Final HIPAA privacy and security regulations released

The Department of Health and Human Services (HHS) released long-anticipated (and long-overdue) final omnibus regulations under the Health Insurance Portability and Accountability Act (HIPAA) on January 17, 2013. The rules update HIPAA’s privacy, security, enforcement, and breach notification requirements. While it will take some time to analyze the almost 600-page document, covered entities – including group health plans – should prepare for changes that will be necessary as a result of these rules. These changes will mean updates to HIPAA policies and procedures, business associate agreements, privacy notices, and workforce training. Covered entities generally must comply with the new rules by September 23, 2013.

In this article: Background | Omnibus regulation highlights | What’s next for employer plan sponsors?

Background

HIPAA’s administrative simplification rules have evolved since their initial release in 1996, and several rounds of government guidance have addressed how HIPAA protects an individual’s health information (PHI) including:

- The privacy and security rules, which became effective for most “covered entities” (health providers, health plans, and health data clearinghouses) in 2003 and 2005 respectively. These foundational rules provide the basic structure of how covered entities must protect PHI in all formats.

- The Health Information Technology for Economic and Clinical Health (HITECH) Act extended certain HIPAA provisions and penalties to covered entities’ business associates (e.g., third party administrators, contractors, subcontractors, and other vendors) directly, just as they apply to covered entities. The HITECH Act also added new breach notification requirements and individual privacy rights, and it strengthened enforcement with significantly increased penalties for HIPAA violations. (See our April 27, 2009 For Your Information.)

- The Genetic Information Nondiscrimination Act (GINA) imposed certain privacy requirements in connection with the use of genetic information. (See our October 15, 2009 For Your Information.)

- Proposed regulations published in 2011 on the accounting of disclosure rules would change the timeframes for providing an accounting of disclosures and allow individuals to receive a report showing who “accessed” their PHI. (See our July 8, 2011 For Your Information.)
Omnibus regulation highlights

The new omnibus regulations, generally requiring compliance by September 23, 2013, respond to public comments and finalize most of the prior guidance into one comprehensive set of rules, with modifications in certain areas. Some of the rules' highlights include:

- Finalizing business associates’ direct liability for HIPAA compliance. Business associate agreements will need to be updated to reflect this new liability. A special transition rule applies to valid business associate agreements in effect before January 25, 2013.
- Imposing additional limits on the use of PHI for marketing and fundraising purposes
- Prohibiting the sale of PHI without an individual’s permission (some exceptions apply)
- Making it easier to give permission to share a child’s immunization proof with a school
- Expanding individual rights
- Adopting the increased and tiered civil monetary penalties provided by the HITECH Act
- Changing the analysis for determining if a HIPAA breach must be reported
- Adopting the GINA standards prohibiting the use or disclosure of genetic information for underwriting purposes
- Expanding the ability for certain family members to access a decedent’s PHI

Notably, the omnibus rules do not appear to include 2011 proposed regulations on accounting of disclosures and an individual’s right to receive an access report.

What’s next for employer plan sponsors?

The omnibus regulations are detailed and affect a broad range of HIPAA issues. HHS has characterized these rules as “the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented.” As such, plan sponsors will need to review – and in most cases update – their HIPAA policies and procedures, business associate agreements, and privacy notices to confirm they meet the new mandates by September 23, 2013. Plan sponsors will also need to conduct workforce training to update individuals with access to PHI on the new rules. We will publish a detailed analysis of these regulations shortly.
Authors
Mary Harrison, JD
Tami Simon, JD

Produced by the Knowledge Resource Center of Buck Consultants at Xerox
The Knowledge Resource Center is responsible for national multi-practice compliance consulting, analysis and publications, government relations, research, surveys, training, and knowledge management. For more information, please contact your account executive or email fyi@xerox.com.

You are welcome to distribute FYI® publications in their entireties. To manage your subscriptions, or to sign up to receive our mailings, visit our Subscription Center.

This publication is for information only and does not constitute legal advice; consult with legal, tax and other advisors before applying this information to your specific situation.

©2014 Xerox Corporation and Buck Consultants, LLC. All rights reserved. Xerox® and Xerox Design® are trademarks of Xerox Corporation in the United States and/or other countries. Buck Consultants® is a registered trademark of Buck Consultants, LLC in the United States and/or other countries.