Client Alert

pillsbury

Employment

Health Care & Life Sciences

Privacy, Data Security & Information Use

February 7, 2013

Omnibus Final Rule Issued on HIPAA/ HITECH Act: Significant Changes for 'Business Associates'

By Gerry Hinkley, Allen Briskin and Caitlin Bloom

On January 25, 2013, the Department of Health and Human Services published the much-anticipated Omnibus Final Rule (the "Final Rule"), which, with respect to business associates and their subcontractors, conforms HIPAA's Privacy and Security Rules to a number of changes brought about by the HITECH Act, implements a number of regulatory changes seen in HHS's proposed rule-making, and modifies a number of other proposed regulatory changes.

The Final Rule expands the reach of the HIPAA Rules by clarifying that those who "maintain and transmit" protected health information on behalf of covered entities are subject to many of those rules as business associates of those covered entities. Moreover, certain subcontractors of business associates are now to be treated as business associates themselves. As a result, business associates and those subcontractors are required to enter into business associate agreements with each other, and those subcontractors will be responsible for HIPAA compliance not only under those contracts but also directly under the HIPAA Rules themselves. Finally, the Final Rule also changes a number of the mandated terms of business associate contracts and will require covered entities, business associates and subcontractors to revisit their existing agreements for compliance with the Final Rule's new requirements.

The Final Rule takes effect March 26, 2013, and compliance generally is required by September 23, 2013. Business associate contracts that were in effect on January 25, 2013, and that complied with the HIPAA Rules in effect on that date, may qualify for an extension of the compliance deadline if those contracts are neither modified nor renewed between March 26 and September 23, 2013. Business associate contracts that do not qualify for the extension must be brought into compliance by September 23, 2013. After that date, contracts that do qualify for the extension must be brought into compliance when they are renewed or modified and in no event later than September 22, 2014.

Expanded Definition of 'Business Associate'

Parties That "Create, Receive, Maintain or Transmit" Protected Health Information ("PHI"). The Final Rule clarifies and expands the HIPAA Rules' definition of "business associate" to include one who, other than in the capacity of a member of a covered entity's workforce, "creates, receives, maintains, or transmits" PHI on behalf of a covered entity for a function or activity that is regulated under HIPAA. As a result, as indicated under the HITECH Act, parties that provide data transmission services for covered entities (or for their business associates, as explained below), and who require routine access to PHI, are to be treated as business associates. In addition, those that provide data storage and other maintenance services and that have ongoing access to that PHI also now clearly fall within the HIPAA Rules' requirements for business associates. In contrast, those that act as mere "conduits" for the transmission of PHI, such as telecommunications carriers, remain outside HIPAA's regulation.

Subcontractors of Business Associates. Perhaps the most dramatic change with respect to business associates brought by the Final Rule is HHS's decision to implement its earlier rulemaking proposal to expand the definition of "business associate" to include certain subcontractors. The Final Rule adds a new definition of "subcontractor" that includes any person to whom a business associate delegates a function, activity or service, other than in the capacity of a member of the business associate's workforce. Any such subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate is also considered to be a business associate. As a result, like the business associate for which it provides services, the subcontractor is directly regulated under the Privacy and Security Rules, and is subject to compliance audits and potentially liable for civil money penalties and other enforcement measures for non-compliance.

Business Associate Contracts Between Business Associates and Subcontractors. Prior to the Final Rule, a business associate's contract with a subcontractor was required only to include the subcontractor's agreement to be bound by the same restrictions and conditions with respect to the treatment of PHI that applied to the business associate under its business associate contract with the covered entity. Under the Final Rule, the business associate and the subcontractor are required to enter into a business associate contract that includes all the terms and conditions for such contracts mandated by the Privacy and Security Rules. As a result, following the Final Rule, subcontractors will be responsible for an expanded set of legal obligations that arise both directly under the HIPAA Rules and under their business associate contracts.

Downstream Subcontractors. As a consequence of subcontractors being included within the definition of "business associate," the Final Rule provides that, if a subcontractor delegates functions to sub-subcontractors that involve the creation, receipt, maintenance, or transmission of PHI on behalf of a business associate, those sub-subcontractors will be treated as business associates and therefore be directly subject to the HIPAA Rules' requirements and required to enter into business associate contracts with their own subcontractors, if any, down to and including all downstream contractors that perform functions involving the creation, receipt, maintenance or transmission of PHI.

