2018

The Computer Made Me Do It: Is There a Future for False Claims Act Liability Against Electronic Health Record Vendors?

Deborah R. Farringer
Belmont University - College of Law

THE COMPUTER MADE ME DO IT: IS THERE A FUTURE FOR FALSE CLAIMS ACT LIABILITY AGAINST ELECTRONIC HEALTH RECORD VENDORS?

Deborah R. Farringer*

> *"The time has come to put the medical clipboard out of business and replace it with the computer. In doing so, we can transform our health care system so that we achieve fewer medical mistakes, lower costs, better care, and less hassle. We all agree transformation must take place; now let's all agree to work together to do it. An entrepreneur I admire said, 'There are three ways to handle change. You can fight it and die; accept it and survive; or, lead it and prosper.' This is the United States of America. I say, let's lead and prosper."*
>
> - *Mike Leavitt, U.S. Department of Health and Human Services Secretary*[1]

TABLE OF CONTENTS

---

* Deborah R. Farringer is an Assistant Professor of Law at Belmont University College of Law in Nashville, TN. J.D., Vanderbilt University Law School; B.A., University of San Diego. I would like to thank my research assistant Andy Goldstein for his work and help in bringing this article to fruition. Thanks also to Christopher Kelly and all of the editorial staff at the Nevada Law Journal for their very helpful suggestions and edits to this article. Finally, thank you to my husband and children for their patience with me through this process.

[1] Mike Leavitt, U.S. Dep't. of Health and Human Servs. Sec'y, Speech at the Health Information and Management System Society Conference (Jun. 6, 2005), http://www.providersedge.com/ehr_news_views_quotes.htm [https://perma.cc/5Q7H-L88J].

INTRODUCTION

Since the advent of the movement toward the use of electronic health records (EHRs), an axiom in the promotion of EHRs has been the idea that the use of EHRs will reduce medical errors.[2] Certainly, there are countless examples of how technology can improve the health care experience and aid providers in reducing medical errors, including errors of medication administration, medication management, access to decision support tools, telemedicine, immediate access to diagnostic tests and other clinical information and treatment results—just to name a few.[3] Even with such improvements, however, EHRs have not entirely eliminated medical errors, and new technology has in fact created its own challenges and issues that might lead to liability in a different way.[4] As the use of EHRs proliferates, so too does the reliance of healthcare workers on the systems themselves and the inevitable blame game wherein an individual claims that whatever errors occurred were the result of "the computer" or the "system" that dictated the manner in which the care was provided or the manner in which the services were reimbursed.[5] Ultimately, this "blame game" leads all to ask the question—whose fault is that? Can one blame the EHR vendor? To the extent that the answer may in fact be, "Yes," and the EHR vendor is at fault, are such claims easy to maintain? Historically, providers and other purchasers of EHRs have had little leverage against EHR vendors. One of the primary challenges arises out of the contract between the provider-purchaser and the EHR vendor.[6] Ultimately, the purchase or licensing of an EHR system is actually just the purchase or licensing of software and, as such, the contracts resemble standard software licensing agreements, replete with disclaimers of

---

[2] *See* Nicolas P. Terry, *An eHealth Diptych: The Impact of Privacy Regulation on Medical Error and Malpractice Litigation*, 27 AM. J.L & MED. 361, 376 (2001) (citing a 2001 report issued by the Committee on the Quality of Health Care in American that noted, "IT has enormous potential to improve the quality of health care. . . . In the area of *safety*, there is growing evidence that automated order entry systems can reduce errors in drug prescribing and dosing. . . . There are many opportunities to use IT to make care more *patient-centered*. . . .").

[3] *Id.*; *see also* John W. Hill et al., *Law, Information Technology, and Medical Errors: Toward a National Healthcare Information Network Approach to Improving Patient Care and Reducing Malpractice Costs*, 2007 U. ILL. J.L., TECH. & POL'Y 159, 162 (2007).

[4] *See* Hill, *supra* note 3, at 213 (noting that questions remain regarding legal responsibility for maintaining up to date EHRs, ensuring information is true and correct, deciding which provider should take action if a medical-threat is identified in the record, etc.).

[5] *See* Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKELEY TECH. L.J. 1523, 1537–55 (2009) (highlighting risks of EHR systems due to challenges related to operation of systems, reliance on others' diagnosis and treatment decisions, input errors such as cut and paste functions, decision support challenges, responsiveness, patient access, and product defects).

[6] *Id.* at 1554.

implied and express warranties and "hold-harmless" or indemnification clauses that protect the vendor from third party liability.[7] Recent litigation—including one particular case involving the federal government's allegations of fraud—has started to erode the disconnect between the potential responsibility of the EHR vendor and the ability to hold the vendor actually liable for its actions related to its software.

On May 31, 2017, the United States Department of Justice (DOJ) entered into a $155 million settlement with eClinicalWorks (eCW), one of the nation's largest electronic health records vendors,[8] to resolve a False Claims Act[9] (FCA) lawsuit in which the DOJ alleged that eCW caused the submission of false claims for federal incentive payments made under the Electronic Health Records (EHR) Incentive Program.[10] This settlement is unique not only because of the rarity of settlements or judgments against an entity based on an allegation that the falsity was in causing *another* to submit a false claim—as opposed to an action against an entity that has falsely filed its own claim and received payment directly[11]—but also because it is one of the first of its kind against an

---

[7] *Id.*; *see also* Deborah R. Farringer, *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals*, 40 SEATTLE U. L. REV. 937, 972 (2017) (citing Lisa Schencker, *EHR Safety Goes to Court*, MOD. HEALTHCARE (June 25, 2016), www.modernhealthcare.com/article/20160625/MAGAZINE/306259982 [https://perma.cc/75TP-NHDE]).

