POLSINELLI

in the news

Health Care

July 2014

# **It's No Surprise**: Health Care Data Breaches Are on the Rise and So Is Government Enforcement

## In this Issue:



Pursuant to Congressional mandate, the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), the agency charged with enforcing the Health Insurance Portability and Accountability Act (HIPAA), recently issued its Annual Report to Congress on Breaches of Unsecured Protected Health Information (Breach Report) and its Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance (Compliance Report) for calendar years 2011 and 2012.

Although the information contained in these reports may seem dated (as a lot of HIPAA activity occurred in 2013 and the first half of this year, including the passage of the long-awaited HIPAA Final Rule and several highly-publicized enforcement actions), the reports do provide some helpful insight into risk areas and government enforcement efforts. The reports also serve as yet another reminder to covered entities and business associates to examine their compliance efforts and determine if additional compliance measures are necessary.

The Breach Report (accessible here) provides detail on the number and nature of breaches that occurred in calendar years 2011 and 2012. Key points include:

- Theft and loss of protected health information (PHI) were the primary causes of breaches affecting 500 or more individuals. In 2011, 50 percent of these breaches involved a theft, and 17 percent involved a loss. In 2012, these numbers changed to 53 percent and 12 percent, respectively.

- The largest breach in 2011 involved the loss of back-up tapes by a business associate and affected 4.9 million individuals. In 2012, the largest breach derived from a hacking/IT incident of an unencrypted server containing the PHI of 780,000 individuals.

- The most common cause of breaches involving less than 500 individuals was unauthorized access or disclosure (84 percent in 2011 and 74 percent in 2012).

- Although electronic PHI (ePHI) is the source of most large breaches, paper records were still a significant source of breaches (27 percent in 2011 and 23 percent in 2012).

- The improper disposal of PHI continued to be an issue, although slight (3 percent in 2011 and 4 percent in 2012).

- In calendar years 2011 and 2012, OCR entered into resolution agreements with seven covered entities in response to breach reports submitted to the agency. Four of the seven cases involved the theft of laptops or other electronic devices. Those resolution agreements (which are contracts signed by HHS and the entity) total more than $8 million in settlements and include stringent corrective actions plans (CAPs). [Author's Note: According to HHS' website (accessible here) as of the date of this publication, HHS has entered into 21 resolution agreements since 2008 (five of the 21 were in the first half of this year)].

The Compliance Report (accessible here) provides details on OCR's past enforcement efforts and the direction the agency intends to take in the future. Key points include:

- Of the 77,190 complaints received by OCR from April 2003 to December of 2012, 91 percent were resolved informally and only one case resulted in the imposition of a civil monetary penalty (CMP)—though many resulted in resolution agreements, as described above.

- OCR closed a number of cases after investigation because it determined that the corrective action taken by the organization appropriately addressed the underlying cause of the breach so as to avoid future incidents and mitigated potential harm to affected individuals.

- In 2011, OCR imposed its first CMP of $4.3 million on a covered entity for violating the HIPAA Rules. The penalty was based on the provider's failure (i) to provide patients with copies of their medical records; (ii) to comply with OCR's demand to produce the records; and (iii) to cooperate with OCR's investigation. OCR found the entity's failure to cooperate was due to willful neglect.

- The resolution agreements highlighted in the Compliance Report include settlements ranging from $100,000 to $1 million. In addition to monetary settlements, OCR required covered entities to implement CAPs, requiring the covered entities: (i) to engage in internal monitoring; (ii) to issue regular reports to OCR (generally for a period of three years); (iii) to implement new HIPAA policies and procedures; (iv) to train employees on the importance of the new HIPAA policies and procedures; (v) to conduct a risk analysis; and (vi) to identify a security official.

- The Health Information Technology for Economic and Clinical Health (HITECH) Act requires OCR to conduct periodic audits of covered entities and business associates. OCR initiated the audit pilot phase in November 2011 but is still in the process of fully implementing the audit program. The findings from the audit pilot program indicated that the majority of the entities audited (especially smaller entities) showed deficiencies in security compliance.

