THE NATIONAL LAW REVIEW

HHS Office of Inspector General Calls for Increased Oversight and Enforcement of HIPAA

Thursday, November 12, 2015

Article By Amy C. Pimentel
Daniel F. Gottlieb Edward G. Zacharias
McDermott Will & Emery
Publications - Insights

Communications, Media & Internet
Health Law & Managed Care
All Federal

On September 29, 2015, the ***U.S. Department of Health & Human Services Office of the Inspector General (OIG)***, Office of Evaluation and Inspections, released two studies calling on the HHS Office for Civil Rights (OCR) to strengthen its efforts in both general enforcement of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Standards and enforcement of security breach reporting requirements. OIG commissioned both studies out of concern for the increased risk of an invasion of privacy and exposure to fraud, identity theft, and other harm that patients face in an ever-expanding digital health environment.

In its response to OIG, OCR generally concurred with the OIG's recommended improvements to its HIPAA investigation and enforcement practices and stated that OCR will launch its delayed its phase 2 audits (Phase 2 Audits) of compliance with the HIPAA Privacy, Security and Breach Notification Standards in early 2016. The anticipated launch of the Phase 2 Audits, as well as OCR's public statements that it intends to step up its enforcement activities, should be an impetus for covered entities and business associates to assess their privacy, security and breach notification practices for compliance with the HIPAA standards and to mitigate the risks, threats and vulnerabilities to protected health information (PHI) that lead to breaches. OCR's responses to the studies are consistent with its prior statements over the past couple of years that enforcement is a high priority. For more information on the Phase 2 audit program, see "OCR Launches Phase 2 HIPAA Audit Program with Pre-Audit Screening".

Study of OCR Oversight of HIPAA Privacy Standards

The OIG study entitled, "OCR Should Strengthen its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards", concludes that OCR's oversight is "primarily reactive" and OCR investigates covered entities' possible noncompliance in response to complaints instead of proactively auditing covered entities' compliance under the audit program required by the Health Information Technology for Economic and Clinical Health Act (HITECH).

OIG recommended that OCR take the following five key steps to improve its oversight of covered entities:

- Fully implement the permanent HIPAA audit program;
- Maintain complete documentation in OCR's Program Information Management System (PIMS) case tracking system of corrective action taken by covered entities in cases investigated by OCR;
- Develop an efficient method in PIMS to search for and track covered entities;
- Require OCR staff to check whether covered entities have been previously investigated to identify any history of noncompliance; and
- Expand outreach and education efforts, including by targeting health industry and professional health care associations.

In its response letter to the OIG study, OCR accepted the recommendations and reported that it has already addressed certain of the recommendations and is in process on others. As of September 2015, OCR reported that it has updated PIMS and is developing policies to ensure its staff reviews a covered entity's history of prior investigations upon the initiation of a new investigation and fully documents investigations and corrective actions. As noted above, OCR reported that it plans to start the Phase 2 Audits in 2016.

Study of OCR Follow-up of Reported Breaches

The OIG study entitled, "OCR Should Strengthen its Follow-up of Breaches of Patient Health Information Reported by Covered Entities", concludes that OCR has not completely or adequately documented or investigated reports of data breaches. OIG recommended that OCR take five key steps to improve its response to reported breaches, which generally mirror the recommendations in the OIG's other study discussed above.

In addition, OIG recommends that OCR enter information about small breaches affecting fewer than 500 individuals into PIMS to facilitate identification of covered entities that experience multiple breaches and may have systemic problems. This recommendation and OCR's concurrence is a warning to covered entities and business associates that routinely experience smaller breaches in their business operations.

What Should You do to Prepare for Phase 2 Audits?

Covered entities and business associates should take the following steps to ensure that they are prepared for the possibility of a Phase 2 Audit and minimize the risk of civil money penalties in the event of a security breach or complaint by an individual patient or health plan member:

- Confirm that the organization has recently completed a comprehensive assessment of potential security risks and vulnerabilities to the organization (Risk Assessment)
- Confirm that all action items identified in the Risk Assessment have been completed or are on a reasonable timeline to completion
- If the organization has not implemented any of the Security Standards' addressable implementation standards for any of its information systems, confirm that the organization has documented (1) why any such addressable implementation standard was not reasonable and appropriate, and (2) all alternative security measures that were implemented
- Ensure that the organization has implemented a breach notification policy that accurately reflects the content and deadline requirements for breach notification under the Breach Notification Standards
- For health care provider and health plan covered entities, ensure that the organization has a compliant Notice of Privacy Practices and not only a website privacy notice
- Ensure that the organization has reasonable and appropriate safeguards in place for PHI that exists in any form, including paper and verbal PHI that is not regulated by the Security Standards
- Confirm that workforce members have received training on the HIPAA Standards that are necessary or appropriate for workforce members to perform their job duties
- Confirm that the organization maintains an inventory of information system assets, including mobile devices (even in a bring-your-own-device environment)
- Confirm that all systems and software (including networked medical devices) that transmit electronic PHI employ encryption technology, or that the organization has a documented risk analysis supporting the decision not to employ encryption
- Confirm that the organization has adopted a facility security plan for each physical location that stores or otherwise has access to PHI, and not only a security policy that requires a physical security plan
- Review the organization's HIPAA security policies to identify any actions that have not been completed as required (physical security plan, disaster recovery plan, business continuity plan, etc.)