[8] *See* OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., QUICK-STATS: CERTIFIED HEALTH IT DEVELOPERS AND EDITIONS REPORTED BY AMBULATORY PRIMARY CARE PHYSICIANS, MEDICAL AND SURGICAL SPECIALISTS, PODIATRISTS, OPTOMETRISTS, DENTISTS, AND CHIROPRACTORS PARTICIPATING IN THE MEDICARE EHR INCENTIVE PROGRAM, HEALTH IT DASHBOARD (July 2017) [hereinafter QUICK STATS], https://dashboard.healthit.gov/quickstats/pages/FIG-Vendors-of-EHRs-to-Participating-Professionals.php [https://perma.cc/UY94-EC5B].

[9] 31 U.S.C. § 3729 (2012).

[10] Press Release, U.S. Dep't of Justice, Electronic Health Records Vendor to Pay $155 Million to Settle False Claims Act Allegations (May 31, 2017) [hereinafter Press Release], www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations [https://perma.cc/L474-T6JG]. The settlement also resolved allegations that eCW paid kickbacks to certain customers in exchange for such customers promoting eCW products. *Id.*

[11] 31 U.S.C. § 3729(a)(1)(A)–(B). Under both clauses of the False Claims Act, it is a violation for an entity that contracts with or submits claims directly to the government to knowingly present a false or fraudulent claim or knowingly make or use a false record or statement. It is also a violation of both clauses if an entity that does not itself directly contract with or directly submit claims to the United States government nevertheless causes a false or fraudulent claim to be presented or causes another to cause to be made a false record or statement material to a false claim. While claims against entities that directly contract with or submit claims to the federal government are common, there are far fewer cases that involve application of provisions under these two sections of the False Claims Act that rely on causing another entity to submit a false claim or record. *See infra* notes 25–28.

EHR vendor.[12] Following this case, many are wondering whether this settlement with eCW stands alone as an example of the government simply snaring one "bad actor,"[13] or if this settlement is indicative of what might lie ahead for EHR vendors under the FCA. Will the FCA be a new tool under which EHR vendors are going to be held responsible for the role that their software might play in the delivery of care or the billing and collection of services rendered? Indeed, many in the information technology industry took note of this settlement and have speculated that this may not be a singular incident.[14] Farzad Mostahsari—former National Coordinator for Health IT—stated, "Let me be plain-spoken. eClinicalWorks is not the only EHR vendor who flouted certification/misled customers. Other vendors better clean up."[15]

Is Mr. Mostahsari correct and this could be a sign of things to come if EHR vendors are not careful about their actions? This Article will examine the existing eCW settlement agreement, along with other case law against EHR vendors, to determine whether this settlement is simply an outlier among FCA cases, meant only to punish particularly egregious behavior, or the beginning of a new era of FCA activity akin to other industries, like the pharmaceutical industry. Part I of this Article will provide a brief history of the FCA and the instances in which the DOJ has utilized provisions under the law against entities that or individuals who *cause another* to submit a false claim or make a material, false record. It will further review the types of cases outside of the FCA context that have been filed against EHR vendors since providers began more widespread adoption of EHR systems, especially after the enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH) and the EHR Incentive Program.[16] Part II will then study the eCW

---

[12] *See* Arthur Allen, *Feds Levy $155M Fine Against Software Vendor for Faulty Patient Records*, POLITICO (May 31, 2017, 6:56 PM), www.politico.com/story/2017/05/31/health-records-faulty-software-239004 [https://perma.cc/F4AX-KE6F].

[13] More precisely, it could be argued that the government snared several bad actors because the settlement was not only a settlement with eCW, but also with three of eCW's founders: the Chief Executive Officer, Girish Navani; Chief Medical Officer, Rajesh Dharampuriya, M.D.; and Chief Operating Officer, Mahesh Navani, all of whom were found jointly and severally liable. Additionally, a developer settled separately for $50,000 and two project managers settled separately for $15,000 each. Press Release, *supra* note 10.

[14] *See* Allen, *supra* note 12; *see also* Heather Landi, *What Are the Potential Ripple Effects of the eClinicalWorks Settlement?*, HEALTHCARE INFORMATICS (June 14, 2017), https://www.healthcare-informatics.com/print/article/what-are-potential-ripple-effects-eclinicalworks-settlement [https://perma.cc/Q2MH-6JUP].

[15] *See* Landi, *supra* note 14 (quoting Mostashari's post on his Twitter account in response to the eCW settlement).

[16] The HITECH Act was established under the American Recovery and Reinvestment Act of 2009 in Division A, Title XIII. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (codified as amended in scattered sections of 42 U.S.C. (2009)). The EHR Incentive Program was established under this law. *Id.* at § 3000. For further discussion on the EHR Incentive Program and its involvement in the spread of the use of EHRs, see *infra* notes 101–16.

case in more detail, examining the actions that led to the settlement and determine whether such actions are an indication of a new era of FCA cases and EHR vendor liability. Part II will additionally examine existing case law against EHR vendors to determine whether any patterns can be gleaned from the cases that will predict the continued use of the FCA as an enforcement tool against EHR vendors. In Part III, this Article will argue that, although the eCW case is based on unique facts, it is likely that EHR vendors will face other FCA cases as the healthcare industry places increasing responsibility and reliance on electronic systems. These suits will likely include allegations of fraud arising not only out of the EHR Incentive Program but also the submission of claims more generally. Unlike in other FCA cases involving entities that do not contract directly with the federal government, however, it is unlikely that the federal government will be able to realize as much success or generate the same type of monetary rewards against EHR vendors as it has against the pharmaceutical industry because of the distinctions between these two disparate sectors of the health care industry. Finally, the Article will conclude by providing some thoughts on the impact of the eCW settlement agreement, which puts the EHR industry on notice regarding the potential for future liability.

