Health Information Compliance Alert

Fraud & Abuse: Feds Target EHR-Related Fraud

Investigate your vendors thoroughly to avoid problems.

Digital platforms make the practice of medicine more efficient and enhance patient engagement. However, several enforcement actions over the past year suggest that these important tools - plus the manufacturers and EHR users - are coming under greater federal scrutiny.

Background: With all the technical updates, attestation requirements, and certification mandates coming down the pike from the feds, it's easy to get overwhelmed. And on top of that, federal enforcers like the **Department of Justice** (DOJ) and the **HHS Office of Inspector General** (OIG) now use these same health IT tools to monitor and investigate providers and their business associates (BAs).

In the most recent Semiannual Report to Congress, the feds weigh in on their primary targets and what they're looking at. "OIG's talented and dedicated workforce uses multidisciplinary approaches, cutting-edge data and technology, and collaborations at the federal, state, and local levels to achieve our mission," explains **Joanne M. Chiedi**, acting HHS-OIG inspector general in the report. "Our work demonstrates that promising technology that can help patients...can also be misused for fraud and put patients at risk. At this transformational time in healthcare, OIG will be vigilant and innovative in advancing program integrity."

See 2 Cases That Highlight the Feds' Focus on EHR Vendors

Unfortunately, you need to investigate the practices of your associates - from the software firms you utilize to your cloud providers, cautions **Kurt J. Long**, founder and CEO of **FairWarning, Inc.** in Clearwater, Florida. For example, consider the compliance of your cloud providers. "Not all cloud vendors are alike. It is more nuanced than that," he explains.

Long advises practices to research and check into the backgrounds of their EHR vendors. "Look for third-party evidence when choosing a vendor for your EHR - a good-looking website does not equate to a mature product or adequate security."

Two recent EHR-related cases show how easy it is for organizations to become embroiled in False Claims Act (FCA), Anti-Kickback Statute (AKS), or Stark Law violations. Examine the logistics and settlements of the cases:

1. Review the EHR's capabilities thoroughly.

The San Francisco-based EHR firm **Practice Fusion, Inc.** engaged in an opioid-related scheme utilizing its EHR software that led to both civil and criminal investigations. On Jan. 27, the company

agreed to pay a substantial sum to the government to resolve its plethora of crimes, which included kickbacks and false claims.

Practice Fusion's reconciliation includes $26 million in fines and forfeiture as part of a deferred prosecution agreement. Plus the organization will pay an additional $118.6 million to "resolve allegations that it accepted kickbacks from the opioid company and other pharmaceutical companies and also caused its users to submit false claims for federal incentive payments by misrepresenting the capabilities of its EHR software," noted a DOJ release on the case.

Of interest: Though Practice Fusion engaged in several fraudulent acts, the most worrisome relates to its acceptance of $1 million from a pharmaceutical company to push an extended-release opioid drug in the EHR.

"Practice Fusion allegedly permitted pharmaceutical companies to participate in designing the [clinical decision support] CDS alert, including selecting the guidelines used to develop the alerts, setting the criteria that would determine when a healthcare provider received an alert, and in some cases, even drafting the language used in the alert itself. The CDS alerts that Practice Fusion agreed to implement did not always reflect accepted medical standards," DOJ said.

The CDS alerts were pushed on unknowing providers from 2014 to 2019, who then wrote prescriptions when they might not have been medically necessary.

"While the **Department of Health & Human Services** [HHS] contemplates whether changes in the regulation are necessary to preserve the integrity of decision alerts embedded in EHR systems, DOJ will likely continue to scrutinize the software developers," says partner attorney **Thomas E. Jeffry Jr.**, with national law firm **Arent Fox LLP** in the Health Care Counsel Blog.

Important: "Across the country, physicians rely on electronic health records software to provide vital patient data and unbiased medical information during critical encounters with patients," warned **Ethan Davis**, principal deputy assistant Attorney General in the DOJ civil division in the release. "When a software vendor claims to be providing unbiased medical information - especially information relating to the prescription of opioids - we expect honesty and candor to the physicians making treatment decisions based on that information."

See a DOJ breakdown of the Practice Fusion settlement at www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0.

2. Double-check EHR certifications.

Tampa, Florida-based EHR firm **Greenway Health LLC** forked over $57.25 million for FCA violations for illegal claims it submitted to the government while "misrepresenting the capabilities of its EHR product 'Prime Suite' and providing unlawful remuneration to users to induce them to recommend Prime Suite," indicated a DOJ release.

The vendor falsely acquired 2014 Edition certifications for Prime Suite; however, the EHR did not actually "fully comply" with the federal certification requirements, said the DOJ. Greenway didn't rectify its issue, but instead promoted Prime Suite and encouraged others to suggest it. In addition, after reporting using the faulty Prime Suite EHR, users "falsely attested that they were eligible for EHR incentive payments" - when they weren't, said the report.

Food for thought: Despite regulatory rollbacks that streamline healthcare, the feds don't seem to be easing up on providers or their BAs. In fact, evidence suggests the opposite, and rather that enforcement against healthcare fraudsters is on the rise.

DOJ reported that for the fiscal year (FY) 2019, which ended in September 2019, more than $3 billion in settlements and judgments from civil suits related to all false claims against the U.S. government. Moreover, $2.6 billion of that massive total correlated specifically to cases in the healthcare industry that involved "drug and medical device manufacturers, managed care providers, hospitals, pharmacies, hospice organizations, laboratories, and physicians," noted a DOJ brief. "This is the tenth consecutive year that the department's civil healthcare fraud settlements and judgments have exceeded $2 billion."

Review all the DOJ 2019 false claims stats, including in-depth details on Greenway Health at www.justice.gov/opa/pr/justice-department-recovers-over-3-billion-false-claims-act-cases-fiscal-year-2019.