comply with all relevant HIPAA regulations. The principal compliance obligations include the following: (a) restricting access to protected health information (PHI) to employees who perform plan administration functions; (b) ensuring that these employees use and disclose PHI only as permitted under the HIPAA Privacy Rule; (c) implementing the physical, technical and administrative safeguards described in the HIPAA Security Rule for electronic PHI; (d) notifying plan participants when a security breach occurs; (e) refraining from disclosing PHI to third-party service providers, known in HIPAA parlance as "business associates," until the business associate signs a contract (or "business associate agreement"), which contains certain language required by the Privacy Rule; (f) notifying employees of the plans' privacy practices; (g) establishing policies and procedures to administer the rights of plan participants under HIPAA; and (h) amending plan documents.

After the Omnibus Final Rule becomes effective March 26 and compliance with most changes becomes mandatory September 23, 2013 employers will still be required to engage in all of these compliance activities, but several of them will require modification. Most significantly, the Omnibus Final Rule materially lowers the security breach notification standard. That change, coupled with revisions to the HIPAA Enforcement Rule, substantially increases enforcement risk. In addition, most employers will be required to distribute updated notices of privacy practices during the 2013

open enrollment season and to negotiate amendments to their business associate agreements. Finally, because the Omnibus Final Rule, for the first time, incorporates prohibitions against genetic discrimination into HIPAA, employers also will need to review their health risk assessments to ensure that they do not provide incentives to plan participants to disclose their genetic information. All of these changes are described in more detail below.

The Revised Security Breach Notification Standard Increases the Risk of HIPAA Enforcement

The Omnibus Final Rule establishes a new and materially lower standard for determining whether an employer is required to notify plan participants of a security breach involving their PHI. The prior standard required notification only if an unauthorized use or disclosure of unencrypted PHI "posed a significant risk of financial, reputational or other harm" to the individual.[1] Under the revised standard, *any* unauthorized use or disclosure of unencrypted PHI triggers a security breach notification obligation unless the employer can prove "a low probability that the [PHI] has been compromised based on a risk assessment."[2]

The referenced risk assessment must consider at least the following four factors: "(i) the nature and extent of the [PHI] involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the [PHI] or to whom the disclosure was made; (iii) whether the [PHI] was actually acquired or viewed; and (iv) the extent to which the risk to the [PHI] has been mitigated."[3] Other factors may also be considered where necessary.[4] When an employer determines that notice is not required, it must document its risk assessment supporting that conclusion and, if that decision is questioned in an investigation, carry the burden of proving a low probability of compromise to the HHS or to state attorneys general who also are authorized to enforce HIPAA.[5]

Ironically, nowhere in the massive regulatory commentary, or in the Omnibus Final Rule itself, does HHS define the word "compromise." However, the second risk assessment factor suggests that receipt of PHI by an unauthorized person as a result of the impermissible use or disclosure of PHI, standing alone, generally is not enough; otherwise, the other factors in the mandatory risk assessment would be unnecessary. Consequently, it appears that to justify a decision *not* to provide notice, an employer must establish a low probability that an unauthorized recipient (or a potential unauthorized recipient in the case where PHI is lost) misused, or may misuse, the information. In addition, in light of the first risk assessment factor, the regulators likely will take the position that the more sensitive the PHI received by the unauthorized recipient, the lower the likelihood of misuse will need to be in order to justify *not* providing notification.

With this understanding of the revised security breach notification standard, it becomes apparent that employers likely will be required to provide security breach notification more frequently under the Omnibus Final Rule. In our experience, impermissible uses and disclosures of PHI involving employee benefits information most commonly involve the following: (a) email attachments containing PHI that are sent to the wrong recipient; (b) email sent to the correct recipient but with an attachment containing PHI not intended for that recipient; (c) the loss or theft of a portable electronic storage device containing unencrypted PHI; (d) explanations of benefits (EOBs) sent to the wrong plan participant; (e) EOBs with PHI either printed on the envelope or viewable through a clear envelope window; and (f) benefits websites that because of a technical error permit viewing of one plan participant's PHI by other plan participants. In most of these situations, especially those involving dozens, hundreds, or thousands of plan participants (which often is the case), it will be infeasible or overly burdensome to gather the facts necessary to *prove* what each unauthorized recipient did with, or might have done with, the errant PHI. Consequently, it likely also will be difficult to *prove* to the satisfaction of regulators "a low probability that the [PHI] has been compromised" because the employer likely will not have adequate documentation to support that conclusion.