I. BACKGROUND

A. *History of the False Claims Act*

Enacted in 1863 and often referred as "Lincoln's Law," the FCA was originally designed to incentivize private individuals to assist the federal government—then, more accurately, the Union Army[17]—by filing claims on behalf of the government against entities or individuals who are suspected of defrauding the government.[18] While application of the statute has waned and surged over the years based on various changes and amendments, the FCA has become one of the federal government's most effective enforcement tools against fraud.[19] One of primary reasons that use and application of the FCA tends to swell is due to adjustments to the percentage of amounts given to so-called *qui tam* re-

---

[17] James B. Helmer, Jr., *False Claims Act: Incentivizing Integrity for 150 Years for Rogues, Privateers, Parasites and Patriots*, 81 U. CIN. L. REV. 1261, 1264–66 (2013).

[18] *See* United States *ex rel.* Graber v. City of New York, 8 F. Supp. 2d 343, 352 (S.D.N.Y. 1998).

[19] *See* Press Release, U.S. Dep't of Justice, Justice Department Celebrates 25th Anniversary of False Claims Act Amendments of 1986 (Jan. 31, 2012), www.justice.gov/opa/pr/justice-department-celebrates-25th-anniversary-false-claims-act-amendments-1986 [https://perma.cc/AJZ3-9D6F] ("The False Claims Act has been called the single most important tool that American taxpayers have to recover funds when false claims are made to the federal government, including health care fraud, mortgage fraud, and procurement fraud. 'In the last quarter century, the False Claim Act's success has been unparalleled with more than $30 billion dollars recovered since it was amended in 1986 and $8.8 billion since January 2009,' said Attorney General Eric Holder.").

lators or whistleblowers.[20] The recent increased application of the FCA began with amendments enacted in 1986 and its use against health care companies was further bolstered as a result of certain DOJ pleading strategies that enabled the *qui tam* relator to allege not only violations of the FCA,[21] but also violations of the federal Anti-kickback Statute ("AKS")[22] and federal Physician Self-Referral Law (known as the "Stark Law").[23] What this means for purposes of recovery is that if the government or *qui tam* relator is successful with the claim, the government and relator will be able to recover *all* of the following as damages: (a) all amounts paid in error by the government pursuant to each false claim submitted; (b) the imposition of fines ranging between $10,781.41–$21,562.80 per claim submitted; (c) treble damages based on the total amount of improperly paid claims; (d) and any additional penalties that would be assessed for violations of the underlying AKS or Stark Law claim in the amount of $21,916 per claim and at least $24,253 per claim, respectively.[24] Given that

---

[20] 31 U.S.C. § 3730(b) permits private individuals, known as *qui tam* relators, to bring a civil action for a violation of 31 U.S.C. § 3729 on behalf of such individuals and the United States Government. The individual who files the claim, subject to certain restrictions and limitations, receives a portion of the proceeds of any judgment or settlement. 31 U.S.C. § 3730(d) (2012). The amount of the award is dependent on whether the government intervenes in the case. If the government intervenes, the *qui tam* relator receives between fifteen and twenty-five percent, and if the government does not intervene, then the relator receives between twenty-five and thirty-five percent. § 3730(d)(1)–(2).

[21] Beginning in the 1990s, the DOJ and other whistleblowers began alleging violations of the FCA based on violations of the AKS and the Stark Law. *See* United States *ex rel.* Thompson v. Columbia/HCA Healthcare Corp., 20 F. Supp. 2d 1017, 1037–38 (S.D. Tex. 1998); United States *ex rel.* Pogue v. Am. Healthcorp, Inc., 914 F. Supp. 1507, 1509 (M.D. Tenn. 1996) (noting that a number of cases have recently begun to allege that violations of the AKS or the Stark Law constitute violations of the FCA). With amendments to the AKS under the Patient Protection and Affordable Care Act (ACA), a violation of the AKS is now—statutorily—a violation of the FCA. 42 U.S.C. § 1320a-7b(g) (2012). Because the Stark Law is a strict liability statute and does not contain the same scienter requirements of the AKS and the FCA, it is still possible to maintain an FCA claim based on allegations of the Stark Law, but it is necessary to prove that such violation was knowing and willful, in order to satisfy the scienter requirements, set forth under the FCA. *See* United States *ex rel.* Kosenske v. Carlisle HMA, Inc., No. 1:05-CV-2184, 2010 WL 1390661, at *7–9 (M.D. Pa. Mar. 31, 2010).

[22] The federal Antikickback Statute imposes penalties against "knowingly and willfully [offering or paying] any remuneration (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in kind . . . [in return for referring] an individual to a person for the furnishing or arranging for the furnishing of any item or service for which payment may be made in whole or in part under a Federal health care program. . . ." 42 U.S.C. § 1320a-7b(b)(2).

[23] The Stark Law prohibits a physician (or the physician's immediate family member, as defined in the statute) from making referrals for certain services known as "designated health services" to any entity with which the physician has a "financial relationship." 42 U.S.C. § 1395nn(a)(1) (2012).

