ReedSmith

Alert

Life Sciences Health Industry

If you have questions or would like additional information on the material covered in this Alert, please contact the author:

Brad M. Rostolsky
Partner, Philadelphia
+1 215 851 8195
brostolsky@reedsmith.com

Jennifer L. Pike
Associate, Washington, D.C.
+1 202 414 9218
jlpike@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

The HITECH Final Rule: Highlights of the Key Changes to HIPAA Privacy and Security

On January 25, 2013, and after more than a two-year wait after the release of the July 14, 2010, proposed regulations ("the Proposed Rule"),[1] the Office for Civil Rights of the U.S. Department of Health & Human Services ("HHS") published the long-awaited HITECH final rule (the "Final Rule").[2] The Final Rule serves as an omnibus rule, and in effect provides final regulations with regard to four distinct aspects of previously proposed rulemaking: (1) the Proposed Rule, (2) the 2009 (interim final) Breach Notification Rule, (3) the 2009 (interim final) Enforcement Rule, and (4) the 2009 Genetic Information Nondiscrimination Act. With limited exception, compliance with the Final Rule is required by September 23, 2013.

Key Compliance Dates

- General Compliance Date – Sept. 23, 2013
- Enforcement Rule Compliance Date – March 26, 2013
- BAA Grandfather Period – Through Sept. 22, 2014

Direct Regulation of Business Associates The Final Rule extends to business associates the requirement to comply directly with the Security Rule and significant aspects of the Privacy Rule. The Final Rule also significantly expands the definition of business associate with regard to which individuals and entities qualify as a business associate. Among other things, this expanded definition of business associate converts subcontractors of business associates that create, receive, maintain, or transmit protected health information ("PHI") on behalf of the business associate into business associates themselves. As a result, a business associate's subcontractors (and subcontractors of a subcontractor, all the way down the chain) will be regulated in the same manner as any other business associate. As of the Compliance Date, business associates and subcontractors will be directly liable for civil monetary penalties ("CMPs") for HIPAA infractions.

Key Changes to Privacy Rule Compliance

- *Business Associate Agreements ("BAAs").* The Final Rule made several changes to the BAA provisions that will require covered entities and business associates to update BAAs executed prior to the publication of the Final Rule. The purpose of these changes is to align the requirements for BAAs with requirements in the HITECH Act and elsewhere within the revised HIPAA regulations. While the general compliance date for the Final Rule is September 23, 2013, the Final Rule extends a significant grandfather period to BAAs that were in effect as of January 25, 2013 if (1) such agreements are in compliance with existing Privacy and Security Rules, and (2) are not renewed or modified from March 26, 2013, until September 23, 2013. Such BAAs are compliant until the earlier of the date of renewal/modification or September 22, 2014 (i.e., one year subsequent to the general compliance date).

- *Marketing and Sale of PHI.* The Final Rule imposes additional burdens on covered entities and business associates that sell PHI or utilize PHI in furtherance of marketing activities. The Final Rule expands the types of communications that meet the definition of marketing, such that, with limited exception, authorizations are required for all treatment and health care operations communications where the covered entity receives financial remuneration for making the communication from a third party whose products or services are being described. Subject to certain exceptions, the Final Rule prohibits the sale of PHI by a covered entity or business associate unless the covered entity or business associate obtains an authorization from the individual. Unlike the marketing provisions, which are triggered only by financial payments, "remuneration" as applied in the sale of PHI is not limited to financial payments and therefore is applicable to the receipt of in-kind as well as financial benefits.

- *Authorizations.* The Final Rule expands the circumstances for which an authorization from an individual must be obtained. An authorization must now be obtained for (1) the sale of PHI, (2) uses and disclosures of PHI for marketing purposes, and (3) most uses and disclosures of psychotherapy notes. At the same time, certain requirements governing authorizations for the use of disclosure of PHI for research purposes have been relaxed.

- *Notice of Privacy Practices ("NPP").* The Final Rule mandates the inclusion of several additional statements in a covered entity's NPP, which triggers a covered entity's obligation under the existing Privacy Rule to redistribute its revised NPP.

- *Individual Rights.* Under the Final Rule, individuals may now restrict the disclosure of their PHI to health plans where the disclosure is for payment or health care operations, and relates to health care services or items for which the individual paid in full out of pocket. Additionally, the Final Rule gives individuals the right to obtain an electronic copy of their PHI that is maintained in any electronic system.

Enforcement Rule The Final Rule adopts wholesale the modifications to the HIPAA Enforcement Rule set forth in the interim final enforcement rule ("IFR")[3] and Proposed Rule to incorporate the tiered CMP structure provided by the HITECH Act. The four CMP categories are:

1. Unknown violations (i.e., in which the person did not know, and by exercising due diligence, would not have known that a violation occurred) – Penalties of $100-$50,000 for each violation.

2. Violations due to reasonable cause and not to willful neglect – Penalties of $1,000-

$50,000 for each violation.

3. Violations due to willful neglect (and the violation has been corrected) – Penalties of $10,000-$50,000 for each violation.

4. Violations due to willful neglect (and has not been corrected) – Minimum penalty of $50,000 for each violation.

There is a maximum annual aggregate penalty of $1.5 million for all violations of the same requirement or prohibition under any of the four categories. Further, the IFR prohibited the imposition of penalties for any violation not involving willful neglect that is timely corrected.[4]

The Final Rule provides that HHS must now formally investigate a complaint or perform a compliance review if a preliminary investigation of the facts indicates a possible violation of HIPAA rules due to willful neglect. Moreover, with regard to willful neglect violations, HHS has the discretion to move directly to imposing a CMP without first exhausting informal resolution efforts.

Breach Notification The Final Rule replaces the interim final breach notification rule's risk of harm assessment with a four-pronged "more objective" test. The Final Rule requires covered entities and business associates to consider the following factors (along with any other relevant considerations) designed to "focus more objectively on the risk that PHI has been compromised," as compared with the interim final rule's focus on the significant risk to an individual caused by the impermissible use or disclosure:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or to whom it was disclosed
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

Essentially, impermissible uses or disclosures of PHI will be presumed to be a breach unless the covered entity or business associate demonstrates that there is a "low probability that the protected health information has been compromised."[5]

* * * *

With the Final Rule's delayed general compliance date, now is the time to review business relationships involving PHI, as well as the associated HIPAA policies and procedures.

For a more detailed analysis of the Final Rule, visit http://www.reedsmith.com/The-HITECH-Final-Rule--The-New-PrivacySecurity-Rules-of-the-Road-Have-Finally-Arrived-02-19-2013/.

1. 75 Fed. Reg 40868 (July 14, 2010).
2. 78 Fed. Reg. 5566 (January 25, 2013).
3. 74 Fed. Reg. 56123 (October 30, 2009).
4. 78 Fed. Reg. at 5577, 5586 (to be codified at 45 C.F.R. § 160.410(b)).
5. 78 Fed. Reg. at 5641.