Health Information Compliance Alert

Case Study: OIG's Takedown of EHR Vendor Highlights Security's Importance

Deficient software vendor faces $155 million in paybacks to the feds.

Most electronic health record (EHR) vendors are on the up and up, but it's still vital to go through a vetting process and investigate their backgrounds and certifications. And if they promise a financial windfall with their product implementation, you may want to look elsewhere for your EHR needs.

That's the takeaway from a recent $155 million settlement that the Department of Justice made with EHR vendor eClinicalWorks to settle allegations that the vendor misrepresented its software's capabilities.

Background: Medical practices are able to participate in the government's EHR Incentive Program only if they use certified EHR technology and meet specific requirements related to their use of the technology. The government suggested that eClincalWorks did not actually comply with the certification requirements, but concealed that from the certifying entity, thus allowing the company to falsely acquire certification. As a result of the software being deficient, the company allegedly allowed practices to collect federal incentive payments that they didn't deserve, which the government classified as the submission of false claims.

"Data is input into an EHR software system that reflects the care that's provided, and it's very critical, just like in the old written medical records, that everything be accurate," said the OIG's Senior Counsel **John O'Brien** during an OIG "Eye on Oversight" video about EHRs. "If there are any defects in that software program, then critical tests, medical prescriptions, may not be accurately processed, and that could have detrimental effects on patient care."

Not only does the settlement serve as a reminder to healthcare practices that they must be careful about trusting software and vendors, but it's also a sign that the fraud arena is evolving. "This settlement is important because it's the first settlement with an electronic health record software company, so we're entering an entirely new area of healthcare fraud," O'Brien said.

The bottom line is that medical practices should use the EHR as a tool to streamline operations, but should only trust it as much as they trusted the data they were submitting via paper records.

"Electronic health records have the potential to improve the care provided to Medicare and Medicaid beneficiaries, but only if the information is accurate and accessible,"

said OIG Special Agent in Charge **Phillip Coyne** in a news release about the case.

Consider These EHR Best Practices

If you're considering adopting a new EHR system, make sure you're on top of the entire process, from researching the vendor to asking for references from other practices that have used it. Don't ask your practice's IT person to handle the selection and implementation process, or the system won't be as user-friendly as it would if clinicians were involved.

In addition, make sure the vendor upgrades the system on a regular basis, especially when new codes or rules are issued, so you're always selecting the most accurate information from the system.

Audit concerns: Due to the severity of the eClinicalWorks landmark case, you can expect the OIG to execute tougher audits, helping the HHS Office for Civil Rights ensure that covered entities (CEs) and business associates (BAs) adequately protect patient ePHI.

Do this: According to Seattle-based associate attorney **Elana Zana, Esq.** 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.

Resource: To read more about the government's settlement with the vendor, visit https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.