[24] 31 U.S.C. § 3729(a)(1)(G) (2012). Penalties under the AKS and the Stark Law also require that any amounts paid in error are reimbursed and then each law imposes civil monetary penalties for violations of each statute. *See* 28 C.F.R. § 85.3(a)(13) (2000); Civil Mone-

each service rendered to a patient constitutes a claim, it is the magnitude and scope of the damages that have made the FCA such a powerful tool.[25] Many entities have learned first-hand how devastating this ability to assess multiple damages can be and thus the potential ramifications of facing such large fines and penalties have resulted in entities engaging in settlement on a widespread basis when faced with potential FCA claims.[26]

Although the bulk of FCA claims are made against providers and other entities who directly submit claims to federal healthcare programs,[27] there has been an increasing use of the FCA against entities that do not themselves submit claims directly to the government, but rather cause others to submit claims, such as pharmaceutical companies and device manufacturers.[28] This theory of liability is typically referred to as the "inducement-of-fraud" theory[29] because it attaches liability to the entity that knowingly causes another entity or individual to submit a false or fraudulent claim.[30] The ability to impose substantial penalties against these particular entities is especially impactful because the FCA has the available tools to impose damages large enough to be noticed in a billion-dollar industry.[31] In fact, to date, the largest settlement in the history of the FCA is a settlement with pharmaceutical manufacturer GlaxoSmithKline (GSK) regarding allegations that GSK unlawfully promoted certain prescription drugs, failed to report certain safety data, and engaged in false price reporting

---

tary Penalties Inflation Adjustment, 81 Fed. Reg. 42,491 (Jun. 30, 2016) (to be codified at 28 C.F.R. pts. 20, 22, 36, 68, 71, 76, 85).

[25] Joan H. Krause, *Health Care Providers and the Public Fisc: Paradigms of Government Harm Under the Civil False Claims Act*, 36 GA. L. REV. 121, 124 (2001).

[26] Perhaps the most public cautionary tale involved Tuomey Healthcare System in South Carolina that was involved in an FCA suit alleging submissions of false claims as a result of Stark Law violations. The Stark Law violations against Tuomey involved 21,730 false claims and thus the damages were a total of $237,454,195 ($39,313,065 in actual damages, $119,515,000 in civil monetary penalties, and $78,626,130 in punitive damages). *See* United States *ex rel*. Drakeford, M.D. v. Tuomey Healthcare Sys., Inc., 792 F.3d 364, 370, 389 (4th Cir. 2015). The entity was unable to pay such a large judgment and eventually settled with the government for just over $72 million dollars. *See* Lisa Schencker, *Tuomey Will Pay U.S. $72.4 Million to Duck $237 Million False Claims Verdict*, MODERN HEALTHCARE (Oct. 16, 2015), www.modernhealthcare.com/article/20151016/NEWS/151019923 [https://perma.cc/U97P-T6KZ].

[27] David Kwok, *Controlling Excessive Off-Label Medicare Drug Costs Through the False Claims Act*, 27 HEALTH MATRIX 185, 215 (2017).

[28] *Id*.

[29] *See id*.; *see also* United States *ex rel*. Franklin v. Parke-Davis, 147 F. Supp. 2d 39, 49 (D. Mass. 2001). This is also sometimes referred to as "fraud in the inducement" theory. *See* Andrew E. Shipley, *Trends in False Claims Act Litigation*, *in* GOVERNMENT CONTRACTS COMPLIANCE, 49, 49 (2013).

[30] 31 U.S.C. § 3729(a)(1)(A)–(B), (G) (2012).

[31] *See* Kwok, *supra* note 27, at 215.

practices.[32] The company agreed to pay $3 billion in total, consisting of about $1 billion for criminal fines and forfeiture and $2 billion for civil liability under the FCA.[33]

While this is the largest settlement in history of the FCA and the sheer dollar amount seems potentially catastrophic, the allegations involved off-label promotion and AKS claims for multiple pharmaceutical products, including Avandia, Paxil, Wellbutrin, Advair, Zofran, Imitrex, Lotronex, Flovent, and Valtrex, for which the reported sales of such products was far more than the $3 billion settlement.[34] For example, GSK generated profits of $10.4 billion in sales from Avandia, $11.6 billion in sales of Paxil, and $5.9 billion in sales of Wellbutrin, in addition to profits from the remaining pharmaceuticals mentioned in the settlement.[35] Thus, although $3 billion is certainly a large settlement, it seems somewhat less impactful when compared to the profits generated through the sale of the products and is one of the reasons that many critics believe that even large settlements such as this one do little to actually deter behavior.[36]

GSK is not the only pharmaceutical company to have entered into a high dollar settlement regarding FCA claims.[37] Since 2009, the United States Department of Health and Human Services (HHS) has reported recovery of $19.3 billion in FCA settlements and judgments relating to health care fraud.[38] In a published report, the largest six settlements were with pharmaceutical companies, including the previously noted GSK settlement and major settlements with Pfizer, Inc. ($2.3 billion), Johnson & Johnson and its subsidiaries Janssen Pharmaceuticals and Scios ($2.2 billion), Abbott Laboratories ($1.5 billion), Merck Sharp & Dohme ($963 million), and a settlement with eight pharmaceu-

---

[32] Press Release, U.S. Dep't of Justice, GlaxoSmithKline to Plead Guilty and Pay $3 Billion to Resolve Fraud Allegations and Failure to Report Safety Data (July 2, 2012), www.justice.gov/opa/pr/glaxosmithkline-plead-guilty-and-pay-3-billion-resolve-fraud-allegations-and-failure-report [https://perma.cc/DLF2-T32N]. It should be noted that the $3 billion settlement involved FCA claims along with FDA claims under the Food, Drug and Cosmetic Act.

[33] *Id*. The civil liability amounts included payments to both federal and state governments.

[34] *Id*.; Katie Thomas & Michael S. Schmidt, *Glaxo Agrees to Pay $3 Billion in Fraud Settlement*, N.Y. TIMES (July 2, 2012), http://www.nytimes.com/2012/07/03/business/Glaxosmithkline-agrees-to-pay-3-billion-in-fraud-settlement.html [https://perma.cc/SQ8H-3PSE].

