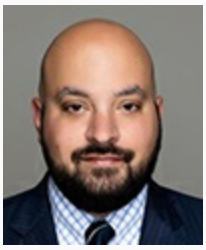
COSMOS
Navigate the Compliance Universe

Compliance Today - July 2022
The government giveth and the government taketh away: Government enforcement and electronic health records


Scott R. Grubman

By Scott R. Grubman

Scott R. Grubman (sgrubman@cglawfirm.com) is a partner at Chilivis Grubman in Atlanta, Georgia, where he focuses his practice on representing healthcare providers of all types and sizes in connection with government investigations and False Claims Act litigation.

- linkedin.com/in/sgrubman/

In 2011, the Centers for Medicare & Medicaid Services (CMS) established the Medicare and Medicaid EHR Incentive Programs—now known as the Medicare Promoting Interoperability Program—to encourage healthcare providers to "adopt, implement, upgrade, and demonstrate meaningful use of certified electronic health record technology."[1] Then, in 2016, CMS announced that it had allocated nearly $35 billion in meaningful use incentive payments to more than 500,000 providers.[2]

As with most well-intentioned, government-backed incentive programs, outlay of those funds has been followed by years of scrutiny and government enforcement actions. In June 2017, the U.S. Department of Health & Human Services (HHS) Office of Inspector General (OIG) announced the findings of an audit alleging that CMS inappropriately paid more than $729 million in incentive payments to healthcare providers who did not meet meaningful use requirements.[3] In December 2019, OIG announced that, out of the $10.8 billion that went to acute-care hospitals, an estimated $93.6 million was incorrectly paid.[4]

It is not surprising then that the Department of Justice (DOJ) has dedicated significant resources to investigating and prosecuting fraud matters related to electronic health record (EHR) incentive payments and other aspects of the EHR industry. In December 2020, Deputy Assistant Attorney General Michael Granston, who oversees False Claims Act (FCA) enforcement, made remarks to the American Bar Association's Civil False Claims Act and Qui Tam Enforcement Institute.[5] Discussing the DOJ's FCA enforcement priorities, Granston identified fraud pertaining to EHRs as a likely "focal point" of the DOJ's future enforcement efforts. According to Granston, "providers increasingly rely on electronic health records to provide vital and unbiased information to improve treatment outcomes for patients. While electronic software is intended to reduce errors and improve the delivery of care, the transition to a digital format has also introduced new opportunities for fraud and abuse."

Enforcement actions against EHR vendors

Almost two months prior to Granston's remarks, the DOJ announced a proposed settlement with opioid manufacturer Purdue Pharma, wherein Purdue and individual shareholders agreed to pay more than $8 billion to resolve various criminal and civil fraud allegations regarding its marketing of OxyContin and other opioid products.[6] Part of that settlement involved allegations that Purdue paid EHR vendor Practice Fusion in exchange for recommending Purdue's opioid products. In January 2020, Practice Fusion agreed to pay $145 million to resolve criminal and civil kickback allegations involving the same arrangement.[7] As part of that

settlement, Practice Fusion admitted that it received kickbacks from Purdue "in exchange for utilizing its EHR software to influence physician prescribing of opioid pain medications." Specifically, Practice Fusion set up "clinical decision support" alerts in its EHR system, where the EHR system alerted the provider-user when certain criteria were met that would make it appropriate to prescribe the opioid. According to the government's allegations, Practice Fusion allowed pharmaceutical companies to participate in the designing of those alerts, "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."

This was not the first time that the DOJ brought a fraud enforcement action against an EHR vendor. For example, in May 2017, it announced that EHR vendor eClinicalWorks (ECW) agreed to pay $155 million to resolve allegations that it violated the FCA by paying kickbacks to certain customers in exchange for promoting its product.[8] The government also alleged that ECW obtained a "meaningful use" certification by concealing that its software failed to comply with certain requirements for such certification. According to the government, this false certification by ECW in turn caused healthcare providers who used the EHR program to submit false claims for meaningful use incentive payments.

Nearly two years later, in February 2019, the DOJ announced another large settlement against EHR vendor Greenway Health, which agreed to pay more than $57 million to resolve FCA allegations.[9] Similar to the allegations in the ECW case, the DOJ alleged that Greenway misrepresented the capabilities of its EHR product, thereby causing its users to submit false claims for meaningful use incentive payments. The following year, EHR vendor Konica Minolta Healthcare agreed to pay $500,000 to resolve similar FCA allegations involving false statements to the meaningful use incentive payment certification authority.[10]

Just a little over a month after Granston's remarks at the American Bar Association conference, in January 2021, the DOJ announced yet another FCA settlement with an EHR vendor, this time athenahealth Inc. (Athena). In this case, the DOJ alleged that Athena violated the FCA and the Anti-Kickback Statute by paying unlawful kickbacks to generate sales of its EHR product.[11] Specifically, the government alleged that Athena violated the law by inviting prospective and existing customers to "Concierge Events," providing free tickets and travel to sporting and entertainment events, as well as luxury accommodations, meals, and alcohol. The government also alleged that Athena paid kickbacks to its existing customers designed to identify and refer perspective clients. Three months later, in April 2021, the DOJ announced a $3.8 million settlement with EHR developer CareCloud Health, alleging that it offered and provided its clients with cash payments and bonuses to recommend its EHR product to perspective clients.[12]

A recent filing by the DOJ in Vermont suggests that the DOJ's enforcement against EHR vendors continue. On March 15, 2022, the DOJ filed a notice to intervene in an FCA qui tam action filed against EHR vendor Modernizing Medicine and several related individuals.[13] According to the relator's complaint in that case, Modernizing Medicine violated the FCA by allegedly misrepresenting its compliance with meaningful use requirements, providing certain remuneration to its users, and programming its EHR software in a way that resulted in "upcoding" of evaluation and management (E/M) codes and use of improper modifiers.