Health Information Compliance Alert

Compliance: Brace Yourself For Amped-Up EHR & HIPAA Compliance Enforcement

Hospitals will endure additional scrutiny from the OIG.

Just when you thought that HIPAA enforcement efforts couldn't get any more severe, the **HHS Office of Inspector General** (OIG) unveiled its fiscal year (FY) 2016 Work Plan and compliance relating to electronic protected health information (ePHI) and electronic health records (EHRs) is firmly in the watchdog's sights.

Here's what you can expect in the coming year from the OIG:

Does OCR Need to Boost Enforcement?

In FY 2016, the OIG will take a hard look at whether the **HHS Office for Civil Rights** (OCR) is providing adequate oversight of ePHI security, according to the Work Plan. Citing the findings of prior OIG audits, the watchdog stated that OCR has not assessed the risks, established priorities, or implemented controls for its Health Information Technology for Economic and Clinical Health (HITECH) Act requirement to provide for periodic audits of covered entities (CEs) and business associates (BAs) to ensure compliance with the Act and HIPAA requirements.

Result: Therefore, OCR had limited assurance that CEs and BAs adequately protected ePHI in the past, the OIG charged. Prior OIG audits also found "numerous vulnerabilities in the systems and controls to protect ePHI at selected [CEs]."

Expect Scrutiny of Your EHR Incentive Payments, Too

As part of its "Delivery System Reform" efforts, the OIG will review the extent to which providers participating in Accountable Care Organizations (ACOs) in the Medicare Shared Savings Program (MSSP) use EHRs to exchange health information in achieving care coordination goals. The OIG will also assess providers' use of EHRs to identify best practices and possible challenges for exchanging and using health data, such as degree of interoperability, financial barriers, or information blocking.

Also on the OIG's radar screen are the Medicare and Medicaid incentive payments for adopting EHRs. The OIG plans to review the incentive payment system, as well as **Centers for Medicare & Medicaid Services** (CMS) safeguards to prevent erroneous incentive payments. CMS's plans to oversee incentive payments and corrective actions it's taken regarding erroneous incentive payments will also be under the microscope.

Cost: As of July 2015, Medicare EHR incentive payments totaled more than $20 billion and Medicaid incentive payments totaled more than $9 billion. The OIG will review incentive payment data to identify payments to providers who should not have received incentive payments, for reasons such as they didn't meet selected meaningful use criteria.

Prepare for More Yes, More Audits

Further, the OIG plans to perform audits of various CEs receiving EHR incentive payments from CMS to find out whether they adequately protect ePHI that the certified EHR technology creates or maintains. And one way the OIG will do this is by determining whether you've conducted a risk analysis.

CPT® 2023 American Medical Association. All rights reserved.

Important: "A core meaningful use objective for eligible providers and hospitals is to protect electronic health information created or maintained by certified EHR technology by implementing appropriate technical capabilities," the OIG stated. "To meet and measure this objective, eligible hospitals must conduct a security risk analysis of certified EHR technology as defined in Federal regulations and use the capabilities and standards of Certified Electronic Health Record Technology."

Approximately 20 percent of physicians fail this objective, and the most common reason for failure is the lack of an adequate security risk analysis and appropriate remediation, according to a Nov. 4 analysis by consultant **Gary Pritts** of **Eagle Consulting Partners**.

What's more: Also, beware that these newly announced audits are among several different audits that will occur in 2016, Pritts warned. You also have to prepare for the meaningful use audits by CMS contractor **Figliozzi & Company** next year, as well as the OCR Phase 2 audits, which are further delayed until the second quarter of 2016.

Hospitals: Your Contingency Planning is Under Scrutiny

In FY 2016, the OIG will also crack down on hospitals' compliance with the HIPAA Security Rule's requirements for contingency planning. Specifically, the OIG will compare hospitals' contingency plans with government- and industry-recommended practices.

The contingency planning requirement under HIPAA "is one of the most important of the HIPAA regulations," Pritts noted. The implementation specifications include the following five elements:

1. Data Backup Plan;

2. Disaster Recovery Plan;

3. Emergency mode operation plan;

4. Testing and revision procedure; and

5. Applications and data criticality analysis.

Takeaway: "Certainly, a robust Backup/Recovery/Contingency Plan is appropriate for all hospitals and is required not only by HIPAA but other regulatory requirements," Pritts stressed. "Our experience with hospitals is that some have been unable (or unwilling) to make the investment in a proper contingency plan."

Another New Target: Networked Medical Devices

Get ready: And the OIG will investigate controls over networked medical devices at hospitals, to examine whether the **U.S. Food and Drug Administration's** (FDA's) oversight of hospitals' networked medical devices is sufficient to effectively protect associated ePHI and ensure beneficiary safety. This is a new initiative that the OIG is undertaking in FY 2016.

In particular, the OIG will look at computerized medical devices, such as dialysis machines, radiology systems and medication dispensing systems, that are integrated with electronic medical records (EMRs) and the larger health network.

The OIG cited medical device manufacturers' Manufacturer Disclosure Statement for Medical Device Security (MDS2), so watch out for the OIG to scrutinize whether you're using MDS2 forms to assess the vulnerabilities and risks associated with the ePHI that a medical device transmits or maintains.

CPT® 2023 American Medical Association. All rights reserved.

Do this: "In highlighting the MDS2 forms, the OIG has effectively signaled that HIPAA-covered entities that use networked medical devices should document the ways in which they have considered the disclosure statements for such devices as part of their HIPAA security risk assessments and overall HIPAA compliance plans," stated a Nov. 6 legal alert from **McGuireWoods Consulting LLP**.

Also: Although not mentioned in the 2016 Work Plan, improper disposal of networked medical devices carries significant HIPAA risks, McGuireWoods cautioned. "Specifically, for any of these devices that store ePHI locally, there is a risk of a HIPAA violation if the device is not stripped of all ePHI or otherwise destroyed prior to disposal."

Example: In 2013, **Affinity Health Plan Inc.** entered into a $1.2-million settlement agreement with HHS for returning multiple photocopiers to a leasing agent without first erasing the data contained on the copiers' hard drives.

Link: To read the OIG's FY 2016 Work Plan, go to http://oig.hhs.gov/reports-and-publications/archives/workplan/2016/oig-work-plan-2016.pdf.

CPT® 2023 American Medical Association. All rights reserved.