[35] *See* Thomas & Schmidt, *supra* note 34.

[36] *Id*. (quoting Patrick Burns, spokesperson for the whistle-blower advocacy group Taxpayers Against Fraud); *see also* Kwok, *supra* note 27, at 217–18 ("[I]f there is concern that sanctions are too great or improperly calculated, it is important to note that the prevalence of off-label promotion cases suggests that manufacturers are not deterred by FCA sanctions.").

[37] U.S. DEP'T OF JUST., SIGNIFICANT FALSE CLAIMS ACT SETTLEMENTS & JUDGMENTS, FISCAL YEARS 2009–2016 (2016) [hereinafter SETTLEMENTS & JUDGMENTS], https://www.justice.gov/opa/press-release/file/918366/download [https://perma.cc/VPQ6-XYBP].

[38] *Id*.

tical manufacturers ($900 million).[39] Device manufacturers have also faced high dollar settlements under the inducement-of-fraud theory in a similar manner to pharmaceutical manufacturers, such as the settlement with Olympus Corporation of the Americas, the leading endoscope distributor, for $646 million, and Quest Diagnostics Inc., a manufacturer of diagnostic test kits, for $302 million.[40]

Despite the large settlements that have been achieved against pharmaceutical companies and device manufacturers, the reported cases that premise the inducement-of-fraud theory of the FCA remain relatively rare.[41] While this provision of the FCA is not as frequently applied as allegations related to direct submissions, courts have affirmed the viability of these types of claims over the years.[42] Most recently reported inducement-of-fraud cases arise primarily out of Massachusetts and the First Circuit.[43] Some of this prevalence in the First Circuit may be due to the court's finding in the case of *United States ex rel. Hutcheson v. Blackstone Medical, Inc.*, which was particularly favorable to relators and prosecution in its application of the knowledge requirement under the FCA.[44] In *Blackstone Medical*, the *qui tam* relator[45] alleged that Blackstone Medical, Inc. ("Blackstone"), a manufacturer of devices used in spinal surger-

---

[39] *Id.* The settlement with eight pharmaceutical manufacturers involved allegations that the manufacturers knowingly reported inflated drug prices that cause providers to submit inflated claims. It involved Abbott Laboratories, B. Braun Medical Inc., Roxane Laboratories, Par Pharmaceutical Inc., Watson Pharmaceuticals Inc., Sandoz, Inc., and Mylan Inc. *Id.*

[40] *Id.*

[41] Joan H. Krause, *Truth, Falsity, and Fraud: Off-Label Drug Settlements and the Future of the Civil False Claims Act*, 71 FOOD & DRUG L.J. 401, 425–26 (2016) (describing the challenge of the bringing these types of claims and the frequency of settlements).

[42] United States *ex rel.* Marcus v. Hess, 317 U.S. 537, 544 (1943) (holding that "causing to be presented" provisions under the FCA "indicate a purpose to reach any person who knowingly assisted in causing the government to pay claims which were grounded in fraud. . . .").

[43] While cases in jurisdictions other than the First Circuit have involved FCA allegations premised on one party causing another to submit a false claim, the large majority have arisen out of the First Circuit. *See, e.g.*, United States *ex rel.* Brown v. Celgene Corp., 226 F. Supp. 3d 1032 (C.D. Cal. 2016); United States *ex rel.* Kroening v. Forest Pharmaceuticals, Inc., 155 F. Supp. 3d 882 (E.D. Wis. 2016); United States *ex rel.* Nevyas v. Allergan, Inc., No. 09-432, 2015 WL 4064629 (E.D. Pa. July 2, 2015); United States *ex rel.* Solis v. Millennium Pharmaceuticals, Inc., No. 2:09-cv-03010-MCE-EFB, 2015 WL 1469166 (E.D. Cal. Mar. 30, 2015); United States *ex rel.* Tran v. Computer Sciences Corp., 53 F. Supp. 3d 104 (D.D.C. 2014); United States *ex rel.* Webb v. Miller Family Enterprise, No. 1:13-cv-00169-DBH, 2014 WL 6611012 (D. Me. July 2, 2014); United States *ex rel.* Ruscher v. Omnicare, Inc., No. 4:08-cv-3369, 2014 WL 2618158 (S.D. Tex. June 12, 2014); United States v. Villaspring Health Care Center, Inc., No. 3:11-43-DCR, 2011 WL 6337455 (E.D. Ky. Dec. 19, 2011).

[44] *See* United States *ex rel.* Hutcheson v. Blackstone Medical, Inc., 647 F.3d 377, 389 (1st Cir. 2011).

[45] The Department of Justice declined to intervene in the case, however, it did support the relator as an amicus in the district court and on appeal. *Id.* at 378–79.

ies,[46] paid kickbacks to physicians in the form of consulting agreements, development projects, research grants, and royalties (all of which were sham arrangements), and in the form of exorbitant entertainment expenses, high-end travel arrangements, and speaking engagements, all to induce the physicians to utilize Blackstone products during surgery.[47] While the key issue in the case was whether the *qui tam* relator was able to show that the alleged false claims, which were based on an implied false certification theory,[48] were material,[49] the court also explored the question of whose knowledge of the falsity was required to prove an FCA claim in this instance.[50] Blackstone argued that it had not violated the FCA because the hospital submitting the claim had no knowledge that the claims were false at the time of submission.[51] The court rejected this position, however, finding that the mere fact that the FCA includes "caused to be presented" as part of what may constitute a false claim implies that the knowledge requirement under the statute is applied to the party that "causes" the submission and not the party actually submitting the claim.[52] Thus, under First Circuit precedent, if an FCA action is brought against a party based on that party causing another to submit a false claim, it is sufficient that the entity causing the claim to be submitted do so "knowingly."[53]

---

[46] *Id.* at 378.

