Dermatology Coding Alert

Compliance: Target Your EHRs for Scrutiny

Watch incentive payments, too.

HIPAA enforcement just keeps getting tougher that's the word on the street from the HHS Office of Inspector General's (OIG) fiscal year (FY) 2016 work plan.

Focus: Compliance relating to electronic protected health information (ePHI) and electronic health records (EHRs) is firmly in the OIG's sights for 2016. Read on for what you need to know to get your general surgery practice ready.

Prepare for Possible Enforcement Boost

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 its prior audits, the OIG 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 requirements. Those requirements include providing periodic audits of covered entities (CEs) and business associates (BAs) to ensure compliance with the Act and HIPAA requirements.

Upshot: More and tougher audits may be in the wings, so that the OCR can ensure that CEs and BAs adequately protect patient ePHI.

Do this: According to Seattle-based associate attorney **Elana Zana** in an analysis for Ogden Murphy Wallace Attorneys, you can take the following specific steps to prepare for OIG audits:

- Gather information about the existing security infrastructure in place, including your organization's PHI-sharing relationships with BAs and downstream providers
- Evaluate your health IT vendors to determine if they're compliant with BA agreements consider asking your BAs to provide evidence and results from a recent security risk assessment;
- Identify team members who will respond to an audit request; and
- Conduct a mock audit to fully assess your organization's security.

Expect Scrutiny of Your EHR Incentive Payments, Too

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 CMS safeguards to prevent erroneous payments.

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 find out whether CEs receiving EHR incentive payments adequately protect ePHI. One way the OIG will do this is to find out if you've "conducted a security risk analysis of certified EHR technology as defined in Federal regulations and used the capabilities and standards of Certified Electronic Health Record Technology."

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

What's more: 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 Center for Medicare and Medicaid Services (CMS) contractor Figliozzi & Company, as well as the OCR Phase 2 audits, which are further delayed until the second quarter of 2016.

Clean Your Networked Medical Devices

The OIG will investigate controls over networked medical devices that are integrated with electronic medical records (EMRs) and the larger health network. Specifically, audits will determine whether you're using Manufacturer Disclosure Statement for Medical Device Security (MDS2) forms to assess the vulnerabilities and risks associated with the ePHI that a medical device transmits or maintains.

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 legal alert from **McGuireWoods Consulting LLP.**

Related concern: Remember that 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: Affinity Health Plan Inc. entered into a $1.2-million settlement agreement with HHS in 2013 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 bit.ly/OIG-2016.