FCA Attention Turns To Electronic Health Records

By **Jaime Jones and Brenna Jenny |** December 6, 2017, 11:58 AM EST

Touting the potential patient benefits of health care providers using electronic health records (EHR) systems in place of paper, the Centers for Medicare & Medicaid Services is committing significant resources toward encouraging the use of EHR systems. One of the primary initiatives is the "meaningful use" program, through which CMS offers incentive payments to health care providers who demonstrate and attest to using EHR systems that have certain qualities and satisfy specific objectives. The flow of funds has become a torrent: as of September 2017, over half a million health care providers received close to $40 billion in meaningful use payments from CMS.

Unsurprisingly, the increased adoption of EHR systems and the government's subsidization thereof has attracted attention from relators filing qui tam suits under the False Claims Act. These suits assert a range of theories, from alleged submission of claims for unearned meaningful use payments to EHR-facilitated "upcoding," and they have been aimed at both EHR vendors and health care providers. Intensifying the focus, the U.S. Department of Justice has made clear that fighting fraud relating to the use of EHR systems is an enforcement priority. As a result, both EHR vendors and health care providers are under increased pressure to timely identify and return overpayments stemming from their use of EHR systems.

On the eve of CMS's first meaningful use incentive payments in 2011, the Office of Inspector General for the U.S. Department of Health and Human Services (HHS-OIG) began expressing interest in policing incentive payments relating to EHR use. HHS-OIG explained in its fiscal year 2010 work plan that it would review "CMS's safeguards against incentive payments made in error." That work was completed in June 2017 and HHS-OIG estimated, based on extrapolation, that from May 2011 to June 2014, CMS paid out $730 million in Medicare meaningful use payments to providers who did not meet program requirements.[1] From late 2014 through late 2016, OIG released a series of reports summarizing its audits of the Medicaid meaningful use payments made by 17 state agencies. Those reports concluded that only three states had accurately made incentive payments in accordance with federal and state requirements; the others had erred in the direction of overpaying, with Texas ($12.5 million)[2], Arizona ($14.8 million)[3], and

California ($22 million)[4] each exceeding $10 million in net overpayments, even without OIG extrapolating the errors identified in the samples.

This summer, HHS-OIG posted a video on YouTube ("Eye on Oversight - Electronic Health Records") highlighting the DOJ's own efforts to police fraud relating to EHR systems, especially in the context of inappropriate meaningful use payments. Those efforts resulted in the government's first major FCA settlement with an EHR vendor in May 2017, the $155 million settlement with eClinicalWorks (eCW). The settlement resolved allegations in a qui tam suit — filed by a consultant who had worked for several eCW customers — that eCW had falsely represented that its EHR system satisfied meaningful use criteria when it in fact suffered from various system defects. The relator alleged that those defects caused health care providers using eCW software falsely to attest to eligibility for meaningful use payments. The government intervened and also expanded upon the relator's complaint to allege that eCW violated the Anti-Kickback Statute, including by offering a "referral program" through which it paid users a fee for each provider they referred to sign a contract with the company. The settlement agreement announced by the DOJ similarly resolved these allegations.

Beyond being the first FCA settlement to address claims based on the use of EHR systems and meaningful use payments, the eCW settlement is notable because three of the company's founders and executives are jointly and severally liable for the $155 million settlement. The settlement is structured this way despite the fact that neither the government's complaint in intervention nor the settlement agreement specify their roles in the alleged misconduct. eCW is a privately held company, and the settlement structure may simply help ensure the DOJ will be able to collect the amount due. It may also have been driven by the Yates memo's directive that the DOJ hold individuals personally responsible, including under the FCA, in appropriate circumstances.

Both the DOJ's complaint in intervention and press release issued in connection with the settlement agreement make clear that the government is concerned with addressing not only the harm to the federal fisc arising from flawed EHR systems, but also patient harm that could arise from the use of such systems. For example, the DOJ cited the potential for EHR systems to fail to "send accurate NDC codes when transmitting medication orders" as a risk to patients.