[47] *Id.* at 380–81.

[48] Many FCA cases are filed based on the theory of false certification; that is, the theory that the falsity of the claim rests not in false factual information that has been misrepresented in the claim (*e.g.*, submission of a claim for a service that was never rendered), but instead in falsity as it relates to legal compliance (e.g., submission of a claim for a service that had certain legal preconditions and such legal preconditions were not met). *See* Joan H. Krause, *Reflections on Certification, Interpretation, and the Quest for Fraud that "Counts" Under the False Claims Act*, 2017 U. ILL. L. REV. 1811, 1817–18 (2017). At the time of this case, courts were divided on whether one could sustain an FCA claim based on an allegation that submission of the claim *implied* certification with an underlying law or regulation, otherwise known as an implied false certification. *See Blackstone Medical, Inc.*, 647 F.3d at 387. When this case was decided, whether the implied false certification theory of liability was viable was a matter of first impression for the First Circuit. *Id.* The court held that the implied false certification theory was a viable theory of liability, but rejected rigid framework that had been applied previously in other circuits. *Id.* at 379–80.

[49] *Id.* at 394–95. The court found the claims were not material because while the physicians were induced to use Blackstone products, they were not induced to submit medically unnecessary claims and thus the services themselves (and the claims) were properly rendered, regardless of the medical device that was utilized for the surgery.

[50] *Id.* at 393.

[51] *Id.* at 389–90. Blackstone argued that a claim can only be false if it fails to comply with an express requirement of a statute and, as such, the hospital needs to be aware that the claims were false because an implied false certification claim cannot be sustained based on the representation of the non-submitting entity alone.

[52] *Id.* at 382, 390.

[53] 31 U.S.C. § 3729(b)(1) (2012) (defining "knowing" and "knowingly" as "actual knowledge of the information," "deliberate ignorance of the truth or falsity of the information" or "reckless disregard of the truth or falsity of the information").

Courts in a few other circuits have echoed this position. A District of Columbia district court described various instances in which these "caused to be submitted" provisions have been utilized in the past, setting forth the paradigmatic case as "when the non-submitting party takes advantage of an unwitting intermediary, thereby causing that party to submit a false claim."[54] The *Blackstone Medical* case is a good example of this type of situation: the hospital submitted claims for drugs or medical devices entirely unaware that the pharmaceutical company or device manufacturer was paying illegal kickbacks to physicians on its medical staff.[55] The D.C. court went on to state that these types of claims are also actionable (a) if one can prove that the non-submitter was the "driving force behind an allegedly fraudulent scheme,"[56] (b) when the non-submitting party "caused the presentation of false claims where they had agreed to take certain critical actions in furtherance of the fraud,"[57] or even when the "non-submitter continued to do business with an entity upon becoming aware that that entity was submitting false claims."[58] The court thus concluded that liability of a non-submitting party is determined by the "degree to which that party was involved in the scheme that results in the actual submission."[59]

Despite this rather expansive view of liability and the typically exorbitant settlement amounts that the government has been able to achieve against pharmaceutical companies and some device manufacturers, cases premised on the inducement-of-fraud theory remain relatively rare.[60] It is difficult to glean whether similar claims could be as successful in other contexts, in part because of the disconnect between the settlement amounts the government has realized under the FCA and the profits the companies have generated by the sale of certain drugs.[61] As mentioned above, while settlements between pharmaceutical companies and the DOJ are some of the largest settlements in the history of the FCA, many companies view any payments required to settle allegations worth the benefit realized by incentivizing physicians to prescribe the drugs.[62] Given the vast distinctions in the profit margin, product offering, and marketing tactics between the EHR industry and the pharmaceutical industry, it is not entire-

---

[54] United States *ex rel.* Tran v. Computer Sciences Corp., 53 F. Supp. 3d 104, 126 (D.D.C. 2014).

[55] *Blackstone Medical, Inc.*, 647 F.3d at 389.

[56] *Computer Sciences Corp.*, 53 F. Supp. 3d at 127 (citing United States v. Toyobo Co, Ltd., 811 F. Supp. 2d 37, 48 (D.D.C. 2011)).

[57] *Id.* (citing United States *ex rel.* Sikkenga v. Regence Bluecross Blueshield of Utah, 472 F.3d 702, 715 (10th Cir. 2006)).

[58] *Id.* (citing United States *ex rel.* Long v. SCS Bus. & Technical Inst., 999 F. Supp. 78, 91 (D.D.C. 1998)).

[59] *Id.*

[60] *See* Krause, *supra* note 41, at 425–26.

[61] *See* Kwok, *supra* note 27, at 217.

[62] *See id.*

ly clear whether application of the fraud in the inducement theory will realize success against EHR vendors in the same way as in the pharmaceutical context.

B. EHR Vendor Liability

Since the enactment of Health Insurance Portability and Accountability Act of 1996 (HIPAA)[63] and the HITECH Act,[64] health care providers have increased their use of and reliance on EHRs dramatically.[65] While, for the most part, EHRs are seen as a tool that will help the fragmented and disjointed health care system become more efficient and enable better continuity of care,[66] the increased reliance has also led to some unintended consequences.[67] Some of the challenges reported when using an electronic system include cutting and pasting into medical records leading to inaccurate charting,[68] inaccurate patient tracking or improperly prescribed medications,[69] and ransomware attacks making access to records impossible, which leads to providers having to turn away patients.[70] Even as incidents from EHRs affecting patient health and patient safety arise, the liability of the EHR vendor up to this point has been relatively elusive.[71]

---

[63] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.). HIPAA was enacted to assure that individuals could maintain health insurance between jobs and to protect the privacy and confidentiality of patient data as the health care industry began more widespread use of electronic transmission of patient data.

