

## Healthcare

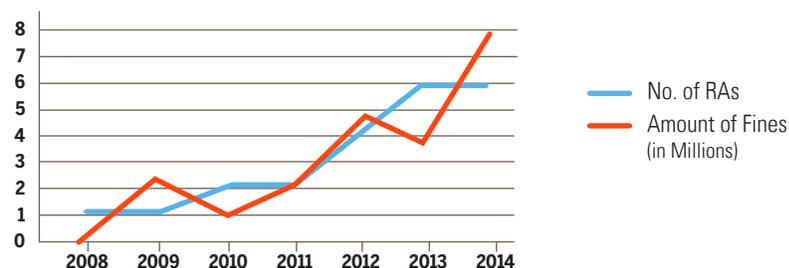
# Healthcare Data Breach Enforcements and Fines At A Glance

The Department of Health and Human Services' ("HHS") Office for Civil Rights ("OCR") is responsible for enforcing the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Enforcement of the Privacy Rule began on April 14, 2003, while enforcement of the Security Rule began on April 20, 2005. Furthermore, covered entities were required to comply with the HIPAA Breach Notification Rule beginning on September 23, 2009.<sup>1</sup>

The OCR relies on complaints filed by third parties, self-reports of data breaches, and media reports to identify targets for compliance reviews. If a covered entity is found to have committed serious violations during a compliance review, HHS may require the entity to enter into a "Resolution Agreement" ("RA") that may include a fine and a corrective action plan.



### Trends in Enforcement Activities and Fines



### What to consider when assessing the impact of an OCR investigation:

- ✓ There is an upward trend in enforcement activities and fines.
- ✓ Only a minority of investigations lead to fines and penalties.
- ✓ Cooperation in government-initiated compliance reviews is key to reducing the risk of a penalty.
- ✓ Preventing unauthorized access to patient information on stolen laptops and portable electronic devices by encrypting the information will reduce exposure.
- ✓ Less than 25 companies have received fines or penalties from OCR.
- ✓ Passwords should be enforced on laptops and other types of portable media.

Bryan Cave's Healthcare Team and Global Data Privacy and Security Team can help you devise a data security program that is compliant with HIPAA, and implement measures to mitigate the risk and damages resulting from a breach.

#### David A. Zetonyy

Partner

david.zetonyy@bryancave.com

#### Darryl Landahl

Partner

darryl.landahl@bryancave.com

#### Pou-I "Bonnie" Lee

Associate

bonnie.lee@bryancave.com

#### Frank Fabiani

Law Clerk

frank.fabiani@bryancave.com

**BRYAN CAVE**

<sup>1</sup> The HIPAA Breach Notification Rule requires covered entities and their business associates to notify the HHS Secretary, individuals, and in some cases, provide notice in media, regarding breaches of unsecured protected health information.

<sup>2</sup> <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/> (last reviewed March 2015)

<sup>3</sup> <http://www.hhs.gov/news/press/2014pres/05/20140507b.html> (last reviewed March 2015)