AHLA

VOLUME 19 ISSUE 2 November 2017

Health Care Liability & Litigation

A Publication of the American Health Lawyers Association
Health Care Liability and Litigation Practice Group

Table of Contents

False Claims Act Lawsuits Are Ready to "Go Viral" in the Health IT Industry

Melissa L. Jampol
Epstein Becker & Green PC
New York, NY and Newark, NJ

Richard W. Westling
Epstein Becker & Green PC
Nashville, TN and Washington, DC

Yulian Shtern
Epstein Becker & Green PC
Newark, NJ

On May 31, 2017, in a first of its kind settlement, eClinical Works (ECW), one of the nation's largest electronic health records (EHR) vendors,[1] agreed to pay $155 million to settle a False Claims Act (FCA) lawsuit, filed by a qui tam relator, after the Department of Justice (DOJ) intervened.[2] The settlement resolved allegations that ECW falsely certified the capabilities of its EHR software and paid kickbacks to customers in exchange for promoting its product. ECW also agreed to a unique corporate integrity agreement (CIA), tailored specifically for EHR vendors, which, among other things, requires it to hire an independent software quality oversight organization.

While health information technology (IT) vendors generally have stayed out of the spotlight in FCA litigation, the nature and amount of the ECW settlement is sure to increase the risk that other vendors will face FCA actions. Indeed, the complaint, settlement agreement, and CIA provide a roadmap for future actions against other health IT vendors.

The False Claims Act—Health IT and Meaningful Use

The FCA imposes civil liability on any person who knowingly, among other things, (1) presents, or causes to be presented, to the government a false or fraudulent claim for payment or approval; or (2) makes, uses, or causes to be made or used a false record or statement to get a false or fraudulent claim paid or approved by the government.[3] The FCA's application to the health care industry continues to increase and, in fiscal year 2016 alone, the DOJ recovered $2.5 billion from health care-related FCA actions, while whistleblowers filed 702 qui tam suits—an average of 13.5 new cases every week.[4]

FCA claims against IT vendors can be traced back to the 1990s, when several software contractors were the subject of relator-initiated actions.[5] For example, one contractor faced FCA liability for falsifying progress reports in connection with the delivery of software to the Department of Labor's Pension and Welfare Benefits Administration (PWBA).[6] Since payments to the contractor were based, in part, on the accuracy of these progress reports, any material misrepresentations made therein were treated as false claims to the PWBA.

More recently, health care fraud enforcement relating to IT vendors has focused on non-compliance with the "meaningful use" incentive payment program. The Health Information Technology for Economic and Clinical Health Act (HITECH)[7] provides incentive payments to providers who demonstrate "meaningful use" of certified EHR technology.[8] To be eligible for incentive payments, providers must certify the adoption of certified EHR software and their meaningful use of such technology.

A key component of HITECH is that software must be certified in accordance with applicable regulations to be eligible for the meaningful use program.[9] The certification process is overseen by the Office of the National Coordinator for Health Information Technology (ONC), which delegates software certification functions to accredited testing laboratories and authorized certification bodies.[10] These accrediting organizations must verify the software's compliance with meaningful use criteria through testing and attestations submitted by the vendors. An accrediting agency may certify EHR software for meaningful use once it has determined that an EHR program meets the standards set forth by the ONC.[11]

The majority of EHR-related enforcement activity has focused on providers, since they are the recipients of incentive payments. Providers can face liability by failing to adopt certified EHR software or by failing to implement meaningful use of such software. Providers who falsely certify their eligibility for incentive payments can be punished criminally, as evidenced by the criminal conviction of a hospital's chief financial officer for falsely certifying eligibility for meaningful use incentives.[12] More commonly, however, providers are subject to overpayment liability for meaningful use non-compliance.[13]

Meaningful use enforcement activity against IT vendors has been, to date, relatively rare. The ECW lawsuit is the first major FCA enforcement action against an EHR vendor, although other EHR vendors have faced administrative penalties for their non-conforming software.[14] The ECW settlement arguably paves the road for more FCA litigation against other EHR vendors that have engaged in questionable conduct.

The Allegations Against ECW

According to the government's complaint, ECW violated the FCA by falsely certifying that its EHR software met the certification criteria, causing its customers to obtain millions of dollars in improper meaningful use incentive payments.[15] ECW's customers—more than 850,000 users across the United States—received incentive payments from government health care payers after certifying that they adopted ECW's EHR software. Unbeknownst to ECW's customers, the software was not fully compliant with certification standards, and ECW allegedly obtained certification under false pretenses. The complaint alleges that ECW caused its users to "submit inaccurate attestation information in connection with their requests for Meaningful Use incentive payments."[16]

The government also alleged that ECW rigged its EHR software to cheat the testing performed by the accrediting agency.[17] According to the government, the software was "hardcoded" to make it seem as though it fully implemented "RxNorm," an EHR functionality mandated by ONC's certification standards.[18] Rather than programming the full RxNorm capability into its software, ECW allegedly only included 16 RxNorm codes knowing that the accrediting organization would only test for these codes. By designing the EHR software to pass the test, it obtained certification despite its failure to fully integrate RxNorm capability, the government alleged.

