

Presented:
The University of Texas School of Law
26th Annual Health Law Conference
April 10, 2014,
Houston, TX

Anatomy of a Health Care Data Breach: Reporting, Investigation and Enforcement

Kristen Rosati

Author contact information:
Kristen Rosati
Polsinelli PC
Phoenix, Arizona

krosati@polsinelli.com
602-650-2003

**Anatomy of a Health Care Data Breach:
Reporting, Investigation and Enforcement¹**

Kristen Rosati, J.D.

Polsinelli PC

krosati@polsinelli.com

602-650-2003

When the Health Insurance Portability and Accountability Act of 1996 (HIPAA)² Privacy Rule initially hit the scene at the end of 2000,³ health care organizations scrambled to get a huge number of policies and business associate contracts in place, train their employees, and set up compliance mechanisms for tracking and responding to potential HIPAA violations. Many health care organizations found compliance challenging because the HIPAA Privacy Rule touched on every aspect of their operations. HIPAA compliance eventually settled down to a dull roar as HIPAA became simply one of a panoply of federal and state regulatory requirements.

However, with new HIPAA breach reporting obligations and enforcement initiatives, HIPAA compliance is once again a major concern worthy of the commitment of institutional resources to ensure compliance. This paper covers the final regulations concerning reporting HIPAA violations to patients, Department of Health and Human Services (HHS) and the media, and HHS enforcement authority.

Breach Reporting under the HITECH Act

One of the most substantial changes required by the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009,⁴ was the requirement to affirmatively report certain HIPAA violations to individuals, the HHS Office for Civil Rights (OCR), and sometimes the media. This self-reporting requirement triggered an avalanche of breach reporting and subsequent investigations by OCR. According to OCR's Annual Report to Congress on Breaches of Unsecured Protected Health Information (for Calendar Years 2009 and 2010), OCR received approximately 253 reports of large breaches (breaches involving more than 500 individuals) and

¹ This paper consists of excerpts from *HIPAA: Once Again a Major Compliance Concern*. Reproduced with permission of Bloomberg BNA, Health Law Resource Center, *Health Care Program Compliance Guide*. Copyright 2014 by The Bureau of National Affairs, Inc. Ms. Rosati acknowledges her co-authors, Lisa Acevedo, Esq., Erin Fleming Dunlap, Esq., Rebecca Frigy, Esq., and Brett Heger, Esq., all of Polsinelli PC.

² Pub. L. No. 104-191.

³ See 65 Fed. Reg. 82462 (Dec. 28, 2000), *codified at* 45 C.F.R. Part 160, Part 164, Subpart E.

⁴ Pub. L. No. 111-5.

over 30,000 reports of small breaches (breaches involving less than 500 individuals) between September 23, 2009 and December 31, 2010.⁵

OCR has a website on which it displays all breaches involving 500 or more individuals—the so-called “HIPAA Wall of Shame.”⁶ Over the last three years, OCR has announced a number of breach settlements – many in excess of \$1.5 million. In January 2013, OCR announced its first HIPAA breach settlement involving less than 500 individuals. The message from OCR continues to be -- regardless of size, covered entities must take action and will be held accountable for safeguarding their patients’ health information. There is no question potential reportable breaches deserve prompt and careful attention.

The HITECH Act created a new federal breach reporting requirement for HIPAA covered entities and their business associates.⁷ The Act requires a covered entity that “accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information” to “notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.” Business associates are required to notify covered entities of breaches by the business associate.⁸

In August 2009, OCR published interim final regulations implementing the HITECH Act breach reporting requirements.⁹ These regulations (referred to as the “Interim Final Rule”), and the Preamble to those regulations, provided detail on what constitutes “unsecured PHI” and what is a “breach” and provided additional guidance on how to determine whether, to whom and when to report.

In January 2013, OCR published the long-awaited Final Rule,¹⁰ which made a few changes to the breach reporting requirements from the Interim Final Rule. Most significantly, the Final Rule altered the definition of “breach” and reshaped how covered entities and business associates must evaluate their breach notification obligations. The Final Rule became effective on March 26, 2013, and compliance with the Final Rule’s changes to the breach reporting requirements was required by September 23, 2013.

Definition of “Unsecured” PHI

Section 13402(h) of the Act defined the term “unsecured PHI” as PHI that is not secured through the use of a technology or methodology that renders PHI “unusable, unreadable, or

⁵ See OCR, “Report to Congress on Breach Notification Program,” available on the HHS website at <http://www.hhs.gov/ocr/privacy/index.html>.

⁶ See OCR, “Breaches Affecting 500 or More Individuals,” available on the HHS website at <http://www.hhs.gov/ocr/privacy/index.html>.

⁷ HITECH Act § 13402 [42 U.S.C. § 17932.

⁸ *Id.*

⁹ 74 Fed. Reg. 42740 (Aug. 24, 2009) (45 C.F.R. Part 164, Subpart D)

¹⁰ 78 Fed. Reg. 5566 (Jan. 25, 2013) (called the “Final Rule” throughout this paper).