UT LAW CLE | THE UNIVERSITY OF TEXAS SCHOOL OF LAW

**PRESENTED AT**

2016 Essential Cybersecurity Law

August 19, 2016
Austin, Texas

# HIPAA Breach Reporting

**Kristen B. Rosati**

# HIPAA Breach Reporting[1]

Kristen Rosati
Coppersmith Brockelman PLC

The Health Information Technology for Economic and Clinical Health Information Act (the HITECH Act)[2] brought a sea change in enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[3] In addition to giving the Department of Health and Human Services (HHS), Office for Civil Rights (OCR), sharper teeth by increasing the penalties available, the HITECH Act also required OCR to implement a Breach Notification Rule requiring health care providers, health plans, and other entities covered by HIPAA to notify OCR and individuals when protected health information (PHI) is compromised.

Before the enactment of the HITECH Act and the implementation of the Breach Notification Rule, OCR's enforcement activities focused on providing covered entities with technical assistance, rather than requiring formal settlements or imposing civil monetary penalties. In fact, the first significant penalty was not imposed until 2009, nearly six years after Privacy Rule and four years after Security Rule became effective.[4] Post-HITECH, the pace of enforcement increased substantially. To date, penalties for HIPAA violations up to $4.8 million.[5]

Because OCR's enforcement actions predominately derive from self-reported breach incidents,[6] covered entities and business associates should pay close attention to their breach reporting policies and processes. This paper provides guidance on determining if a breach is reportable; notifying individuals, OCR, and the media of breaches; and getting ready for an OCR investigation.

## I. DETERMINING WHETHER THERE IS A REPORTABLE BREACH INCIDENT

In August 2009, OCR issued an Interim Final Rule (IFR) to implement the provisions of the HITECH Act requiring covered entities to self-report breach incidents to the Secretary of HHS.[7] The IFR defined a "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted [by the Privacy Rule] which compromises the

---

[1] Some of this content was included in *2015 Health Law and Compliance Update*, and is republished with permission from the publisher, Wolters Kluwer.
[2] The Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5.
[3] The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, enacted August 21, 1996.
[4] *See* OCR, "CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case," available on the HHS website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresolutionagreement.html.
[5] *See* OCR, "Case Examples and Resolution Agreements" available on the HHS website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.
[6] *Id.*
[7] 74 Fed. Reg. 42,740 (Aug. 24, 2009), *adding* 45 C.F.R. Part 164, Subpart D.

security or privacy of the protected health information."[8] Furthermore, the IFR provided that "compromises the security or privacy of the protected health information" meant a breach that posed a significant risk of financial, reputational, or other harm to the individual.[9]

In January 2013, OCR published the Omnibus Final Rule (the Final Rule).[10] The Final Rule significantly modified the analysis of when an impermissible use or disclosure constitutes a reportable breach. In contrast to the IFR, the Final Rule no longer defined what it means to "compromise" the security of privacy of PHI.

When a potential breach incident occurs, a covered entity or business associate should determine: (i) whether there was an impermissible acquisition, access, use, or disclosure of PHI; (ii) whether an exception to the definition of breach applies; and (iii) whether the incident involved PHI that has been rendered "secured" [11] such that the incident falls within the scope of the safe harbor. If no exceptions apply and the PHI was not "secured," an unauthorized use or disclosure is "presumed to be a breach," unless the entity can demonstrate that there is a "low probability that the PHI has been compromised."[12]

### A. Exceptions to the Definition of Breach

One of the first steps covered entities or business associates should take after discovering a potential breach incident is to analyze whether or not an exception to the definition of breach applies. The Final Rule excluded three types of uses or disclosures of PHI from the definition of breach:

1. The unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if made in good faith and within the scope of authority, and it does not result in any further impermissible use or disclosure;

2. An inadvertent disclosure of PHI by an authorized person to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement, and it does not result in any further impermissible use or disclosure; and

3. Disclosures of PHI where the entity has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.[13]

---

[8] 74 Fed. Reg. at 42,745 (Aug. 24, 2009).
[9] *Id.*
[10] 78 Fed. Reg. 5,566 (Jan. 25, 2013).
[11] *See* OCR, "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," available on the HHS website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html (referred to as "OCR Guidance to Render PHI Unusable, Unreadable, or Indecipherable"); 74 Fed. Reg. 19,006 (Apr. 27, 2009).
[12] 45 C.F.R. § 164.402(1)(iii).
[13] 45 C.F.R. § 164.402(1)(iii).

# Title search: HIPAA Breach Reporting

Also available as part of the eCourse
HIPAA Data Breach Reporting

First appeared as part of the conference materials for the
2016 Essential Cybersecurity Law session
"HIPAA Breach Reporting"