[64] The HITECH Act was established under the American Recovery and Reinvestment Act of 2009 in Division A, Title XIII. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (Feb. 17, 2009).

[65] *See* Farringer, *supra* note 7, at 946.

[66] *Why Adopt EHRs?*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/why-adopt-ehrs [https://perma.cc/D2H7-LTYY] (last visited Mar. 18, 2018) [hereinafter *Why Adopt EHRs*].

[67] *See* Lisa Schencker, *EHR Safety Goes to Court*, MODERN HEALTHCARE (June 25, 2016), http://www.modernhealthcare.com/article/20160625/MAGAZINE/306259982 [https://perma.cc/8TWW-Y78B].

[68] *See* Eugenia L. Siegler & Ronald Adelman, *Copy and Paste: A Remediable Hazard of Electronic Health Records*, 122 AM. J. MED. 495, 495–96 (2009); *see also* Arthur Allen, *Electronic Record Errors Growing Issue in Lawsuits*, POLITICO (May 4, 2015, 6:40 AM), https://www.politico.com/story/2015/05/electronic-record-errors-growing-issue-in-lawsuits-117591 [https://perma.cc/T8M8-7GDJ] (noting that UCLA professor of medicine, Keith Klein, decried the cut-and-paste function of EHRs because, "There are cloned records everywhere, and if you get sued, you're going to have a problem in court. . . .").

[69] *See* Schencker, *supra* note 67.

[70] *See, e.g.*, Richard Winton, *Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating*, L.A. TIMES (Feb. 18, 2016, 10:44 AM), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html [https://perma.cc/HY2M-G5HR].

[71] *See* Schencker, *supra* note 67 (noting that "EHR-related issues contributed to less than 1% of all claims closed by [Doctors Co., a malpractice insurer] during [Jan. 2007 to June 2014]").

There are a multitude of factors that have contributed to the ability of EHR vendors to escape from liability relatively unscathed up to this point. First, many of the incidents that arise out of EHR usage involve, at least at some level, human error.[72] To the extent that human error in use of an EHR factors into the injury or damages caused by its use, it is difficult to assess whether the problem is really the EHR itself or, instead, the individual's use of the EHR.[73] For example, one study identified a number of challenges that affect patient care when human error, such as incorrect user input and related dosage errors, is made in the EHR, including the fact that "[p]hysicians may fail to enter discontinuation orders for particular drugs when they change patients' medications so that the pharmacy continues to provide the old drugs as well as the new ones" or "[p]roblematic log-off procedures cause physicians to order medications on the system before the previous user has fully logged out, resulting in the wrong patient receiving the newly-ordered therapy."[74] Certainly, there are changes an EHR vendor could make to its product that would, for example, ask a follow-up question or require a box to be checked acknowledging the ordering of a new drug and the resulting discontinuation of an old drug or require a log-in confirmation prior to ordering any new therapy or medication. But, could a litigant that is potentially harmed by these errors sustain an action against the EHR vendor when much of the blame extends to its users, especially if the vendor can claim that the users were thoroughly and extensively trained on the dangers of failing to log out of the system or failing to discontinue any medications *prior* to ordering any new medications?

While there have been some successful claims based on allegations that the error was caused by an inherent flaw in the structure, design, or operation of the EHR system,[75] EHR vendors have also avoided liability through contracting practices that are commonplace in the lease or purchase of software.[76] Like most software companies, EHR vendors include onerous contractual language

---

[72] *See* Hoffman & Podgurski, *supra* note 5, at 1544.

[73] *See id.* at 1544–45 (citing various ways in which human error affects use and liability associated with EHR systems).

[74] *Id.* at 1545 (citing Ross Koppel, *Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors*, 293 J. AM. MED. ASS'N 1197, 1199–1201 (2005)).

[75] *See id.* at 1552 (noting a 2009 case involving the EHR system of the Veterans Administration in which the system exposed patients to potentially life-threatening doses of medication, had software that provided erroneous calculations of intercranial pressure, and omitted ninety-three minutes of data from an automated anesthesia record of a patient who was quadriplegic following brain surgery); *see also* Schencker, *supra* note 67 (citing a report by The Doctors Co., a physician-owned medical malpractice insurer, stating that of their ninety-seven medical malpractice claims involving EHRs, about 39 percent were allegations of injury being caused by the EHR: "10% involved a failure of system design . . . 9% involved electronic systems or technology failure . . . 7% were due to a lack of EHR alert or alarm for support . . . 6% System failure—electronic data routing . . . 4% Insufficient scope/area for documentation . . . 3% Fragmented EHR").

