Codify by AAPC

Health Information Compliance Alert

Audits: What To Expect From The New OIG Security Audits

BAs are off the hook for ePHI security reviews □ for now.

If you're participating in the Electronic Health Record (EHR) Incentive Program, get ready for the **HHS Office of Inspector General** (OIG) to conduct security audits. Here's what to expect.

The OIG will conduct in-depth security audits of Eligible Hospitals (EHs) and potentially Eligible Professionals (EPs), according to Seattle-based associate attorney **Elana Zana** in a recent analysis for **Ogden Murphy Wallace Attorneys**. Unlike other HIPAA-related audits, the **Centers for Medicare & Medicaid Services** (CMS) and the **HHS Office for Civil Rights** (OCR) are not involved.

EHs and EPs will face pending audits from CMS, including the necessary documentation and security risk analysis requirements, Zana noted. But the OIG audits "may come as quite a surprise □ especially the level of thoroughness the OIG pursues in these audits."

The OIG audits "look nothing like a CMS audit, but instead are an in-depth HIPAA security audit," Zana added.

Blame the OIG's 2015 Work Plan

Background: These audits came about in the OIG's 2015 Work Plan, and they stretch beyond a typical Meaningful Use (MU) audit, Zana said. The audits will not only focus on the security of electronic protected health information (ePHI) stored in the Certified EHR Technology (CEHRT), but also look at the relationships with downstream service providers.

Changes: The OIG's updated plan no longer includes a review of whether business associates (BAs) also are adequately securing ePHI, according to **Jim Sheldon Dean**, founder and director of compliance services for **Lewis Creek Systems LLC** in Charlotte, VT. Also, the OIG won't review CMS' oversight of hospitals' security controls over networked medical devices.

How the Audit Process Will Work

OIG investigators will conduct these audits, which will begin with a phone call followed by a formal letter notifying you of the audit, Zana explained. The OIG will then send out a questionnaire/document request containing 17 categories and subcategories under investigation. The OIG will review your responses, and then OIG auditors will come on-site for two to three weeks to conduct interviews and personally review your security infrastructure.

"It is unknown how many audits the OIG will conduct and the ultimate goal of these audits," Zana noted. "We believe that the OIG plans on creating a roll-up report to describe the findings of these audits, rather than publishing individual reports □ however this has not been verified because the OIG has denied Freedom of Information Act requests."

Take 4 Steps to Prepare

Still, you can take specific steps to prepare for the OIG audits. Zana recommends that you:

1. **Gather information** about the existing security infrastructure in place, including your organization's PHI-sharing relationships with BAs and downstream providers;

2. **Evaluate your health IT vendors** to determine if they're compliant with BA agreements (BAAs) □ consider asking your BAs to provide evidence and results from a recent security risk assessment;

3. **Identify team members** who will respond to an OIG audit request; and

4. **Conduct a mock audit** to fully assess your organization's security.

Keep Your Eye on the Horizon for Other Audits

The OIG Work Plan also cites four other related types of audits, including audits of the Medicare EHR Incentive Program, of the Medicaid EHR Incentive Programs, of Contingency Plans, and of Adopting, Implementing or Upgrading (AIU) Participants.

According to Sheldon-Dean, as part of its 2015 Work Plan, the OIG will review:

- The use of EHRs by accountable care organizations (ACOs) to coordinate care;
- The extent that providers participating in ACOs in the Medicare Shared Savings Program (MSSP) use EHRs to exchange health information to achieve their care coordination goals;
- Providers' use of EHRs to identify best practices and possible challenges in their progression toward interoperability;
- EHR contingency planning required by HIPAA;
- Whether providers that received Medicare and/or Medicaid MU incentive payments were entitled to the money; and
- Whether covered entities (CEs) are adequately securing ePHI created or maintained by certified EHR technology.

Resource: To read the OIG's 2015 Work Plan, go to http://oig.hhs.gov/reports-and-publications/archives/workplan/2015/FY15-Work-Plan.pdf.