Health Information Compliance Alert

Compliance Update: OIG Calls for Crackdown on Faulty HIPAA Security

Prepare for scrutiny of your security practices in 2009.

Now's not the time to let your guard down on your Health Insurance Portability and Accountability Act compliance. Federal enforcers could be on your doorstep in 2009, thanks to a recent OIG report highlighting lapses in reviews of HIPAA

compliance programs.

The Office of Inspector General of the Department of Health and Human Services released a report on Oct. 27 that criticizes the Centers for Medicare and Medicaid Services' effectiveness of "oversight and enforcement of covered entities'

implementation of the HIPAA Security Rule."

HIPAA defines mandatory national standards to protect the confidentiality and integrity of electronic Protected Health Information while it is being stored or transmitted between entities. But CMS "had not conducted any HIPAA Security Rule

compliance reviews of covered entities" as of February 16, 2006, the OIG said. Instead, CMS "relied on complaints to identify any noncompliant covered entities that it might investigate."

The result: "CMS had no effective mechanism to ensure that covered entities were complying with the HIPAA Security Rule or that ePHI was being adequately protected," OIG said.

Tracking Isn't Enough

But it's not as if CMS isn't doing anything right. The OIG praised CMS for having an "effective process for receiving, categorizing, tracking, and resolving complaints." But the report pointed out that OIG audits of various hospitals nationwide

showed that CMS needs to do much more in ensuring implementation of the HIPAA Security Rule by using compliance reviews. The OIG pointed to "numerous, significant vulnerabilities in the systems and controls intended to protect ePHI at

covered entities." On the positive side, the OIG said that CMS has begun taking steps to conduct compliance reviews.

CMS disagreed with the OIG draft report by stressing its belief that its "complaint-driven enforcement process" has been very effective, particularly in promoting "voluntary compliance." But CMS agreed that compliance reviews are useful as part of

a broad-spectrum enforcement strategy that would include "complaint investigation and resolution, outreach, and education" among other measures.

The OIG confirmed that what CMS has done to enforce HIPAA compliance has still encouraged providers to "voluntarily" comply, but the OIG also pointed to significant vulnerabilities in hospitals across the nation that would have fallen under the

radar in HIPAA Security Rule complaints. **The message for healthcare providers?** Be prepared for more HIPAA reviews from CMS in the coming months and years.

Codify
BY AAPC