



© 2013 American Health Lawyers Association

February 1, 2013 Vol. XI Issue 4

Finally! HHS Office For Civil Rights Releases HIPAA Omnibus Rule With Sweeping Changes To Compliance Requirements And Enforcement

By Dianne J. Bourque, Kimberly J. Gold, and Stephanie D. Willis, Mintz Levin

The final regulations^[1] from the Department of Health and Human Services Office for Civil Rights (OCR) containing modifications to the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, Enforcement, and Breach Notification Rules (Omnibus Rule)^[2] have finally been released.^[3] But the challenging task of interpreting them has just begun for covered entities, business associates, and downstream entities of business associates, all of whom are significantly affected by the rule.

OCR Director Leon Rodriguez declared that the new provisions in the Omnibus Rule “not only greatly enhance a patient’s privacy rights and protections, but also strengthen the ability of [OCR] to vigorously enforce the HIPAA privacy and security protections.”^[4] The official press release announcing the Omnibus Rule confirms agency enforcement positions previously hinted at by HIPAA-related agency leaders, such as extending direct liability under HIPAA to business associates and subcontractors. The press release highlights other “sweeping changes” under the rule, including:

- streamlined authorization requirements for the use of individuals’ protected health information (PHI) for research purposes;
- new limits on permissible uses of information for marketing and fundraising purposes;
- prohibitions on the sale of individuals’ PHI without their permission; and
- increased penalties for noncompliance.

The Omnibus Rule also includes the following significant changes.

No Mercy for Business Associates:

- As expected, business associates now have direct liability under HIPAA and must comply with the Security Rule and certain provisions of the Privacy Rule. OCR did not provide business associates additional time to comply beyond the September 23, 2013 deadline applicable to covered entities, despite requests for additional time submitted during the public comment period.
- Business associate subcontractors (vendors of business associates) have identical compliance obligations, no matter how far removed or how “downstream” their services are from a covered entity.
- The business associate exception for “conduits” of PHI is limited to organizations that merely transmit PHI. Organizations that store PHI, such as cloud vendors, are considered business associates even if they do not access PHI. This analysis is important as cloud-based solutions become more widespread in the healthcare industry.
- Existing business associate agreements must be updated for compliance with the revisions in the Omnibus Rule, but organizations can continue to operate under certain existing contracts until September 23, 2014 (one year after the date required for compliance with the Omnibus Rule).

Dramatic Changes to Marketing Activity Requirements

The Omnibus Rule now requires that prior to sending any marketing materials to an individual relating to a product or service paid for by a third party, a covered entity sending the marketing must obtain the individual’s authorization to receive the communication. OCR removed the distinctions between authorization requirements for communications relating to treatment versus those for healthcare operations included in its proposed rule. As in the proposed rule, the final rule contains exceptions including subsidized face-to-face communications and subsidized communications regarding a drug or biologic currently being prescribed to an individual.

Breach Analysis Changes

The Omnibus Rule moves away from the “harm standard” provided in the proposed rules. Instead, a covered entity or business associate must overcome the presumption that the breach must be reported by performing a four-factor risk assessment to determine

whether or not PHI has been compromised. The new standard has the effect of eliminating a covered entity's discretion regarding whether or not a breach must be disclosed to affected individuals, the government, and potentially the media.

Family Access to Decedents' PHI

Family members of a decedent who were involved in the person's care prior to his or her death may now access the decedent's PHI.

This summary does not include revisions under the Genetic Information Nondiscrimination Act (GINA), also published in the Omnibus Rule.

Overall, the Omnibus Rule provides confirmation of OCR's strengthening enforcement position regarding security precautions that covered entities and business associates must implement to ensure patient privacy. The stakes are high for noncompliant parties, so the Omnibus Rule should grab the attention of multiple players in the healthcare industry who deal in the electronic exchange of patient data.

Dianne J. Bourque is a Member of Mintz Levin's Health Law Section in the firm's Boston office. She advises a variety of health care clients and other business entities on a broad range of health care issues, including the requirements of the HIPAA Privacy Rule and Security Standards, including new requirements under the HITECH provisions of the American Recovery and Reinvestment Act of 2009 (ARRA), and state-imposed medical privacy laws. She regularly assists clients with the implementation of HIPAA-mandated policies and procedures, privacy audits, third-party requests for information, and review of HIPAA-related contracts and forms. She has successfully defended clients in both civil and criminal HIPAA enforcement actions and regularly assists clients with the management of data breaches and other losses of protected health information. Recently, she was a featured co-presenter for the Mintz Levin webinar titled, "The New HIPAA Omnibus Rule & Your Liability."

Kimberly J. Gold is a Health Law associate in Mintz Levin's New York office. Her experience includes advising health care clients on HIPAA and state privacy laws and regulatory compliance. Her practice also focuses on corporate and transactional matters.

Kimberly is the Chair of the AHLA HIT Practice Group Emerging Uses Affinity Group. She frequently writes and speaks about privacy and security matters and was a featured co-presenter for the Mintz Levin webinar titled, “The New HIPAA Omnibus Rule & Your Liability.”

Stephanie D. Willis is a Health Law associate in Mintz Levin’s D.C. office. She primarily works with health care clients who seek to comply with state and federal laws and regulations governing licensure, reimbursement, health care fraud and abuse, telemedicine, and health information privacy requirements. She frequently writes about health care fraud and health information privacy enforcement matters and has co-authored articles for Law360 and Westlaw publications.

[1] HHS Office for Civil Rights, *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules*, 78 Fed. Reg. 5566 (Jan. 25, 2013), available at: <http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf>.

[2] These regulations were promulgated under the Health Information Technology for Economic and Clinical Health Act (HITECH).

[3] Proposed regulations were previously released for public comment: the October 30, 2009 interim final enforcement rule detailing HITECH’s then-new tiered penalty structure; and the August 24, 2009 interim final breach notification rule published pursuant to HITECH proposed privacy, security, and enforcement standards. The following chart provides a section-by-section comparison of how the regulatory provisions published on January 25, 2013 as part of the Omnibus Rule modify provisions of the proposed rules: <http://www.mintz.com/newsletter/2013/Advisories/2587-0113-NAT-HL/index.html>.

[4] Department of Health and Human Services, “New rule protects patient privacy, secures health information,” *News Release*, (Jan. 17, 2013), available at: <http://www.hhs.gov/news/press/2013pres/01/20130117b.html>.

© 2013 American Health Lawyers Association
1620 Eye Street NW
Washington, DC 20006-4010
Phone: 202-833-1100 Fax: 202-833-1105