HHS Issues Final Omnibus HIPAA Rule

2013-01-24

On January 17, 2013, the Department of Health and Human Services issued long-awaited final regulations implementing the privacy, security, and breach-notification provisions of the HITECH Act and provisions of the Genetic Information Nondiscrimination Act ("GINA").[1] The regulations amend the HIPAA Privacy, Security, and Enforcement Rules and finalize a modified HIPAA Breach Notification Rule, which has been in effect on an interim basis since 2009.[2] The most important changes made by the omnibus rule include:

- expanding the definition of "business associate" to include a broad category of subcontractors, vendors of personal health records, patient safety organizations, health information organizations, e-prescribing gateways, and other entities that facilitate data transmission;
- finalizing the rule that business associates are directly liable under the Security Rule and many provisions of the Privacy Rule;
- revising the Privacy Rule by requiring new and more extensive notices of privacy practices, strengthening the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and expanding individuals' right to receive electronic copies of their health records;
- incorporating GINA requirements into the Privacy Rule to ban covered health plans, except those providing long-term care, from using or disclosing genetic information for underwriting purposes;
- finalizing the Breach Notification Rule, with new provisions to create a rebuttable presumption that any unauthorized acquisition, access, use, or disclosure of protected health information constitutes a breach, which can be rebutted by demonstrating that "there is a low probability" that the information has been "compromised"; and
- amending the Enforcement Rule to increase penalties and restrict affirmative defenses.

The new rules take effect March 26, but covered entities and business associates will generally have until September 23 to come into compliance.[3]

Expanded "Business Associate" Definition and Flow Down Requirements

HIPAA currently defines a "business associate" as an individual or organization that is not a member

of the workforce of a "covered entity" (health plans, health care clearinghouses, and health care providers that transmit electronic health information)[4] and that performs certain functions on behalf of, for, or to a covered entity that involve the use or disclosure of protected health information ("PHI").[5] The final omnibus rule broadens the definition of business associate to include a non-workforce member that "creates, receives, maintains, or transmits" PHI on behalf of a covered entity for the specified services and functions.[6] The final omnibus rule expressly provides that "business associates" includes (i) subcontractors of business associates that create, receive, maintain, or transmit PHI on behalf of another business associate;[7] (ii) personal health record vendors;[8] (iii) patient safety organizations;[9] and (iv) health information organizations, e-prescribing gateways, and other entities that routinely access and transmit PHI.[10] On the other hand, business associates do not include "mere conduits" of PHI such as mail delivery services and ISPs,[11] financial organizations that provide only payment processing and similar services,[12] and many third-party researchers.[13]

Two aspects of the definition of "subcontractor" added by the final omnibus rule are particularly noteworthy: (a) it encompasses all persons or entities that act as agents of a business associate in performing functions involving PHI, whether or not the relationship is defined by a written contract;[14] and (b) it covers subcontractors at all tiers.[15] Thus, the final omnibus rule, implementing a HITECH Act mandate, requires business associates to enter into written business associate agreements ("BAAs") with their subcontractors that include "satisfactory assurances" that PHI will be protected, "no matter how far 'down the chain' the information flows."[16]

Amendments to the Security and Privacy Rules

The final omnibus rule implements the HITECH Act provisions that made business associates directly subject to the entire Security Rule, which concerns electronic PHI only, and many provisions of the Privacy Rule, which applies to PHI in all forms.[17] One of the central tenets of the Privacy Rule now directly applicable to business associates and subcontractors is the requirement that uses and disclosures of PHI must be limited to the "minimum necessary" to accomplish an intended purpose.[18]

Among other changes in the Privacy Rule: Covered entities must revise their Notices of Privacy Practices to advise individuals that they have a right to be notified of a breach and that they must authorize the entity's uses and disclosures of their PHI for sale, marketing, fundraising, and certain other purposes.[19] Covered entities and business associates must also obtain patients' authorization before disclosing PHI for "remuneration" when the disclosure is not for patient treatment.[20] The amended Privacy Rule also implements individuals' right to review or receive copies of their PHI in electronic form, if electronic records are readily available.[21] Finally, the revised Privacy Rule requires covered entities to provide third parties with access to copies of an individual's PHI, upon the individual's signed, written request.[22]

The final omnibus rule also bans covered health plans (other than those providing long-term care) from using or disclosing genetic information for "underwriting purposes" such as determining eligibility, benefits, premiums, and cost sharing.[23]

Compliance with the revised provisions of the Security and Privacy Rules must generally be

achieved by September 23, 2013,[24] but entities operating under existing BAAs may be entitled to a transition period of up to one additional year to make any modifications that may be needed to attain compliance.[25]

Breach Notification Requirements

The HITECH Act called for a Breach Notification Rule, which the final omnibus rule revises into a final form.[26] Under the revised Breach Notification Rule, a covered entity that experiences a breach of unsecured PHI must notify affected individuals within sixty days of the end of the calendar year in which the entity learns of the breach.[27] If the breach affects 500 or more individuals, the entity may also be required to notify the Secretary of HHS, and, in certain cases, the media.[28]