ECW also was accused of making false attestations to the accrediting organization concerning the software's adherence to specific certification criteria. While certain software features, such as RxNorm, are tested by the accrediting body, other certification criteria may be verified through attestations from the vendor.

ECW's software allegedly was certified based on false attestations from ECW's employees, who according to the government, knew that the EHR program did not fully adopt the features required for certification. For instance, ECW falsely represented that its software implemented the required audit log functionality. However, the audit log features failed to accurately record vital information concerning diagnostic imaging orders, such as the names and details of ordered diagnostic procedures. ECW allegedly certified that the audit log features met meaningful use standards, even though employees and customers noted problems.[19]

Finally, the complaint alleges traditional Anti-Kickback Statute violations.[20] ECW allegedly paid kickbacks to customers to recommend its product to prospective clients through various referral programs.[21] Customers were given remuneration in exchange for referring leads to ECW or for convincing other providers to purchase the EHR software. The complaint also alleges that ECW gave certain influential customers remuneration in the form of consulting fees, gift cards, electronic devices, meals, travel reimbursement, and entertainment benefits. The payments allegedly were provided to customers to induce the referrals of new business to ECW, while "consulting" and "speaker" fees were provided to "influential users who promoted its software."[22]

Yates Memorandum in Action

The settlement demonstrates the DOJ's continuing commitment to its policy of seeking individual accountability for FCA violations. The "Yates Memo," formally called the Individual Account-

ability Policy,[23] is DOJ's blueprint for culpable individuals when settling white collar fraud-related cases. Under the terms of ECW's settlement agreement, the Chief Executive Officer, Chief Medical Officer, and Chief Operating Officer agreed to be jointly and severally liable along with ECW for payment of $154.92 million. Furthermore, three lower-level employees also agreed to payments as part of the settlement for their role in the alleged misconduct. While it is not surprising that the DOJ continues to seek individual accountability for C-suite executives, the ECW settlement shows that the DOJ also will target lower-level employees whom it deems responsible for an organization's misconduct.

Lessons Learned and Outlook

The ECW settlement should be a wake-up call for software vendors. While regulators have stated that they do not plan to punish ECW customers who unknowingly filed the false claims based upon ECW's conduct and received federal incentive payments through EHR Incentive Programs,[24] it seems likely that the DOJ will probe more EHR vendors.[25] In turn, health care-related IT vendors should expect more FCA scrutiny in the coming years.

Vendors should be proactive in resolving EHR certification deficiencies and implementing compliance programs focused on preventing, detecting, and correcting these issues. The innovative CIA between ECW and the Department of Health and Human Services Office of Inspector General can serve as a reference when establishing or revising compliance policies and vendors should consider implementing safeguards including:

- Incorporating ONC and other industry software standards into an organization's monitoring and auditing functions;
- Developing quality assurance programs that focus on proactively monitoring software deficiencies and their root causes;
- Promptly notifying customers of patient safety, certification, and other urgent issues;
- Organizing interdisciplinary teams focusing on EHR usability, patient safety, and EHR certification compliance issues;
- Establishing a compliance officer, a well-funded compliance program, and a process to address compliance-related issues; and
- Engaging a third-party software quality oversight consultant to review the adequacy of the vendor's internal systems and to identify and address potential issues.

The ECW settlement leaves many unresolved questions, such as what degree of non-compliance is required to establish an FCA violation and whether a health-care related customer can be held responsible for knowingly using defective software. While materiality was stipulated in the ECW settlement agreement, there may be other IT related problems that are not material to the government's decision to make payments. For instance, courts have previously dismissed FCA actions based solely on technical EHR compliance violations.[26] Many areas are ripe for future litigation in this new and emerging area.

1 *See* Press Release, U.S. Dept. of Justice, District of Vermont, Electronic Health Records Vendor to Pay $155 Million to Settle False Claims Act Allegations (May 31, 2017), *available at* https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.

2 *United States ex rel. Delaney v. EClinical Works, LLC*, No. 2:15-CV-00095 (D. Vt. May 12, 2017), Complaint in Intervention at ¶ 10, (hereinafter, DOJ Complaint).

3 31 U.S.C. § 3729(a)(1)(A) & (B).

4 U.S. Dep't of Justice, Press Release, Justice Department Recovers Over $4.7 Billion From False Claims Act Cases in Fiscal Year 2016 (Dec. 14, 2016), *available at* https://www.justice.gov/opa/pr/justice-department-recovers-over-47-billion-false-claims-act-cases-fiscal-year-2016.

5 *United States ex rel. Schwedt v. Planning Research Corp.*, 59 F.3d 196, 199 (D.C. Cir. 1995).

