

HHS Releases the Long-Awaited Final Omnibus HIPAA Rules

Gregory M. Fliszar • 215.665.7276 • gfliszar@cozen.com

William P. Conaboy, Jr. • 215.665.5580 • wconaboy@cozen.com

A pre-publication version of the much anticipated final Omnibus Health Insurance Portability and Accountability Act (HIPAA) rule (the Final Rule) was issued January 17, 2013 with publication in the Federal Register scheduled for January 25, 2013.

While the Final Rule becomes effective **March 26, 2013**, covered entities and business associates have until **September 23, 2013**, to comply and, in the case of existing business associate agreements, covered entities have until **September 2014** to make changes. The full breadth of the nearly 600-page rule will take some time to fully analyze.

As we continue to analyze the complex regulations, however, here are a few highlights:

- **Probably the most significant change in the Final Rule is a modification to the determination of what is a reportable breach.** The Final Rule removes the risk of significant harm standard, which, in the interim final rule, limited breach notification obligations to breaches that a covered entity determined to pose a significant, financial, reputational or other harm to individuals affected by the breach. The Final Rule replaced the risk of significant harm standard with the provision that “an impermissible use or disclosure of protected health information (“PHI”) is presumed to be a breach unless the covered entity or business associate ... demonstrates that there is a low probability that the PHI has been compromised.” In other words, the Final Rule now requires a covered entity to notify individuals about a breach *unless* it can demonstrate a low probability that PHI has been compromised. This presumption that all impermissible use of PHI is a breach is a significant departure from the risk of significant harm standard.

- **The Final Rule and Business Associates.** As required by the Health Information Technology and Clinical Health Act (HITECH), the Final Rule extends Privacy and Security compliance obligations to business associates, and it defines business associates to include subcontractors of business associates whose work involves protected health information. To the disappointment of many in the industry, there is no new model language for business associate agreements.
- **The Final Rule strengthens HIPAA enforcement.** As required by HITECH, the Final Rule increased civil monetary penalties and caps them at an annual \$1.5 million, up from \$25,000. (Note: in a previous Alert, [which can be found here](#), we illustrated OCR's enforcement ability under HITECH.)
- **The Privacy Rule is amended as mandated in the Genetic Information Nondiscrimination Act (GINA):** The Final Rule, as required in GINA, prevents covered entities from disclosing or otherwise using an individual's genetic information for underwriting purposes.

We will follow this alert with a more comprehensive review of these important and long-awaited HIPAA regulations. In the meantime, please feel free to contact the authors with any questions or concerns.

Atlanta • Charlotte • Cherry Hill • Chicago • Dallas • Denver • Harrisburg • Houston • London • Los Angeles • Miami
New York • Philadelphia • San Diego • Seattle • Toronto • Washington, D.C. • West Conshohocken • Wilkes-Barre • Wilmington