PUBLICATION

OIG Pushes OCR to Step Up HIPAA Enforcement [Ober|Kaler]

2015: Issue 17

In two recent reports, each with a specific focus, the OIG strongly recommended that the Office for Civil Rights (OCR) step up its HIPAA oversight and enforcement activities. One report assessed the OCR's oversight of covered entities' compliance with the HIPAA privacy rule and the second analyzed the OCR's enforcement related to reported breaches. The OIG's conclusions overlapped to some degree between the two reports, but all had the same theme of recommending increased OCR activity.

In conducting its analysis under both reports, the OIG reviewed closed cases involving alleged or actual violations of HIPAA privacy requirements and previously reported breaches. The analysis also involved surveys of OCR staff and interviews with OCR officials. The OIG's findings and recommendations are summarized below.

Proactive Measures

The OIG took issue with the fact that, rather than proactive initiatives, the OCR's oversight activities are primarily reactive in response to complaints, self-reporting (in the context of a breach), tips or media reports. The OCR stated that it has not fully implemented its proactive audit program, as mandated by HITECH Act, which is to assess covered entities' compliance with the privacy standards. Accordingly, the OIG recommended that the OCR implement a permanent audit program to supplement the OCR's investigation activities.

The OCR concurred with OIG's recommendations and noted that it will be launching a permanent audit program in early 2016 to include both desk reviews and onsite reviews. These audits will also include HIPAA business associates. Notwithstanding the anticipated audit program, the OCR noted that budgetary constraints have presented an obstacle to the OCR implementing additional responsibilities as may have been required. Accordingly, the OCR stated, the longevity of the audit program will depend on the availability of necessary resources.

Documentation Maintenance

In both reports, the OIG found that the OCR did not maintain complete information in its information management database – Program Information Management System (PIMS). Specifically, the OIG stated that the OCR did not track small (i.e., less than 500 individuals) breach reports, a covered entity's compliance history or complete documentation of OCR-mandated correction actions when an investigation was closed on condition of such actions. The OIG views this information as necessary for the OCR to identify covered entities and business associates who have repeated compliance issues indicative of greater systemic HIPAA compliance issues. This information could also guide the OCR in deciding upon the most appropriate response to certain cases, such as deciding between an onsite or desk review audit and/or a resolution agreement versus the imposition of a civil monetary penalty.

The OCR not only concurred with these recommendations but, by the time of the report's publication, had implemented enhancements to PIMS. Now, the OCR states that it can capture small and large breach

information alike in PIMS and track a covered entity's and business associate's history of compliance and past reported breaches. The OCR's response stated that the OCR will also be changing its policies to ensure OCR staff review an entity's past compliance when commencing a new investigation.

Accordingly, while "repeat offenders" may not have been subject to heightened scrutiny as compared to "first timers" in the past, covered entities and business associates alike should be prepared for that to change when undergoing or reporting a subsequent investigation or breach.

Education and Outreach Activities

OIG recommended expanded education and outreach activities. Specifically, OIG recommended that the OCR continue presenting to health care associations, providing electronic communications on websites and listservs and posting resources such as template policies. OIG also recommended that the OCR take effort to assess the impact of these educational activities.

The OCR responded that it will continue its educational efforts and dissemination of resources, such as its YouTube channel, HIPAA training modules; various guidance documents including CMS MedLearn matters fact sheets and participation in speaking events involving stakeholders.

Ober¦Kaler's Comments

Though the OCR concurred with the OIG's recommendations in both reports, it did cite budgetary constraints as a main obstacle to implementing many of these suggestions on the required timeline. It also conditioned its ability to continue the recommended improvements, such as permanent audit program, based upon the continued availability of resources. The HITECH Act permitted fines and penalties to be used, in part, to fund OCR activities. HITECH Act §13410(c). Therefore, considering the strong push from the OIG to increase this activity and the OCR's agreement to do so, coupled with the OCR's cited struggle with resources, covered entities and business associates would be prudent to prepare for more monitoring, proactive auditing and potentially heftier fines in the very near future.