- For future enforcement, OCR plans to continue to review all of the cases and complaints, but to "work smarter" to resolve smaller issues quicker and focus more time and effort on issues pervasive in the health care industry. The agency will focus on "high-impact" cases, much like the seven cases requiring resolution agreements in 2011 and

2012. OCR will also update its audit protocol in accordance with the HIPAA Final Rule (published January 25, 2013) and publish the updates on its website. Lastly, OCR will engage in an extensive outreach program to educate covered entities and business associates on the HIPAA Rules.

## The Take-Aways for Covered Entities and Business Associates

- As a majority of the breaches occurring in 2011 and 2012 involved the loss or theft of PHI, covered entities and business associates must take steps to ensure PHI, especially ePHI, is truly protected. Encrypting data is the best way to prevent these types of breaches (e.g., encrypting all ePHI used or viewed on a laptop, via a portable storage drive [such as a flash drive], or viewed off the entity's server). It is also important to educate (and re-educate) employees on how to protect, and the importance of protecting, PHI (e.g., not leaving PHI unattended).
- Look at the CAPs (which are appendices to the resolution agreements reported on OCR's website) for guidance on ways to stay compliant with the HIPAA Rules. If you proactively review your organization's training programs, risk management plans and HIPAA policies and procedures, you may catch a compliance issue before it results in a HIPAA violation (and possibly an investigation by OCR).
- If your organization has a breach, take appropriate corrective action to address the underlying cause of the breach and mitigate any potential harm to affected individuals (e.g., notify individuals immediately by phone and offer credit monitoring if there is a risk of identity theft). OCR wants to see that organizations are appropriately responding to breaches and protecting patients.
- OCR's implementation of the audit program increases the chance that OCR may come knocking on your organization's door. OCR reported that a majority of the entities that were audited had deficiencies under all of the HIPAA Rules. Entities who are proactively analyzing their HIPAA compliance programs against the audit protocol (which should soon be updated to reflect the HIPAA Final Rule) will be better prepared if selected for an OCR audit—or, worse, targeted for an investigation.
- The only CMP imposed thus far was due to a failure to cooperate with OCR, which rose to the level of willful neglect. Covered entities and business associates stand much to gain for diligent cooperation with any investigation or audit.

## For More Information

If you have questions regarding this alert, please contact:


- Erin Fleming Dunlap | 314.622.6661 | edunlap@polsinelli.com
- Kathleen D. Kenney | 312.463.6380 | kdkenney@polsinelli.com


**To contact another member of our Health Care team,** click here or visit our website at www.polsinelli.com > Services > Health Care Services > Related Professionals.

**To learn more about our Health Care practice,** click here or visit our website at www.polsinelli.com > Services > Health Care Services.

## About Polsinelli's Health Care Practice

The Health Care practice comprises one of the largest concentrations of health care attorneys and professionals in the nation. From the strength of its national platform, the firm offers clients a depth of resources that cannot be matched in their dedication to and understanding of the full range of hospital-physician lifecycle and business issues confronting health care providers across the United States.

Recognized as a leader in health care law, Polsinelli is ranked no. 2 by The American Health Lawyers Association and no. 3 by *Modern Healthcare.* Polsinelli's highly trained attorneys work as a fully integrated practice to seamlessly partner with clients on the full gamut of issues. The firm's diverse mix of seasoned attorneys, well known in the health care industry, along with young lawyers with outstanding law school credentials, enables our team to provide counsel that aligns legal strategies with our clients' unique business objectives.

## About Polsinelli

*real challenges. real answers.*[SM]

Polsinelli is a first generation Am Law 100 firm serving corporations, institutions, entrepreneurs and individuals nationally. Our attorneys successfully build enduring client relationships by providing practical legal counsel infused with business insight, and with a passion for assisting General Counsel and CEOs in achieving their objectives. Polsinelli is ranked 18th in number of U.S. partners* and has more than 740 attorneys in 19 offices. Profiled by *The American Lawyer* and ranked as the fastest growing U.S. law firm over a six-year period**, the firm focuses on healthcare, financial services, real estate, life sciences and technology, energy and business litigation, and has depth of experience in 100 service areas and 70 industries. The firm can be found online at www.polsinelli.com. Polsinelli PC. In California, Polsinelli LLP.

* Law360, March 2014
** The American Lawyer 2013 and 2014 reports

## About this Publication

*Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. The choice of a lawyer is an important decision and should not be based solely upon advertisements.*

*Polsinelli PC. In California, Polsinelli LLP.*

POLSINELLI

real challenges. real answers. SM