The increased likelihood of a duty to notify translates into an increased risk of enforcement. HHS' record to date demonstrates a pattern of "breach-driven enforcement." Most of the publicized settlements with a covered entity originated in a security breach. The reason for this pattern is obvious: under the HIPAA Breach Notification Rule, covered entities are required to notify HHS of a security breach, effectively putting a target on their back.[6]

---

1 Interim Final HIPAA Breach Notification Rule, 45 C.F.R. § 164.402.

2 Final HIPAA Breach Notification Rule, 78 Fed. Reg. 5566, 5695 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 164.402).

3 *Id.*

4 *Id.*

5 *Id.* at 5641, 5646.

6 Interim Final HIPAA Breach Notification Rule, 45 C.F.R. § 164.408.

In light of the above, employers should take steps to reduce the risk that the most common, impermissible uses and disclosures of plan participants' PHI will occur and also should be prepared to respond rapidly to those incidents to establish, when possible, a low probability that the PHI will be compromised. For example, employers should encrypt email containing PHI, where feasible, because an impermissible disclosure of encrypted PHI does not trigger a notification obligation. Benefits professionals and other employees who perform plan administration functions should receive additional training and/or periodic reminders on steps that can reduce the risk of a mis-addressed email or the creation of attachments containing PHI not intended for the email's recipient. Employers can implement a clearance procedure before any communication containing the unencrypted PHI of more than a small number of plan participants is emailed or mailed or can consider implementing data loss prevention (DLP) software. Employers also can implement policies that generally prohibit storage of unencrypted PHI on portable electronic media. Finally, employers should carefully vet the security procedures of printers and other service providers responsible for mailing EOBs and other communications containing plan participants' PHI.

To complement these measures, employers should develop a plan of action that will permit them to document that erroneous recipients of unencrypted PHI never actually viewed the PHI. For example, a corporate IT Department can recall email sent internally or delete it from corporate inboxes before the email is opened. If actual receipt of the misdirected PHI cannot be prevented, the employer may be able to call or email unauthorized recipients to confirm that they destroyed the PHI before reading it or promptly after realizing the communication containing the PHI was not intended for them. By documenting these steps, the employer could credibly prove "a low probability that the [PHI] was compromised," justifying a decision not to provide notice.

The Omnibus Final Rule Makes an Enforcement Action More Dangerous for Employers

While HHS has issued no public report to date of an employer paying a civil monetary penalty or a monetary settlement, that record might be coming to an end, due, in part, to two significant modifications by the Omnibus Final Rule to the HIPAA Enforcement Rule. First, the Omnibus Final Rule removes the requirement in the Enforcement Rule that HHS try to resolve investigations of complaints and compliance reviews by informal means and now makes informal resolution discretionary.[7] In other words, under the Omnibus Final Rule, HHS can move directly to a penalty proceeding.

Second, the Omnibus Final Rule permits HHS to impose a penalty on a covered entity for a violation by its business associate when the business associate is the covered entity's agent as determined by the federal common law of agency.[8] This somewhat obscure change is critical for employers that sponsor self-insured, HIPAA-covered plans because they rely heavily, if not exclusively, on service providers, such as third-party administrators, pharmacy benefits managers, flex spending account administrators, and EAP providers, to administer their health benefit plans. These employers also very often delegate to their business associates HIPAA compliance functions, such as storing and safeguarding PHI, responding to requests by plan participants to exercise their individual rights, and managing security breach notification—at least when the business associate is responsible for the breach.

To complicate matters for employers, it can be difficult to determine whether a business associate is acting as an agent or an independent contractor, and a business associate could act as both in the same business associate relationship. To distinguish between the two roles, HHS explains in the regulatory commentary to the Omnibus Final Rule that "[t]he right or authority to control the business associate's conduct … is the essential factor in determining whether an agency relationship exists . . . .[9] The regulatory commentary then provides the following additional guidance: If the only avenue of control is for a covered entity to amend the terms of the agreement or sue for breach of contract, this generally indicates that a business associate is not acting as an agent. In contrast, a business associate generally would be an agent if it enters into a business associate agreement with a covered entity that granted the covered entity the authority to direct the performance of the service provided by its business associate after the relationship was established. For example, if the terms of a business associate agreement between a covered entity and its business associate stated that "a business associate must make available protected health information in accordance with §164.524 based on the instructions to be provided by or under the direction of a covered entity," then this would create an agency relationship between the covered entity and business associate for this activity because the covered entity has a right to give interim instructions and direction during the course of the relationship.[10]

---

7 Final HIPAA Enforcement Rule, 78 Fed. Reg. 5566, 5690 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160.312(a)).

8 *Id.* at 5691 (to be codified at 45 C.F.R. pt. 160.402(c)).

9 *Id.* at 5581.

10 *Id.*

Given the potential under the Omnibus Final Rule for multimillion dollar penalties (discussed below), employers should now scrutinize their relationships with their business associates and take steps to reduce the risk that they could be penalized for their business associates' HIPAA violations.

