Published on *The National Law Review* https://natlawreview.com

Five Lessons from Office of Civil Rights (OCR's) Reports to Congress on Breaches and HIPAA Rules Compliance

Article By:

Dianne J. Bourque

Last week, the **HHS Office of Civil Rights** (OCR) released two reports required by the **Health Information Technology for Economic and Clinical Health** (HITECH) Act: (i) the Annual Report to Congress on Breaches of Unsecured Protected Information (Breach Report); and (ii) the Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance (Compliance Report). In reviewing the Breach and Compliance Reports, Chief Information Officers, compliance and privacy officers, and information security professionals in the health care field should note five key lessons:

1) Know Where Your Organization's Protected Health Information (PHI) is Primarily Stored and Invest in the Right Protection

The statistics in both reports clearly show that the most breaches still come from "older" sources of PHI, such as paper records, desktop computers, and network servers. The Breach Report states that 225 out of the 458 total reports of breaches (or 49%) affecting 500 or more individuals involved these PHI sources in 2011 and 2012. In fact, the largest breach occurring in the two-year period covered by the Breach Report involved a TRICARE contractor's loss of back-up tapes that affected a total of approximately 4.9 million individuals.

In addition to updating and monitoring security protocols for older PHI sources, covered entities should address security problems with newer storage media. For instance, the Breach Report documents a large jump in the number of breaches involving laptop computers with a corresponding increase in affected individuals between 2011 and 2012: from 48 reports affecting 437,770 individuals in 2011 to 60 reports affecting 654,158 individuals. Because theft was the primary cause of breaches in 2009-2012, ensuring that laptops and other portable electronic devices are secured in accordance with standards acceptable under HIPAA will become even more important as organizations adopt more "bring your own device" policies to ensure the mobility and convenience of health care delivery.

2) Closely Monitor Your Business Associate Relationships

The Breach Report shows that although business associates were the culpable party for 118 out of the 458 breaches (or 26%) covered during the Breach Report's two-year reporting period, the individuals affected by the business associates' acts numbered over 8.7 million individuals, which

equals 59.3% of the total number of individuals affected by all of the breaches reported in 2011 and 2012. (We do note that the PHI of 4.9 million of these individuals' was compromised due to the TRICARE contractor breach described above). The large number of affected individuals in breaches involving business associates likely reflects the reality that business associates may house PHI for multiple covered entities.

Based on these statistics, health care organizations must impose standards for using business associates and subcontractors. In addition, covered entities must ensure that business associates and subcontractors understand their obligations under the HIPAA Privacy and Security Rules, especially because the Omnibus Rule released in 2013 (which we summarize here) now makes it clear that they are subject to the HIPAA Security Rule, other HIPAA compliance obligations and OCR's enforcement authority.

3) Don't Underestimate the Effect of "Small Breaches"

OCR imposed its first Resolution Agreement for a small breach involving less than 500 affected individuals in December 2012 against the Hospice of North Idaho (HONI), which we profiled in a previous blog post. Although HONI's small breach involved the theft of a laptop, the Breach Report notes that based on data it reviewed for all breaches disclosed in the reporting period, "[s]everal incidents [of small breaches] reported for 2011 and 2012 involved misdirected communications."

The problem with small breaches for organizations is that they can occur more frequently than large ones. The occurrence of repeated small breaches can be indicative of a systemic compliance problem, and may suggest to a regulator that the organization has not taken steps to identify or remedy the problem. As we profiled in another blog post, the OCR, in collaboration with the HHS Office of the National Coordinator and the HHS Office of General Counsel recently released the Security Risk Assessment Tool for small and medium-sized health care providers to help them determine their breach risk profile and to identify and remedy compliance gaps. All covered entities should ensure that they account for the likelihood of small breaches as much as they do for large breaches when doing their security risk assessments.

4) Today's Breach Report Can Lead to Tomorrow's OCR Compliance Review

According to the Compliance Report, OCR opens compliance review to investigate "all reported breaches affecting 500 or more individuals, and may open compliance reviews into certain reported breaches affecting fewer than 500 individuals." In fact, the resolution of the HONI breach followed an investigation of the breach reported by the organization. Although it is unclear how many compliance reviews were completed in the same year that OCR received the HIPAA complaint that prompted the review, the Compliance Report still shows how prolific OCR is at performing these reviews – it resolved 8,363 complaints in 2011 and 9,408 in 2012 (or 14,771 in total). Interestingly, OCR determined that it either had no jurisdiction to adjudicate the complaint in 9,534 cases (e.g., because the violation occurred prior to the compliance date or it was untimely filed) or that no violation existed in 2,281 cases during the two-year reporting period. Regardless, a compliance review can often result in technical assistance or required corrective actions, so covered entities and business associates should take them seriously.

5) OCR is Getting More Active in its Compliance and Enforcement Activities

As reported in Law360 on June 12th, Jerome B. Meites, a chief regional civil rights counsel at HHS

told attendees at the American Bar Association's Physicians Legal Issues Conference that the past 12 months of HIPAA enforcement will likely pale in comparison to what OCR will do in the next year. According to the Compliance Report, despite the "ever-increasing volume of complaints, without a corresponding increase in resources, OCR is determining ways to 'work smarter,' that is, to increase the effectiveness of its allocation of staff time and other resources to achieve the most industry compliance with the HIPAA Rules."

OCR is working smarter through its concentration on "high-impact" cases and the Compliance Report noted that it doubled the number of high-impact cases that it resolved through resolutions and corrective action plans in the prior reporting period of 2008-2010. In addition, OCR is working increasingly and sharing more information with other federal and state agencies, including the Federal Trade Commission, the Department of Justice, the HHS Office of Inspector General, and State Attorneys' General, to enforce HIPAA. Lastly, the Compliance Report states that OCR is updating the Audit Protocol to reflect the new requirements under the 2013 Omnibus Rule, which indicates that the Audit Protocol will only become a more important tool in OCR's arsenal to assess compliance with HIPAA and ascertain trends in security risks to PHI throughout the health care industry.

National Law Review, Volume IV, Number 171