6 *Id.*

7 42 U.S.C. §§ 300jj *et seq.*

8 *See* 42 C.F.R pt. 495; 75 Fed. Reg. 44314 (July 28, 2010); 77 Fed. Reg. 53967 (Sept. 4, 2012); 80 Fed. Reg. 62762 (Oct. 16, 2015).

9 45 C.F.R. pt. 170; 76 Fed. Reg. 1261, at 1271 (Jan. 7, 2011).

10 *Id.*

11 76 Fed. Reg. at 1277.

12 *See, e.g.*, .U.S. Dep't of Justice E.D. Tex., Press Release, Former Hospital CFO Charged With Health Care Fraud (Feb. 6, 2014), *available at* https://www.justice.gov/usao-edtx/pr/former-hospital-cfo-charged-health-care-fraud.

13 *See* 42 C.F.R. § 495.316.

14 In 2013, the Department of Health and Human Services (HHS) decertified EHR systems created by two vendors, finding their IT products were not compliant with certification standards (HHS, Press Release, Certification for Electronic Health Record Product Revoked (Apr. 25, 2013)).

15 DOJ Complaint at ¶ 4.

16 *Id.* at ¶ 78.

17 *Id.* at ¶ 38.

18 Certified EHR must be able to generate and transmit prescriptions electronically through the use of "RxNorm," a standardized drug vocabulary that
specifies drug names, formulations, and dosage. RxNorm is essential in ensuring accuracy of electronic prescriptions and for allowing different EHR systems to communicate and interact, so as to identify possible adverse drug interactions. *See* 45 C.F.R. § 170.314(b)(3).

19 DOJ Complaint at ¶ 65.

20 42 U.S.C. § 1320a-7b(b). AKS violations are per se violations of the FCA.

21 DOJ Complaint at ¶ 79.

22 *Id.* at ¶ 83.

23 Memorandum from DAG Sally Quillian Yates, *Individual Accountability for Corporate Wrongdoing* (Sept. 9, 2015), *available at* http://www.justice.gov/dag/file/769036/download. *See also* https://www.justice.gov/dag/individual-accountability.

24 T. Sullivan, *CMS won't punish eClinicalWorks customers for meaningful use EHR attestations*, HealthCareITNews (Jul. 6, 2017), *available at* http://www.healthcareitnews.com/news/cms-wont-punish-eclinicalworks-customers-meaningful-use-ehr-attestations.

25 T. Sullivan, *DOJ will probe more EHR vendors for false claims, sources say*, HealthCareITNews (Jun. 2, 2017), *available at* http://www.healthcareitnews.com/news/doj-will-probe-more-ehr-vendors-false-claims-sources-say.

26 *See, e.g., United States ex rel. Sheldon v. Kettering Health Network*, 816 F.3d 399, 410 (6th Cir. 2016) (holding that security breaches of health IT data do not alone render a false meaningful use certification by a provider).

Resource Corner

New Publication

Medicare Exhaustion: Analysis of the Burgeoning Issue of Whether Providers Must Exhaust Administrative Remedies When Suing MAOs

This Briefing examines recent conflicting court decisions on the issue of whether providers bringing claims against Medicare Advantage Organizations must first exhaust administrative remedies.

Access this Briefing at https://www.healthlawyers.org/HCLLMedicareExhaustionBriefing.

Join the Alternative Dispute Resolution Affinity Group

About the ADR AG

The Alternative Dispute Resolution Affinity Group (ADR AG) provides a forum to network and educate members regarding legal developments and best practices in addressing conflicts within the health care system. The ADR AG assists members who participate in arbitration, mediation, and peer review hearings as an advocate and/or as a neutral as well as those who assist health care organizations in managing internal conflicts and preventing litigation.

How to Join the ADR AG

To enroll in the ADR AG, please contact the Member Satisfaction Center at msc@healthlawyers.org or (202) 833-1100, #2. Membership in the ADR AG is free to all members of the Health Care Liability and Litigation and Post-Acute and Long Term Services Practice Groups as well as government, academic, and student members, and those that have paid for all-PGs access (PG 15). Please note that you must be a member of one of these groups to join.

HEALTH CARE LIABILITY AND LITIGATION PRACTICE GROUP LEADERSHIP

PUBLISHING STAFF

Cynthia Conner
Vice President of Publishing
(202) 833-0755
cconner@healthlawyers.org

Bianca Bishop
Senior Managing Editor
(202) 833-0757
bbishop@healthlawyers.org

Lisa Salerno
Senior Legal Editor
(703) 489-8426
lsalerno@healthlawyers.org

Matt Ausloos
Publishing Administrator
(202) 833-6952
mausloos@healthlawyers.org

DESIGN STAFF

Mary Boutsikaris
Creative Director
(202) 833-0764
mboutsik@healthlawyers.org

Jen Smith
Graphic Designer/ Administrator
(202) 833-0781
jsmith@healthlawyers.org