

Articles

New HIPAA Rule Imposes Data Security and Privacy Obligations Directly Upon Vendors and Contractors of Covered Entities

February 2013

White & Case Technology Newsflash

Daren M. Orzechowski

Technology Newsflash

On January 25, 2013, the Department of Health and Human Services ("HHS") published the Final Rule to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")'s Data Security and Privacy Rules.¹ The Final Rule is the culmination of an over three-year effort to overhaul the existing provisions, which govern how individuals' health information is used and protected.² Many of the changes were required by the 2009 "HITECH" Act³, and most (but not all) are substantially similar to the Proposed Rule that HHS issued in July 2010 (the "Proposed Rule").⁴ Below is a high-level summary of the changes that will affect information technology companies that work with organizations covered by HIPAA.

More Companies are now "Business Associates" and thus Directly Responsible for HIPAA Compliance

HIPAA's Data Security and Privacy Rules have long required "covered entities" (i.e., health care providers, health plans, and health care clearinghouses that handle individuals' protected health information ("PHI")⁵) to contractually ensure that any entity that handles PHI on their behalf also complies with those HIPAA Rules.⁶ Now, any entity handling PHI on a covered entity's behalf (called a "business associate") is *itself* responsible for complying with the HIPAA Data Security and Privacy Rules.⁷ This change directly subjects business associates to HIPAA's enforcement scheme, which, as amended, can yield up to \$1.5 million in annual civil penalties for each HIPAA violation.⁸

In addition to being responsible for ensuring that it has HIPAA-compliant agreements in place with the covered entity it serves, a business associate must now also ensure that it has HIPAA-compliant agreements with all of its own subcontractors who handle PHI.⁹ The changes likely also mean vendors will need to be more focused on the data security and protection practices of the covered entities that they serve. Moreover, the subcontractor is also deemed a "business associate" if its services involve "the creation, receipt, maintenance, or transmission" of PHI, so it too is directly liable for HIPAA compliance and for its own upstream and downstream business associate agreements.¹⁰

The Final Rule describes specific types of entities that will be treated as business associates for HIPAA Data Security and Privacy purposes. Specifically, HHS added the following language to the types of entities that qualify as "business associates":

1. "A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to [PHI] to a covered entity and that requires routine access to such [PHI]; and
2. A person who offers a personal health record to one or more individuals on behalf of a covered entity."¹¹

HHS intends to release further guidance on what constitutes "routine access" to PHI, as such term is used in the Final Rule, but the agency stated that a key factor will be whether the opportunity to access PHI is "transient" or "persistent," noting also that a company cannot avoid the classification solely because it has never actually accessed the PHI.¹² Because the Data Security and Privacy Rules may now apply to any company in a covered entity's service provider chain, all companies who might create, receive, maintain, or transmit PHI should investigate the changes highlighted below and seek legal assistance to ensure that their contracts are still HIPAA compliant.

HIPAA Data Security Rule Delineates New Breach Notification Threshold

In the Proposed Rule, HHS defined a data security "breach" as the "*acquisition, access, use, or disclosure of [PHI] in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the [PHI]*", and clarified that the standard should be whether there was a "significant risk of financial, reputational, or other harm to the individual".¹³ HHS intended for this harm-based standard to avoid excessive breach notifications for inconsequential events.¹⁴ After receiving approximately 70 public comments about the harm-based standard (approximately 60 in favor and 10 opposed), HHS sided with the opponents, which were mostly consumer advocacy groups.¹⁵ Now, under the Final Rule, any unpermitted acquisition, access, use or disclosure of PHI (even those pertaining to a limited data set)¹⁶ is presumed to be a breach unless the party seeking to avoid breach notification obligations can show that there is a "*low probability that the [PHI] has been compromised*."¹⁷ Instead of showing there is no significant risk of harm to the individual as the Proposed Rule required, a company seeking to avoid breach notification obligations must now conduct a risk assessment regarding the PHI's security after the incident. The Final Rule requires this risk assessment to include, at minimum, consideration of all of the following factors:

1. the nature and extent of the PHI involved and the extent to which it is identifiable or could be made so;
2. the unauthorized person who obtained access to the PHI (and that person's own confidentiality obligations, if any);
3. whether the PHI was actually acquired or viewed (or whether there was merely an opportunity to do so); and
4. whether and to what extent the risk to the PHI has been mitigated.¹⁸

If the party can show a "low probability" that PHI has been compromised, then the incident will not be deemed a breach; otherwise, a breach is presumed and the company must undertake the notification obligations prescribed by the Data Security Rule.¹⁹ The new presumption of breach and the risk analysis requirement, in light of the inclusion of subcontractors as business associates, reflects HHS's intention to create a more reliable, consistent inquiry and chain of reporting scheme for data security incidents.²⁰

HIPAA Privacy Rule Limits Sale of PHI for Marketing Purposes

Finally, the Final Rule limits the use and disclosure of PHI for marketing and fundraising purposes and prohibits any sale of PHI without the individual's consent.²¹ The definition of "marketing" now includes all treatment and health care operations communications made by a covered entity using PHI, if, in exchange for making the communication the covered entity receives financial remuneration from the third party whose product or service is being marketed.²² Thus, business associates providing communications services for covered entities must treat all communications as "marketing" communications and so may not transmit them without first obtaining the individual's authorization for PHI to be used for such purposes.²³

Similarly, the Final Rule prohibits all "sales" of PHI, no matter the ultimate use, unless the individual provides written authorization and acknowledges that the disclosing entity is receiving remuneration.²⁴ The Final Rule defines a "sale" as "*a disclosure of [PHI] by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the [PHI] in exchange for the [PHI]*."²⁵ This includes disclosures in connection with access, license, or lease agreements,²⁶ but exempts disclosures for (i) public health purposes, (ii) research, (iii) treatment, and (iv) merger or change of control purposes, as well as disclosures between a covered entity and its business associate pursuant to an otherwise permissible business associate agreement.²⁷

The Rule goes into effect on March 26, 2013, with a compliance date of September 23, 2013.²⁸ Contracts entered into before January 25, 2013 will be deemed compliant through September 22, 2014 if those contracts complied with the previous HIPAA Data Security and Privacy Rules and remain un-renewed and unmodified during the course of this grandfathering period.²⁹ Because the Final Rule requires revision and reissuance of notices of privacy practices,³⁰ companies who may fall under the expanded definition of "business associate" should consult a privacy law practitioner to ensure that their agreements and practices are HIPAA-compliant by September 2013.

1 - HHS Office of Civil Rights, "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules", 78 Fed. Reg. 5,566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164) (hereinafter "Notice of Final Rule"), *available at* federalregister.gov/a/2013-01073.

2 - HHS, "New rule protects patient privacy, secures health information," News Release, (Jan. 17, 2013), *available at* hhs.gov/news/press/2013pres/01/20130117b.html.