The final omnibus rule modifies the definition of "breach" by creating a rebuttable presumption that an unauthorized acquisition, access, use, or disclosure of PHI constitutes a breach, which can be rebutted by demonstrating that "there is a low probability that the [PHI] has been compromised."[29] This will replace the subjective "risk of harm" standard that prevailed under the interim Breach Notification Rule. The revised Rule specifies several objective factors for determining whether PHI was compromised, including the nature of the PHI, the unauthorized persons who obtained it, and whether the information was actually accessed.[30]

Amendments to the Enforcement Rule: Increased Penalties and Fewer Defenses

Even for covered entities that have long been subject directly to HIPAA regulations, the stakes will now be higher. The HITECH Act raised the maximum penalty for HIPAA violations to $50,000 per violation and $1.5 million for a group of identical violations.[31] These increased penalties will now apply to violations by covered entities and business associates alike.[32]

The revised Enforcement Rule limits the affirmative defenses available to an entity that violates HIPAA. A complete defense is available only if the violation was not due to willful neglect and was corrected within thirty days of when the entity knew, or by exercising "reasonable diligence" would have known, of the violation.[33] This means that an entity's reasonable lack of knowledge of a violation, alone, will no longer constitute a complete defense, which it had in the past. Moreover, an employee or business associate's knowledge of a violation may be imputed to a covered entity.[34]

In addition, business associates will become directly liable for their breaches.[35] HIPAA requires BAAs to provide that business associates must notify the covered entity upon discovery of any violation.[36] The new rules also make business associates directly liable for the failure to provide such notice.[37] A covered entity or business associate is non-compliant if it knows "of a pattern of activity or practice of [its business associate or subcontractor] that constituted a material breach or violation of the [BAA]," unless the superior either took "reasonable steps" to cure the breach or end the arrangement.[38] Even when a subordinate's potentially violative activity is not known, the supervising authority may be liable for the violation if the subordinate was acting as the "agent" of the covered entity or business associate.[39]

Audits

In late December 2012, HHS completed a pilot program of audits of covered entities' compliance with the HIPAA Rules.[40] HHS plans to resume the HITECH-mandated audit program in late 2013 or in 2014 and plans to include business associates as potential audit subjects.[41] Audits will likely focus on compliance with the both preexisting requirements and the new HIPAA omnibus final rule.

If an audit report indicates "a serious compliance issue," HHS may initiate further compliance review.[42] Compliance reviews may also be sparked by breach notifications and third-party complaints.[43] To date, most HIPAA compliance reviews have focused on the failure of covered entities to adequately monitor their employees' handling of PHI.[44] Employees' inadvertent losses[45] and improper uses of health records,[46] and even third-party thefts of such records[47] have resulted in substantial payments by covered entities.

Conclusion

The final omnibus rule not only implements changes mandated by the HITECH Act, but also imposes some significant new burdens on covered entities and business associates. Combined with an increasingly aggressive enforcement program and heightened penalties for violations, organizations that handle HIPAA-protected information may need to examine their information-handling practices and their arrangements with business associates in order to ensure compliance with the new requirements.

---

[1] The text of the Final Omnibus HIPAA Rule and HHS's accompanying explanation of its provisions can be found at https://s3.amazonaws.com/public-inspection.federalregister.gov/2013-01073.pdf (last visited Jan. 22, 2013) ("Final Omnibus Rule"). They will be published in the *Federal Register* on January 25, 2013. *Id*. at 1. The HITECH Act is the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 226, codified at 42 U.S.C. §§ 300jj et seq.; §§17901 et seq. The Genetic Information Nondiscrimination Act of 2008 was enacted as Pub. L. No. 110-233, 122 Stat. 881 (2008).

[2] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996). The interim final Breach Notification Rule appeared at 74 Fed. Reg. 42,740 (Aug. 24, 2009).

[3] Final Omnibus Rule, at 15-17.

[4] 45 C.F.R. §§ 160.102, 160.103 (2012).

[5] *Id*. § 160.103.

Health information is not protected under HIPAA if it cannot reasonably be linked to a particular individual. 45 C.F.R. § 160.103. The Privacy Rule and HHS's accompanying *Guidance Regarding Methods for De-identification* explain the two methods by which information may be de-identified and thus removed from the scope of HIPAA. 45 C.F.R. § 164.514(b); *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability*

and Accountability Act (HIPAA) Privacy Rule, U.S. DEP'T OF HEALTH & HUMAN SERVICES (Nov. 26, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf ("*De-identification Guidance*").

De-identification can be accomplished by the removal of 18 individual identifiers in accordance with the "safe harbor" provision in 45 C.F.R. § 164.514(b)(2). Information may also be de-identified under the "expert determination" de-identification standard. Id. § 164.514(b)(1). Under this provision, a person with "appropriate" qualifications and methods may ascertain that there is a "very small" risk that information can be linked to a specific person. Id.

