

Healthcare Privacy Issues under the Omnibus Final Rule

May 28, 2013

Recently, the U.S. Department of Health and Human Services (HHS) announced new guidelines under HIPAA (Health Insurance Portability and Accountability Act of 1996) Privacy and Security Rules. One component of these new guidelines includes the HIPAA Omnibus Final Rule (“the rule”), which will have a dramatic impact on healthcare privacy including two significant updates. First, the rule has expanded the definition of a Business Associate. A Business Associate performs activities or functions on behalf of a Covered Entity (such as a hospital) while handling protected health information (PHI). The expanded definition of a Business Associate encompasses cloud vendors who handle PHI. Such cloud vendors may have denied their status as a Business Associate in the past. Second, the rule has also imposed liability upon a Covered Entity and Business Associate for acts of a subcontractor acting as an agent. The following discusses several of the key changes arising out of the HIPAA Omnibus Final Rule and how these key changes will impact Covered Entities, Business Associates, subcontractors and Business Associate Agreements. Compliance with these changes is required by September 23, 2013.

New Definition of Business Associate First, the new definition of a Business Associate will encompass additional organizations that may not have been considered a Business Associate in the past. A Business Associate is now considered to be an entity that “creates, receives, maintains or transmits” PHI. The rule clarifies that a Business Associate includes a health information organization, e-prescribing gateway, or other person that provides data transmission services with respect to PHI to a Covered Entity and requires access on a routine basis to such PHI. To the extent that a Covered Entity may utilize a cloud vendor to transmit PHI and the cloud vendor accesses such PHI as part of its work for the Covered Entity, the cloud vendor would be considered a Business Associate. In the past, cloud vendors were reluctant to acknowledge that they might be Business Associates, but the rule will likely require cloud vendors to reevaluate such assumptions.

Subcontractors are Business Associates Second, the rule expanded the definition of a Business Associate by including subcontractors. In HIPAA’s Final Rule, HHS explained that it extended HIPAA to subcontractors to “avoid having privacy and security protections for protected health information lapse merely because a function is performed by an entity that is a subcontractor rather than an entity with a direct relationship with a covered entity.” (Omnibus Rule, 78 Fed. Reg. at 5572-73.) The rule applies certain provisions of the HIPAA Privacy and Security Rules to subcontractors. In other words, a subcontractor must comply with HIPAA in the same manner as the primary Business

Associate. Furthermore, Business Associates must now enter into Business Associate Agreements with their subcontractors. **Liability for the Acts of an Agent** Third, the rule expanded the liability that a Covered Entity or Business Associate can incur when working with a subcontractor acting as an agent of the Covered Entity or Business Associate. Prior to the rule, a Covered Entity or Business Associate could assert several exceptions to mitigate any liability for acts committed by a subcontractor. The rule eliminated those exceptions. Federal common law principles will apply to determine the existence of an agency relationship. If an agency relationship is found, then the Covered Entity or Business Associate may be liable for the acts of its subcontractor. **Impact of Final Rule on Healthcare Organizations** The expanded definition of a Business Associate under the HIPAA Omnibus Final Rule and the potential for increased liability for acts committed by a subcontractor may lead to three significant revisions to Business Associate Agreements.

1. Companies operating in the healthcare sphere need to pay particular attention to the indemnification provision in Business Associate Agreements. Given the potential for increased liability, negotiating a strong indemnification clause to mitigate the acts of the subcontractor is important. Alternatively, a healthcare company that is concerned about the acts of a subcontractor could require its subcontractor to carry cyber risk insurance and request that the company be named as an insured in the subcontractor's policy.
2. Furthermore, Business Associates will need to enter into Business Associate Agreements with their subcontractors to the extent they did not have such agreements in place in the past.
3. Finally, Business Associate Agreements must contain certain key provisions to comply with the Final Rule. In the Business Associate Agreement, the Business Associate must:
 - agree to comply with the Security Rule with respect to electronic PHI;
 - agree to report breaches of unsecured PHI to the Covered Entity;
 - ensure that any subcontractors that create or receive PHI on behalf of the Business Associate agree to the same restrictions that apply to the Business Associate.

Navigating these complex changes to the healthcare privacy framework is important to mitigate the liability associated with handling electronic PHI while simultaneously protecting patient privacy.

Originally published on i-Sight.com's blog: "[Healthcare Privacy Issues under the Omnibus Final Rule](#)," *I-Insight* (May 28, 2013)

Related Practices

[Health Care](#)

[Cybersecurity and Privacy](#)

Related Industries

Health Care

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.