- 3 - Health Information Technology for Economic and Clinical Health ("HITECH") Act, 42 U.S.C. §§ 300jj *et seq.*; 17901 *et seq.* (2009).
- 4 - See 75 Fed. Reg. 40,868 (July 14, 2010).
- 5 - PHI includes most individually identifiable information related to a person's past, present, or future physical or mental health, the person's receipt of health care or the person's payment therefor. 45 C.F.R. § 160.103.
- 6 - See 45 C.F.R. §§ 160.103 (as amended), 164.300 *et seq.* (Data Security Rule, as amended), 164.500 *et seq.* (Privacy Rule, as amended); see also Notice of Final Rule, *supra* note 1, at 5,566 (explaining HHS's basis for the amendments and noting that the covered entity itself is not required to enter into any contractual arrangement with, or otherwise monitor, a business associate's subcontractor).
- 7 - *Id.*; see also Notice of Final Rule, *supra* note 1, at 5,570-73.
- 8 - 45 C.F.R. §§ 160.404(b), 160.408 (as amended); see also Notice of Final Rule, *supra* note 1, at 5,578-85 (explaining the new penalty scheme, which is tiered based upon a violator's culpability).
- 9 - 45 C.F.R. §§ 160.103 (as amended) (defining "subcontractor" as "a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate" and defining "business associate" to include "subcontractor"); 164.300 *et seq.* (as amended), 164.500 *et seq.* (as amended).
- 10 - 45 C.F.R. § 160.103 (as amended); see also Notice of Final Rule, *supra* note 1, at 5,570-75.
- 11 - 45 C.F.R. § 160.103 (as amended); see also Notice of Final Rule, *supra* note 1, at 5,570-75 (explaining the reasons for the definitional modification and providing examples of the types of entities meeting the definition).
- 12 - Notice of Final Rule, *supra* note 1, at 5,572 (explaining that, to help clarify that an entity such as a data storage facility will likely qualify as a business associate even if it does not actually view any PHI, the definition of "business associate" now includes "maintenance" of PHI).
- 13 - See Interim Final Rule, 75 Fed. Reg. 19,006 (Apr. 27, 2009) (the July 2010 Proposed Rules did not modify the 2009 Interim Rules with regard to the Data Privacy Rule); see also Notice of Final Rule, *supra* note 1, at 5,639-46.
- 14 - *Id.*
- 15 - *Id.* at 5,640-41.
- 16 - *Id.* at 5,644.
- 17 - 45 C.F.R. § 164.402 (as amended) (definition of "breach").
- 18 - *Id.*; see also Notice of Final Rule, *supra* note 1, at 5,640-46 (explaining the factors in more detail and noting that a party may always elect to forgo the risk assessment and provide notification).
- 19 - 45 C.F.R. § 164.400 *et seq.*
- 20 - Notice of Final Rule, *supra* note 1, at 5,644 (reminding covered entities and business associates that encrypting PHI pursuant to guidance delineated in the Interim Rule still makes breach notifications following a data security incidents unnecessary, as it renders PHI unusable).
- 21 - 45 C.F.R. §§ 164.508(a)(3), 164.502(a)(5)(ii) (as amended); see also Notice of Final Rule, *supra* note 1, at 5,566.
- 22 - 45 C.F.R. § 164.501 (as amended) (definition of "marketing"); see also Notice of Final Rule, *supra* note 1, at 5,595-97 (explaining HHS's decision to abandon the Proposed Rule's exemption of certain communications regarding treatment and health care operations from the definition of "marketing" so as to achieve greater clarity).
- 23 - 45 C.F.R. §§ 164.501, 164.508(a)(3) (as amended).
- 24 - 45 C.F.R. §§ 164.502(a)(5)(ii)(B) (as amended) (definition of "sale" of PHI), 164.508(a)(4)(i) (as amended) (prohibition of sale of PHI without authorization); see also Notice of Final Rule, *supra* note 1, at 5,603-08.
- 25 - *Id.*; see also Notice of Final Rule, *supra* note 1, at 5,606-07 (explaining that "remuneration" means financial or nonfinancial benefits and clarifying that "sale" does not include remuneration paid by a covered entity to a business associate for the business associates' provision of transmission or other services on the covered entity's behalf).
- 26 - *Id.* at 5,606.
- 27 - 45 C.F.R. § 164.502(a)(5)(ii)(B)(2) (as amended).
- 28 - 45 C.F.R. § 160.105 (as amended); see also Notice of Final Rule, *supra* note 1, at 5,566.
- 29 - 45 C.F.R. § 164.532(e) (as amended).
- 30 - See, e.g., 45 C.F.R. § 164.520(b)(1) (as amended).

This article is provided for your convenience and does not constitute legal advice. It is prepared for the general information of our clients and other interested persons. This article should not be acted upon in any specific situation without appropriate legal advice, and it may include links to websites other than the White & Case website. White & Case LLP has no responsibility for any websites other than its own, and does not endorse the information, content, presentation or accuracy, or make any warranty, express or implied, regarding any other website.

This article is protected by copyright. Material appearing herein may be reproduced or translated with appropriate credit.

