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

OCR (Office of Civil Rights) Responds To Critical OIG (Office of Inspector General) Report About the Extent of OCR's HIPAA Enforcement

Article By:

Michael R. Bertoncini

A report issued by the Department of Health and Human Services Office of Inspector General ("OIG") concludes that the Office for Civil Rights ("OCR") did not meet all of its federal requirements for oversight and enforcement of the HIPAA Security Rule. While the report noted OCR met some of these requirements, it also found that:

- OCR had not assessed the risks, established priorities, or implemented controls for its HITECH requirement to provide for periodic audits of covered entities to ensure their compliance with Security Rule requirements.
- OCR's Security Rule investigation files did not contain required documentation supporting key decisions because its staff did not consistently follow OCR investigation procedures by sufficiently reviewing investigation case documentation.

OIG also found that OCR had not fully complied with Federal cybersecurity requirements for its information systems used to process and store investigation data. The report recommended that OCR:

- assess the risks, establish priorities, and implement controls for its HITECH auditing requirements;
- provide for periodic audits in accordance with HITECH to ensure Security Rule compliance at covered entities;
- implement sufficient controls, including supervisory review and documentation retention, to ensure policies and procedures for Security Rule investigations are followed; and
- implement the NIST Risk Management Framework for systems used to oversee and enforce the Security Rule.

OCR's Response. In its response to OIG's findings, attached as an appendix to the report, OCR generally concurred with OIG's recommendations and described actions it has taken to address them. OCR's response to the report provides valuable information to companies as they develop their HIPAA compliance programs, including:

- From 2008 through 2012, OCR obtained corrective action from covered entities in more than 13,000 cases where they found noncompliance with HIPAA and reached resolution agreements in 11 cases with payments totaling approximately $10 million.

- The findings from the pilot audits OCR ran in 2012 indicate that covered entities generally have more difficulty complying with the Security Rule than other aspects of HIPAA and that small covered entities struggle with HIPAA compliance in each of the assessment areas – privacy, security and breach notification.

- **Future audits "are less likely to be broad assessments generally across the Rules and more likely to focus on key areas of concern for OCR identified by new initiatives, enforcement concerns, and Departmental priorities."**

OCR's response also noted that no monies have been appropriated for a permanent audit program. However, covered entities and business associates should not see this lack of funding for a permanent audit program as giving them a pass on HIPAA compliance. The report makes clear that OCR must find a way to meet its audit requirements under HIPAA.

OCR's recent enforcement activity also demonstrates a commitment to holding companies accountable under HIPAA. In 2013 (through December 20), OCR reached five resolution agreements with payments totaling approximately $3.7 million. These figures from a single calendar year represent nearly half the total number of resolution agreements and payments that OCR obtained over the five-year period from 2008 through 2012.

In this enforcement environment, it is imperative that covered entities and business associates regularly review their HIPAA compliance program and implement ongoing HIPAA training for their employees.

National Law Review, Volume IV, Number 1