September 2013

HIPAA Omnibus Final Rule

Enforcement Action Following September 23 Compliance Deadline

As of September 23, 2013, Covered Entities and Business Associates are expected to be in compliance with the Omnibus Final Rule that amended the Health Insurance Portability and Accountability Act of 1996 and accompanying regulations (the statute and regulations together, HIPAA) (the Final Rule), which codified changes to the Enforcement Rule[1] enacted as part of the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). To assist in its efforts to enforce HIPAA and respond to patient complaints of noncompliance, the Office for Civil Rights (OCR), a subagency of the U.S. Department of Health and Human Services (HHS), is empowered to assess tiered penalties tied to corresponding levels of culpability and prescribed to initiate mandatory investigations or compliance audits in instances of willful neglect. In addition to the revised enforcement role of the OCR, there were several modifications made to the affirmative defenses available to Covered Entities and Business Associates under the Final Rule.

Mandatory Action for Willful Neglect

The Final Rule requires the Secretary of HHS (the Secretary) to launch an investigation where a preliminary review of the facts in a complaint filed with its office indicates a possible HIPAA violation due to willful neglect. Similarly, the Secretary must initiate a compliance review where a preliminary review of information received other than through a complaint (such as a media report or communications from a state agency) indicates a HIPAA violation due to willful neglect of a Covered Entity or Business Associate. The Secretary retains continued discretion to investigate all other complaints or initiate compliance reviews. The preamble to the Final Rule suggests that the threshold for mandatory action is the mere possibility, not probability, that a willful violation has occurred based on a preliminary review of the facts. HHS has not provided meaningful guidance regarding such threshold despite commenters' requests for such guidance.

Correspondingly, the Secretary now has discretion to initially attempt to resolve HIPAA violations through informal means. This obligation was previously mandatory, but the preamble to the Final Rule explains that this provision had to be discretionary in order to support the Secretary's mandatory actions described above. Effectively, the Secretary now has discretion to directly impose a civil monetary penalty without exhausting informal resolution avenues, regardless of the level of culpability implicated by a preliminary review of the facts.

Tiered Penalties

Under the revised enforcement regime, violations of HIPAA are assessed by level of culpability of the Covered Entity or Business Associate and penalized by a corresponding civil monetary penalty. The chart below indicates the level of culpability, its definition and the dollar range of civil monetary penalty that the Secretary may impose.

[1] 45 C.F.R. part 160, subparts C and D.

Culpability Level of Covered Entity/Business Associate	Civil Monetary Penalty Amount	Calendar-Year Identical Violation Limit
Did Not Know and Would Not Have Known by Exercising Reasonable Diligence Reasonable diligence is the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances	$100–$50,000 per violation	$1,500,000 aggregate
Reasonable Cause Arises when an act or omission in which a Covered Entity/Business Associate knew, or by exercising reasonable diligence would have known, of the violation, but it did not act with willful neglect	$1,000–$50,000	$1,500,000
Willful Neglect—Corrected Within 30 Days Instances of willful neglect (defined below) where the violation was corrected within 30 days of the date the Covered Entity/Business Associate knew, or by exercising reasonable diligence (defined above) would have known, that the violation occurred	$10,000–$50,000	$1,500,000
Willful Neglect—Uncorrected Conscious, intentional failure or reckless indifference to the obligations to comply and the violation goes uncorrected	$50,000	$1,500,000

Determining Number of Violations and Civil Monetary Penalty Amount

The Enforcement Rule grants the Secretary wide discretion in assessing civil monetary penalties, including the authority to waive the imposition of a penalty altogether. The number of violations will be determined on a case-by-case basis, but for purposes of the calendar-year limit, the preamble provided several illustrative examples. A breach of unsecured protected health information (PHI) would likely be assessed by the number of individuals affected. Thus, a breach of one 100 persons' PHI would constitute 100 identical violations, and the aggregate penalty imposed would be subject to the $1,500,000 calendar-year limit. Similarly, violations for a failure to maintain adequate safeguards would be calculated by the number of days the safeguards were not in place. However, a breach of 100 persons' PHI due to a failure to maintain adequate safeguards for 10 days would be treated as 100 identical violations for breach, and 10 identical violations for failure to maintain adequate safeguards, each of which would be subject to the $1,500,000 calendar-year limit. Ultimately, a Covered Entity or Business Associate could still be fined more than $1,500,000 in any calendar year because a single incident could be the result of identical violations of several different provisions of HIPAA, each subject to the calendar-year limit.