While HHS' newfound discretion to forego informal complaint resolution and its ability to hold a covered entity responsible for its business associates' HIPAA violations are significant, the absence from the Omnibus Final Rule of any restriction on how HHS counts HIPAA violations for purposes of calculating a penalty likely poses the greatest risk for employers in light of the Omnibus Final Rule's penalty structure. Under that structure, penalties are capped at $50,000 per violation and $1.5 million for identical violations during a single calendar year.[11] Notwithstanding these caps, penalties can easily balloon into six- or seven-figure sums given HHS' discretion in calculating the number of violations. For example, in the regulatory commentary to the Omnibus Final Rule, HHS takes the position that in calculating a penalty based on the lack of a required safeguard, the agency can count each day the safeguard is absent as a separate violation. As another example, in calculating a penalty based on a security breach, HHS will count each person affected by the breach as a separate violation. In addition, although the total penalty for identical violations is capped at $1.5 million in a calendar year, HHS takes the position that it can seek up to $1.5 million per calendar year for different types of violations.[12]

Given this penalty structure, employers have a strong incentive to correct any potential violation quickly, so the number of days of violation and the number of plan participants affected will be minimized. In fact, employers should note that under the Omnibus Final Rule, it is an affirmative defense to a penalty that the covered entity corrected the violation within 30 days after it learned of the violation or with reasonable diligence would have known of it.[13]

Many Employers Will Be Required to Issue Revised HIPAA Privacy Notices During the 2013 Open Enrollment Season

The HIPAA Notice of Privacy Practices became a standard feature of open enrollment packets after the HIPAA Privacy Rule went into effect in April 2003. In the past ten years, employers have not been required to make any changes to those notices. The Omnibus Final Rule requires that employers make the following three additions to the privacy notice:

1. The notice must state that the covered health plans are required to obtain plan participants' authorization to use or disclose psychotherapy notes, to use PHI for marketing purposes, to sell PHI, or to use or disclose PHI for any purpose not described in the notice as well as a statement explaining how plan participants may revoke an authorization.[14]
2. The notices must state that the plans (other than a long-term care plan) are prohibited from using PHI that is genetic information for underwriting purposes.[15]
3. The notice must inform plan participants of their right to receive a notice when there is a breach of their unsecured PHI.[16]

Because HHS has determined that this new language constitutes a material change to the notice, employers that maintain a benefits website are required under the HIPAA Privacy Rule to (a) post the revised notice on their benefits website by the Omnibus Final Rule's compliance deadline of September 23, 2013; and (b) distribute the revised policy to the named insured in its next annual mailing to plan participants.[17] Employers that do not maintain a benefits website must distribute the revised notice within 60 days of the material revision to the notice.[18] If this group of employers waits until September 23, 2013 for their revised notice to become effective, then distribution of the notice by November 22, 2013 should coincide with their open enrollment season. Employers can distribute the revised privacy notice by email as long as the named insured agrees to electronic delivery.[19]

---

11 Final HIPAA Enforcement Rule, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160.404(b)(2)).

12 78 Fed. Reg. 5565, 5584 (Jan. 25, 2013).

13 Final HIPAA Breach Notification Rule, 78 Fed. Reg. 5565, 5692 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 164.410(b)(2)(ii)(A)).

14 78 Fed. Reg. 5565, 5701 (to be codified at 45 C.F.R. pt. 164.520(b)(1)(ii)(E)).

15 *Id.* (to be codified at 45 C.F.R. pt. 164.520(b)(1)(iii)(C)).

16 *Id.* (to be codified at 45 C.F.R. pt. 164.520(b)(1)(v)(A)).

17 *Id.* (to be codified at 45 C.F.R. pt. 164.520(c)(1)(v)(A)).

18 *Id.* (to be codified at 45 C.F.R. pt. 164.520(c)(1)(v)(A)).

19 *Id.* (to be codified at 45 C.F.R. pt. 164.520(c)(3)(ii)).

The Hidden Significance for Employers of the Omnibus Final Rule's Incorporation of GINA into HIPAA

Title I of the Genetic Information Non-Discrimination Act of 2008 (GINA), which prohibits employer-sponsored group health plans and health insurers from discriminating based on genetic information, required that the HIPAA Privacy Rule be amended to prohibit the use or disclosure of PHI that is genetic information for underwriting purposes[20]—even though GINA already prohibits such use of genetic information. The HIPAA Privacy Rule, like GINA, defines "underwriting purposes" to include "[t]he computation of premium or contribution amounts under the plan… (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program)."[21] In other words, the HIPAA Privacy Rule, like GINA, now prohibits employers' HIPAA-covered group health plans from offering plan participants an incentive, such as a rebate or discount, to provide genetic information—which HIPAA, like GINA, defines "genetic information" to include family medical history[22]—when completing a health risk assessment.

