Morgan Lewis

alert

FDA & Healthcare LawFlash

January 18, 2013

HHS Releases HIPAA/HITECH Omnibus Final Rule

Rule finalizes many provisions of the proposed rule, imposing new privacy and security obligations directly on business associates and modifying the definition of "breach" and the required factors to be considered in a risk assessment.

On January 17, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) released its much-anticipated and long-awaited omnibus final rule (Final Rule)[1] modifying certain aspects of the Privacy Rule, the Security Rule, and the Enforcement Rule under the Health Insurance Portability and Accountability Act (HIPAA) and the Breach Notification for Unsecured Protected Health Information Rule (Breach Notification Rule) under the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The Final Rule represents the most significant development in healthcare privacy law since the issuance of the final Privacy Rule and Security Rule a decade ago.

The Final Rule comes approximately two and a half years after HHS published its notice of proposed rulemaking (Proposed Rule) to implement provisions of the HITECH Act. The Final Rule takes effect on **March 26, 2013**, and covered entities and business associates are required to comply with the applicable requirements of the Final Rule by **September 23, 2013**. The Final Rule comprises modifications to the four individual rules described below.

HIPAA Privacy, Security, and Enforcement Rules

The Final Rule finalizes modifications to the HIPAA Privacy, Security, and Enforcement Rules, including, but not limited to, those mandated by the HITECH Act. For the most part, the Final Rule adopts the provisions of the Proposed Rule, with a host of clarifications but relatively few significant modifications. The Final Rule's notable provisions include the following:

- **Business Associates**: The Final Rule makes some of the obligations of the HIPAA Privacy and Security Rules directly applicable to business associates. It also includes "subcontractors" in the definition for "business associates," requiring business associates to enter into written contracts with subcontractors that are substantially similar to business associate agreements. Significantly, business associates and subcontractors will be required to come into full compliance with the Security Rule by the September 23 compliance date.
- **Marketing**: The Final Rule modifies the Proposed Rule's approach to marketing, requiring authorization for *all treatment and healthcare operations communications* where the covered entity receives financial remuneration for making the communications from a third party whose product or service is being marketed. HHS notes the difficulty in distinguishing between "treatment" and "health care operations" communications, as the Proposed Rule required, and therefore HHS will treat as marketing communications "all subsidized communications that market a health-related product or service." HHS clarifies that the term "financial remuneration" does not include nonfinancial benefits, but rather it only includes those payments made in exchange for making communications about a product or service.
- **Sale of Protected Health Information**: The Final Rule generally prohibits a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of protected health

1. View the January 17, 2013, HHS press release at http://www.hhs.gov/news/press/2013pres/01/20130117b.html.

information (PHI), unless the covered entity or business associate has obtained an authorization from the individual.

- **Access to Protected Health Information**: The Final Rule expands an individual's right to receive electronic copies of his or her PHI.
- **Restrictions on Certain Disclosures to Health Plans**: The Final Rule restricts disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.
- **Notice of Privacy Practices**: The Final Rule requires covered entities to modify certain elements of their notice of privacy practices and redistribute those revised forms.

Civil Money Penalty Structure

The Final Rule adopts the HITECH Act's tiered system of increasing penalty amounts for violations based on increasing levels of culpability associated with each tier.

Breach Notification Rule

The Final Rule modifies the definition of "breach" and the risk assessment approach set forth in the Breach Notification Interim Final Rule issued by HHS on August 24, 2009 (Interim Final Rule). Under the new definition of "breach," an impermissible use or disclosure of PHI is "presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised." This standard replaces the "significant risk of harm" standard set forth in the Interim Final Rule. HHS notes that the prior focus on "harm to an individual" was too subjective, risking inconsistent interpretations and results across covered entities and business associates. As stated above, HHS is instead requiring covered entities and business associates to demonstrate, through a risk assessment, that there is a "low probability" of the PHI having been "compromised."

The Final Rule also modifies the factors that covered entities and business associates must consider when performing a risk assessment with respect to a potential breach. HHS suggests that covered entities and business associates examine their policies to ensure that all required factors are considered when conducting a breach risk assessment.

GINA

The Final Rule modifies the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes.

Implications

Business associates should prepare for compliance with new HIPAA obligations on September 23, including implementation of a Security Rule compliance program. Covered entities should also begin conforming their HIPAA compliance programs to reflect the new requirements of the Final Rule, including updating and redistributing notices of privacy practices and amending business associate agreements.

Contacts

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis attorneys:

San Francisco

W. Reece Hirsch	415.442.1422	rhirsch@morganlewis.com
Heather Deixler	415.442.1317	hdeixler@morganlewis.com

Chicago

Andy R. Anderson	312.324.1177	aanderson@morganlewis.com

Saghi "Sage" Fattahian	312.324.1744	sfattahian@morganlewis.com
Philadelphia		
Georgina L. O'Hara	215.963.5188	go'hara@morganlewis.com
Pittsburgh		
Lauren B. Licastro	412.560.3383	llicastro@morganlewis.com

About Morgan, Lewis & Bockius LLP

With 24 offices across the United States, Europe, and Asia, Morgan Lewis provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. Our international team of lawyers, patent agents, benefits advisers, regulatory scientists, and other specialists—more than 1,600 legal professionals total—serves clients from locations in Almaty, Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Moscow, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.