Privacy & Security - HIPAA Compliance @ MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Privacy & Security HIPAA Compliance Alert

JANUARY 18, 2013

Finally! HHS Office of Civil Rights Releases HIPAA Omnibus Rule With Sweeping Changes to Compliance Requirements and Enforcement

BY DIANNE J. BOURQUE AND STEPHANIE D. WILLIS

The final regulations[1] from Department of Health and Human Services Office of Civil Rights (OCR) containing modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules (Omnibus Rule) have finally been released, but the hard work 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."[2] The official press release announcing the Omnibus Rule confirms agency enforcement positions previously hinted at by HIPAA-related agency leaders, such as extending liability under HIPAA to business associates and subcontractors. But additionally, the press release gives the following preview to the other "sweeping changes" under the rule, including:

- streamlined authorization requirements for the use of individuals' health information for research purposes;
- new limits on permissible uses of information for marketing and fundraising purposes; and
- prohibitions on the sale of individuals' health information without their permission.

Mintz Levin's initial impressions of the Omnibus Rule include the following:

- ***No Mercy for Business Associates:***
  - As expected, business associates now have direct liability under HIPAA and must comply with all of its security and certain privacy standards. OCR did not provide business associates additional time to comply, despite requests for time submitted during the public comment period.
  - Business associate subcontractors (vendors of business associates) have identical compliance obligations, no matter how removed or how "downstream" their services are from a covered entity.
  - Existing business associate agreements must be updated for compliance with the revisions in the Omnibus Rule, but they 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, the covered entity sending the communication must obtain individual authorization to

receive such communications. OCR removed the distinctions between authorization requirements for communications relating to treatment versus those for health care operations included in its proposed rule.

- ***Breach Analysis Changes:*** The Omnibus Rule requires a potential breaching party to perform a four-factor risk assessment to determine whether the breach must be reported, with the effect of significantly reducing 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' Personal Health Information (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.

Mintz Levin's Health Law Practice is actively preparing a variety of educational materials and resources for covered entities, business associates, and downstream entities affected by the Omnibus Rule. The first of these materials will be a chart comparing the differences between the proposed and final rules to be published early next week.

* * *

View Mintz Levin's Privacy & Security HIPAA Compliance attorneys.

View Mintz Levin's Health Law attorneys.

Read and subscribe to *Health Law & Policy Matters* blog.

Endnotes

[1] HHS Office of 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" (to be published Jan. 25, 2013), available at: http://www.ofr.gov/OFRUpload/OFRData/2013-01073_PI.pdf.

[2] Dept. 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.

2580-0113-NAT-HL