The hidden reason for this apparent duplication is twofold. First, because this modification of the Privacy Rule materially affects how a plan may use PHI, the HIPAA Privacy Rule requires, as noted above, that plan participants be informed in the plan's privacy notice of the prohibition on the use of PHI for underwriting purposes, potentially increasing public awareness of the prohibition on employers' offering incentives to plan participants to provide genetic information in a health risk assessment (HRA). Second, were a member of the newly educated public to complain about an improper HRA incentive, the employer as plan administrator would potentially be subject to HIPAA's much more costly civil penalty scheme (described above), thereby giving regulators more leverage to extract a big-dollar settlement or to obtain a substantial penalty.

Employers can avoid that result in one of two ways. They can eliminate altogether from the HRA questions seeking family medical history. Alternatively, they can create a bifurcated HRA which makes it clear that: (a) the plan participant qualifies for the incentive by completing the portion that does not call for family medical history, and (b) responses to any questions calling for family medical history are purely voluntary.

Employers Should Take Advantage of the Need to Renegotiate Their Business Associate Agreements to Comply with the Omnibus Final Rule

As originally promulgated, the HIPAA Privacy Rule prohibited covered entities from disclosing PHI to a business associate unless the business associate agreed by contract to certain restrictions on its use and disclosure of PHI and to cooperate with the covered entity when responding to an individual's request to exercise certain rights conferred by HIPAA.[23] The Omnibus Final Rule requires that business associate agreements impose the following obligations on the business associate in addition to those originally required by the Privacy Rule:

1. The business associate must limit its uses and disclosures of PHI to be consistent with the covered entity's minimum necessary policies and procedures.
2. The business associate must implement safeguards for electronic PHI in accordance with the HIPAA Security Rule.
3. The business associate must notify the covered entity of a security breach.
4. The business associate must enter into a similarly restrictive business associate agreement with any subcontractor to which the business associate discloses PHI.
5. If the agreement delegates any of the covered entity's HIPAA compliance obligations to the business associate, the business associate must fulfill those obligations to the same extent as the covered entity.[24]

To the extent any business associate agreement does not already contain these provisions, the agreement must be amended to include them when the agreement is next modified, if the modification occurs after the Omnibus Final Rule's compliance deadline of September 23, 2013, or by September 22, 2014, whichever is sooner.[25]

---

20 *See* 42 U.S.C.§ 1320d-9(a)(2).

21 78 Fed. Reg. 5565, 5696 (Jan. 25. 2013) (to be codified at 45 C.F.R. pt. 164.502(a)(5)(i)).

22 *See Id.* at 5688–89 (to be codified at 45 C.F.R. pt. 160.103).

23 45 C.F.R. § 164.504(e).

24 78 Fed. Reg. 5655, 5697–98 (Jan. 25, 2013) to be codified at 45 C.F.R. pt. 164.504(e)(2)(ii).

25 *Id.* at 5702 (to be codified at 45 C.F.R. pt. 164.532(e)(2)).

Employers should use the need to amend their business associate agreements as an opportunity to update those agreements not only to make the mandated changes, but also other changes that may be prudent in light of changes in the legal and technological environments over the past several years. For example, the employer should: (a) identify those services for which the business associate is likely to be deemed an agent and those for which it likely is to be deemed an independent contractor, and (b) decide whether the business associate's duties should be changed in any way to avoid the risk that the employer will be held vicariously liable for the business associate's HIPAA violations. This distinction in the business associate's role is particularly important in the area of security breach notification where, as described above, the risks are particularly high.

Employers also should consider whether any provisions not specifically required by HIPAA should be added to the business associate agreement. For example, the employer should consider including express prohibitions on the use of PHI for underwriting or marketing purposes and on the sale of PHI as embodied in the Omnibus Final Rule. Employers also should consider provisions that help reduce the risks associated with a security breach, such as restrictions on the business associate's use of cloud computing subcontractors to store PHI, a more robust description of required technical safeguards, or a requirement that the business associate obtain cyber risk insurance.

Conclusion

Employers should recognize that the Omnibus Final Rule likely ushers in an era of increased exposure for violations of HIPAA regulations. Employers can mitigate some of that increased exposure by reducing the risk of impermissible disclosures of PHI, revisiting their security incident response plan, updating their privacy notices, revising their HRAs, and amending their business associate agreements. More broadly, employers should take the opportunity created by the need to comply with the Omnibus Final Rule to review and refresh their entire HIPAA compliance program.

Philip Gordon, Chair of Littler Mendelson's Privacy and Data Protection Practice Group, is a Shareholder in the Denver office. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, or Mr. Gordon at pgordon@littler.com.