In determining the amount of civil monetary penalty, the Secretary will consider the following factors: (i) the nature and extent of the violation; (ii) the nature and extent of the harm resulting from the violation; (iii) the history of prior compliance with the administrative simplification provisions, including violations; (iv) the financial condition of the Covered Entity or Business Associate; and (v) such other matters as justice may require.

Affirmative Defenses

Covered Entities' and Business Associates' primary mechanism for defending against the imposition of civil monetary penalties are the affirmative defenses set forth in the regulations. The Final Rule amends these in several notable respects. For violations after February 18, 2011, Covered Entities and Business Associates must demonstrate that a criminal penalty has actually been imposed in order to bar civil monetary penalties. Previously, and still effective for violations prior to February 18, 2011, the Covered Entity or Business Associate needed only to show that the subject violation was criminally "punishable." Further, for violations after February 18, 2009, the Secretary is barred from imposing a civil monetary penalty where the Covered Entity or Business Associate corrects the violation within 30

days of the first date it knew or should have known by exercising reasonable diligence that the violation occurred, absent circumstances of willful neglect.

Disclosure of PHI

In addition to its own enforcement action, the HITECH Act and the Final Rule include provisions to increase coordination among enforcement agencies. Specifically, the Final Rule addresses the ability of the Secretary to disclose the pertinent facts, including PHI protected by HIPAA, to other state and federal agencies. PHI (as defined under HIPAA) that is obtained by the Secretary during an investigation or compliance review is explicitly authorized to be disclosed to other state or federal agencies. Namely, the Secretary may share such information with (i) states' Attorneys General to pursue civil enforcement actions under HIPAA and state privacy laws on behalf of state residents; (ii) the Department of Justice to pursue criminal HIPAA penalties; or (iii) the Federal Trade Commission for purposes of pursuing remedies under consumer protection laws. Covered Entities and Business Associates should be aware that this express permission to disclose PHI in conjunction with the results of compliance reviews and audits could lead to greater exposure and liability for HIPAA violations, depending on the relevant factual circumstances.

Further Information

If you have questions or need further information about the Final Rule or compliance with HIPAA, do not hesitate to contact a member of the Vedder Price HIPAA Task Force or any other Vedder Price attorney with whom you work.

Vedder Price HIPAA Task Force

Health Care

Kathryn L. Stevens .....+1 (312) 609 7803
Michael A. Chabraja .....+1 (312) 609 7790
N. Paul Coyle.....+1 (312) 609 7775
Michael E. Reed .....+1 (312) 609 7640
Richard H. Sanders .....+1 (312) 609 7644
Erin K. L. Norby .....+1 (312) 609 7515
Caitlin C. Podbielski.....+1 (312) 609 7673
Gregory G. Wrobel .....+1 (312) 609 7722

Data Privacy & Security

Bruce A. Radke.....+1 (312) 609 7689
Michael J. Waters .....+1 (312) 609 7726

Employee Benefits

Christopher T. Collins .....+1 (312) 609 7706
Paul F. Russell.....+1 (312) 609 7740
Kelly A. Starr.....+1 (312) 609 7768
Benjamin A. Hartsock .....+1 (312) 609 7922

About Vedder Price

Vedder Price is a thriving general-practice law firm with a proud tradition of maintaining long-term relationships with our clients, many of whom have been with us since our founding in 1952. With approximately 300 attorneys and growing, we serve clients of all sizes and in virtually all industries from our offices in Chicago, New York, Washington, DC, London and San Francisco.

Chicago
222 North LaSalle Street
Chicago, IL 60601
T: +1 (312) 609 7500
F: +1 (312) 609 5005

New York
1633 Broadway, 47th Floor
New York, NY 10019
T: +1 (212) 407 7700
F: +1 (212) 407 7799

Washington, DC
1401 I Street NW, Suite 1100
Washington, DC 20005
T: +1 (202) 312 3320
F: +1 (202) 312 3322

London
4 Coleman Street
London EC2R 5AR
T: +44 (0)20 3667 2900
F: +44 (0)20 3667 2901

San Francisco
275 Battery Street, Suite 2464
San Francisco, CA 94111
T: +1 (415) 749 9500
F: +1 (415) 749 9502