In connection with its settlement, eCW also entered into a corporate integrity agreement

with HHS-OIG. Among the terms of that agreement, eCW must, at any customer's request, transfer the customer's data at no charge to a different EHR vendor and promptly notify customers of any identified system deficiencies.

eCW is not the only EHR vendor currently under DOJ and HHS-OIG scrutiny, and others certainly will follow. Following the eCW settlement, HHS-OIG senior counsel John O'Brien characterized the settlement as reflecting the government "entering an entirely new area of healthcare fraud" enforcement, and he promised that OIG would "vigilantly" continue to work with "law enforcement partners" to crack down on EHR fraud. The former National Coordinator for Health Information Technology warned via Twitter: "eClinicalWorks is not the only EHR vendor who 'flouted certification/misled' customers. Other vendors better clean up."

This ongoing enforcement scrutiny will not be limited to flaws in EHR systems that may cause providers falsely to claim meaningful use payments. For its part, HHS-OIG has made clear that it will assess "fraud vulnerabilities presented by electronic health records" more generally, including inappropriate cloning and "auto-prompts" that encourage upcoding.[5] Both the DOJ and relators are asserting FCA claims based on precisely such EHR vulnerabilities, contending that they facilitate "upcoding" and other forms of provider billing fraud. For example, in a qui tam suit recently unsealed against EHR vendor Epic Systems (Epic), the relator alleges that Epic's software causes providers accidentally to double-bill for anesthesia services.[6] Last year, when the DOJ intervened in a qui tam suit relating to falsified home health services, its complaint in intervention emphasized the provider's use of an EHR system to manipulate documentation: "[The defendant] also utilized an electronic medical records (EMR) system that permitted the [nurses] to easily electronically cut, copy and paste medical notes from prior visits. The ability to migrate notes from visits that occurred weeks, months, or even years prior to the current patient encounter created the illusion that [the defendant's nurses] were performing a significant amount of work during their patient encounters when, in fact, they were not."[7]

The government's enforcement activity to date suggests that both EHR vendors and providers should examine their processes related to the development and use of EHR systems. Vendors should ensure that they promptly notify customers of software issues that may cause their systems to fall short of meaningful use criteria or could produce inaccurate patient or billing data. For their part, providers must be increasingly vigilant about identifying deficiencies with their EHR systems and training employees on the proper use of those

systems, in order to ensure that they can appropriately evaluate, report and return any overpayments received as a result of defects in or the misuse of EHR systems.

Jaime L.M. Jones is a partner at Sidley Austin LLP in Chicago. Brenna E. Jenny is an associate at Sidley in Washington, D.C.

[1] HHS-OIG, Medicare Paid Hundreds of Millions in Electronic Health Record Incentive Payments That Did Not Comply with Federal Requirements (June 2017), available at https://oig.hhs.gov/oas/reports/region5/51400047.pdf.

[2] HHS-OIG, Texas Made Incorrect Medicaid Electronic Health Record Incentive Payments (August 2015), available at https://oig.hhs.gov/oas/reports/region6/61300047.pdf.

[3] HHS-OIG, Arizona Made Incorrect Medicaid Electronic Health Record Incentive Payments to Hospitals (August 2016), available at https://oig.hhs.gov/oas/reports/region9/91502036.pdf.

[4] HHS-OIG, California Made Incorrect Medicaid Electronic Health Record Incentive Payments to Hospitals (September 2016), available at https://oig.hhs.gov/oas/reports/region9/91602004.pdf.

[5]HHS-OIG, FY 2012 Work Plan, https://oig.hhs.gov/reports-and-publications/archives/workplan/2012/work-plan-2012.pdf. CMS published a fact sheet in 2015 describing the agency's perspective on various EHR fraud vulnerabilities. See CMS, Electronic Health Records Provider (December 2015), available at https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Downloads/docmatters-ehr-providerfactsheet.pdf.

[6] United States ex rel. Petrowski v. Epic Systems Corp., No. 8:15-cv-01408 (M.D. Fla.).

[7] Press Release, U.S. Dep't of Justice, Louisville Based MD2U, a Regional Provider of

Home-Based Care, and Its Principal Owners Admit to Violating the Federal False Claims Act and Being Liable for Millions (July 7, 2016), https://www.justice.gov/opa/pr/louisville-based-md2u-regional-provider-home-based-care-and-its-principal-owners-admit.