Permitted Uses and Disclosures of PHI by Downstream Subcontractors. The Privacy Rule will require that each business associate use and disclose PHI only for the purposes, and only when, permitted under the HIPAA Rules. A business associate that contracts directly with a covered entity will also be restricted by the limitations on use and disclosure of PHI imposed under its business associate contract with the covered entity. In turn, that business associate may only disclose PHI to a subcontractor to the extent permitted by that business associate contract with the covered entity, and the subcontractor may be further limited in its use and disclosure of PHI by any limits imposed under its business associate contract with the business associate. As a result, contracts with downstream subcontractors should be drafted and

managed carefully to comply with what may potentially be multiple levels of restrictions imposed upon permitted uses and disclosures of PHI through business associate contracts.

Other Business Associates. The Final Rule's expanded definition of "business associate" also clarifies that it applies to health information organizations, e-prescribing gateways, and others that provide data transmission services to covered entities with respect to PHI, and that require access on a routine basis to that PHI. While many parties offering personal health records ("PHRs") to consumers remain beyond HIPAA's jurisdiction, those who offer PHRs on behalf of a covered entity are covered by the HIPAA Rules as business associates.

Scope of Rules that Apply to Business Associates

Security Rule. The Final Rule requires all business associates, including subcontractors, to comply with the substantive provisions of the Security Rule, and implement administrative, physical and technical safeguards to ensure the confidentiality, integrity and availability of electronic PHI, and the Security Rule's policy and procedure and documentation requirements. However, the Security Rule retains its existing flexibility regarding the implementation of required safeguards, so that business associates and subcontractors may tailor their security measures to be appropriate to their size, complexity, and capabilities, their technical infrastructures and hardware and software capabilities, the cost of security measures, and the probability and criticality of potential risks to the electronic PHI they create, receive, maintain or transmit.

Privacy Rule. The Final Rule requires business associates, including subcontractors, to comply with specified provisions of the Privacy Rule. With some exceptions, business associates are subject to the Privacy Rule's rules concerning permitted uses and disclosures of PHI (though they are further limited to the uses and disclosures that would be permitted for the covered entity), the prohibition on the sale of PHI, and the Rule's requirements to adhere to the "minimum necessary" rule, enter into business associate contracts, and obtain authorizations for uses and disclosures of PHI not permitted by an exception. Under the Final Rule, business associates are required to support covered entities' compliance with their obligations to report breaches of unsecured PHI, to provide individuals with access to and copies of their PHI, to make certain amendments to PHI, and to provide accountings of disclosures.

Review and Revision of Business Associate Agreements

Covered entities, business associates, and those business associates' subcontractors should review their business associate and other contracts for compliance with the Final Rule, and prepare to make amendments or enter into new agreements as is required for compliance.

As noted above, the Final Rule will require business associates' contracts with their subcontractors to incorporate all the terms and conditions the Privacy Rule mandates for business associate contracts. Existing business associate contracts should be reviewed for compliance with the following changes brought by the Final Rule:

- Changes in the definition of "business associate" and the new definition of "subcontractor."
- The business associate must obtain satisfactory assurances that subcontractor(s) will appropriately safeguard PHI.

- The business associate contract must provide that the business associate will comply with applicable requirements of the Privacy and Security Rules.
- The business associate contract must provide that the business associate will ensure that any subcontractors that create, receive, maintain or transmit electronic PHI on behalf of the business associate agree to comply with the applicable requirements of HIPAA by entering into a business associate contract or other arrangement that complies with the Privacy and Security Rules.
- The business associate contract with a subcontractor must allow the business associate to terminate the contract if the business associate knows of a pattern of activity or practice of the subcontractor that constitutes a material breach of the subcontractor's obligations under the contract, and reasonable steps to cure the breach or end the violation are unsuccessful.
- The business associate contract must provide that the business associate will report to the covered entity any breach of unsecured protected health information as required by the Privacy Rule.
- The business associate contract must provide that any subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate agrees to the same restrictions and conditions that apply to the business associate with respect to that information.
- To the extent that the business associate is to carry out an obligation of the covered entity under HIPAA, the business associate agreement must require that the business associate comply with the requirements of HIPAA that apply to that obligation.
- HIPAA's requirements for business associate contracts between a covered entity and a business associate apply to a business associate contract between a business associate and a subcontractor.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Gerry Hinkley (bio)
San Francisco
+1.415.983.1135
gerry.hinkley@pillsburylaw.com

Allen Briskin (bio)
San Francisco
+1.415.983.1134
allen.briskin@pillsburylaw.com

Caitlin B. Bloom (bio)
San Francisco
+1.415.983.1023
caitlin.bloom@pillsburylaw.com