Because unidentifiable information is often of little value to health care entities, the Privacy Rule also provides for a "re-identification" process. 45 C.F.R § 164.514(c). This provision allows the entity to assign to a de-identified record a confidential "code or other means of record identification" so that only the covered entity may identify the subject of that information. *Id*.; *see also De-identification Guidance* at section 1.4.

[6] Final Omnibus Rule, at 26.

[7] *Id*. at 28-35.

[8] *Id*. Such vendors include any "person who offers a personal health record to one or more individuals on behalf of a covered entity." *Id*. at 24.

[9] *Id*. at 19-20.

[10] *Id*. at 20-28.

[11] *Id*. at 20-26.

[12] *Id*. at 38-39; see HIPAA § 1179, codified at 42 U.S.C. § 1320d–8.

[13] *Id*. at 37-38.

[14] *Id*. at 28-31.

[15] *Id*. at 32-35.

[16] *Id*. at 33. The Final Omnibus Rule clarifies that "[a] covered entity is not required to obtain . . . satisfactory assurances from a business associate that is a subcontractor." Final Omnibus Rule, at 523, 536; new 45 C.F.R. §§ 164.308(b)(1), 164.502(e)(1)(i). It is the responsibility of the subcontractor's *immediate superior*, i.e., the business associate, to ensure that the subcontractor signs a business associate agreement. Final Omnibus Rule, at 523, 536; new 45 C.F.R. §§ 164.308(b)(2), 164.502(e)(1)(ii). Nevertheless, because covered entities are ultimately responsible for the security of PHI distributed to their agents, see Final Omnibus Rule, at 60-66, 507-08, new 45 C.F.R § 160.402(c), they are best advised to address subcontractors specifically in business

associate agreements.

[17] HITECH Act § 13401, codified at 42 U.S.C. § 17931.

[18] Final Omnibus Rule, at 105, 536; new 164.502(b)(1).

[19] Final Omnibus Rule at 236-238, 553-556; new 45 C.F.R. § 164.520. Revision is not required where an existing Notice of Privacy Practices already complies with these new requirements. Final Omnibus Rule, at 240.

[20] *Id*. at 153-70, 543-46; new 45 C.F.R § 164.508; *see also* HITECH § 13406, codified at 42 U.S.C. § 17936.

[21] Final Omnibus Rule, at 265-66, 557-59; new 45 C.F.R. § 164.524(c)(2).

[22] Final Omnibus Rule, at 278-79, 557-59; new 45 C.F.R. § 164.524(c)(3).

[23] Final Omnibus Rule, at 533-34; new 45 C.F.R. § 164.502(a)(5).

[24] Final Omnibus Rule, at 2.

[25] *Id*. at 150.

[26] *Id*. at 295-97.

[27] *Id*. at 331, 528; new 45 C.F.R § 164.408(c).

[28] Final Omnibus Rule, at 438.

[29] *Id*. at 525-27; new 45 C.F.R. § 164.402.

[30] Final Omnibus Rule, at 304.

[31] *Id*. at 68-70.

[32] *Id*. at 68-70, 72, 75.

[33] *Id*. at 81-82.

[34] *Id*. at 86-87.

[35] *Id*. at 60-63, 66.

[36] *Id*. at 139, 142.

[37] *Id*. at 133.

[38] *Id*. at 138.

[39] *Id*.

[40] *HIPAA Privacy & Security Audit Program*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html (last visited Jan. 22, 2013).

[41] Marianne Kolbasuk McGee, *HIPAA Enforcer Reveals Audit Timeline*, HEALTHCAREINFOSECURITY (Dec. 14, 2013), http://www.healthcareinfosecurity.com/interviews/hipaa-enforcer-reveals-audit-timeline-i-1736 (interview of Leon Rodriguez, director of the Department of Health and Human Services' Office for Civil Rights).

[42] *Audit Pilot Program*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html (last visited Jan. 22, 2013).

[43] HITECH Act §§ 13401, 13404, codified at 42 U.S.C. §§ 17931, 17934 ; *see also OCR Update: HIPAA and HITECH Changes*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, OFFICE FOR CIVIL RIGHTS (October 11, 2012), *available at* https://www.privacyassociation.org/media/presentations/A12_Welcome_to_the_Jungle_PPT.pdf. Volunteers and trainees are considered a part of the covered entity and thus are not business associates under HIPAA. Final Omnibus Rule, at 45, 500; new 45 C.F.R. § 160.103.

[44] *See All Case Examples*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html (last visited Jan. 22, 2013).

[45] *Massachusetts General Hospital Settles Potential HIPAA Violations*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgeneralra.html (last visited Jan. 22, 2013).

[46] *UCLA Health System Settle Potential Violations of the HIPAA Privacy and Security Rules*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/uclaagreement.html (last visited Jan. 22, 2013).

[47] *HHS Settles HIPAA Case with BCBST for $1.5 million*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/bcbstagrmnt.html (last visited Jan. 22, 2013).

Authors

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089