[76] *See* Allen, *supra* note 12.

in their user agreements, including "hold-harmless" provisions[77] and language that exempts the vendor "from most legal responsibility under a doctrine known as the 'learned intermediary.' "[78] The "learned intermediary" doctrine is generally thought of as a defense in products liability cases and states:

> [a] prescription drug or medical device is not reasonably safe due to inadequate instructions or warnings if reasonable instructions or warnings regarding foreseeable risks of harm are not provided to: [] prescribing and other health-care providers who are in a position to reduce the risks of harm in accordance with the instruction or warnings.[79]

The rationale behind the rule is that the health care provider, and not the patient, is generally the one to whom the warnings are directed, and thus the provider is the individual in the best position to assess the risks and make medical decisions regarding the product.[80] This same concept has been used in connection with EHRs—that vendors provide suggestions and recommendations, but that the physician is ultimately responsible for the actual medical care that is provided.[81] As a result, while there is no question that some EHRs will contain design flaws that medical providers—and, unwittingly, patients—will rely on to their detriment and the detriment of their patients, the widespread success of such claims has been challenging and relatively limited.[82]

Despite the relative rarity of claims against EHR vendors at present, many are predicting that the coming years likely will see an increase in claims against EHR vendors.[83] This increase may be in medical malpractice claims, but it is equally likely that many claims will be outside the malpractice context—between providers and their vendors.[84] Unlike patient-plaintiffs who face the difficult task of identifying a provider's EHR vendor and then determining whether the plaintiff's injury was the result of an EHR error or human error, or a combination of both, a provider may sue under breach of contract principles not just for design flaws that compromise patient safety, but for failure to deliver the promised product.[85] Indeed, there have been a growing number of exam-

---

[77] *See* Schencker, *supra* note 7.

[78] *See* Allen, *supra* note 68.

[79] RESTATEMENT (THIRD) OF TORTS: PRODUCT LIABILITY § 6 (AM. LAW INST. 1998).

[80] *Id.* cmt. b.

[81] *See* Hoffman & Podgurski, *supra* note 5, at 1552–54.

[82] *See* Schencker, *supra* note 7 ("EHR-related issues contributed to less than 1% of all claims closed by the malpractice insurer during that time. In that limited sample, 64% involved user errors while 42% involved issues with the EHR system itself. . . .").

[83] *See id.* ("[T]he number of such malpractice suits will likely continue to climb. Medical malpractice insurer the Doctors Co. closed 28 claims in 2013 involving EHRs, and nearly that many during the first two quarters of 2014. In all, the Doctors Co. closed 97 claims involving EHRs from January 2007 to June 2014.").

[84] Katie Bo Williams, *4 Reasons We May See More Hospitals Suing IT Vendors*, HEALTHCAREDIVE (Mar. 24, 2014), https://www.healthcaredive.com/news/4-reasons-we-may-see-more-hospitals-suing-it-vendors/241663/ [https://perma.cc/WQ6G-4QTK].

[85] *Id.*

ples of provider lawsuits, with allegations ranging from software not performing as the vendor had promised,[86] software failing to meet contractual deadlines necessary to meet federal regulation requirements,[87] software causing budget shortfalls in the billions,[88] and allegations of fraud and breach of contract in connection with errors in the EHR compromising patient safety,[89] just to name a few. It is somewhat unsurprising that these lawsuits are on the rise given how much providers spend to purchase, implement, and maintain EHR systems, which many providers did not want to transition to in the first place.[90] In 2015, *Becker's Health IT & CIO Review* reported on a few of the costly investments that large providers had made in EHR systems, which included an estimated $1.2 billion investment by Partners HealthCare in Boston, $200 million by the Lehigh Valley Health Network, and "hundreds of millions" by the Mayo Clinic.[91] Even small providers spend a large portion of their total revenue on EHR licensing, implementation, and maintenance.[92] Entities that make large invest-

---

[86] Joseph Conn, *Cerner, Trinity Reach $106M Settlement in Software Dispute*, MODERN HEALTHCARE (Mar. 7, 2014), http://www.modernhealthcare.com/article/20140307/news/303079954 [https://perma.cc/MKR4-W52C] (noting the parties settled Trinity Health's allegations that Cerner's financial software was defective causing an estimated $240 million worth of damages to Trinity's North Dakota hospital).

[87] *See* Eve Byron, *White Sulphur Springs Hospital Says Company Never Installed Health Records System*, INDEP. RECORD (Dec. 31, 2013), http://helenair.com/news/local/white-sulphur-springs-hospital-says-company-never-installed-health-records/article_cce3a646-71e3-11e3-aa07-001a4bcf887a.html [https://perma.cc/65RK-GV6Z] (noting that Mountainview Medical Center sued its EHR vendor, NextGen Healthcare Information Systems of Texas, for its failure to install a certified health record system by June 1, 2013, as necessary for the hospital to meet "meaningful use" regulations and the hospital spent over $441,000 to arrange for installment of an EHR that was not compliance with applicable federal standards).

[88] *See* Plaintiff-Appellants' Response to Petition for Discretionary Review at 7–8, Abrons Family Practice and Urgent Care, P.A. v. N.C. Dep't of Health and Hum. Servs., 792 S.E.2d 528 (N.C. Ct. App. 2016) (No. 427A16) (claiming that the State of North Carolina implemented a software system (NCTracks) for its Medicaid program that was riddled with errors, causing payments to "Medicaid providers [to be] delayed, unpaid, or shorted by over half a *billion* dollars in the first 90 days. . . .") (emphasis added).

[89] *See* Schencker, *supra* note 7 (detailing a lawsuit, which has since been settled, between PinnacleHealth and Cerner (as successor in interest to Siemens health IT business) in which Cerner sued PinnacleHealth for breach of contract when PinnacleHealth cancelled its contract and instead contracted with Epic Systems Corp., and PinnacleHealth then countersued for fraud and breach of contract alleging Cerner's product was defective and caused patient safety concerns).

[90] *See* Dawn Heisey-Grove et al., *A National Study of Challenges to Electronic Health Record Adoption and Meaningful Use*, 52 MED. CARE 144, 146–47 (2014), http://journals.lww.com/lww-medicalcare/Documents/13-00342.pdf [https://perma.cc/HKV9-MDUY].

[91] *See 8 Epic EHR Implementations with the Biggest Price Tags in 2015*, BECKER'S HEALTH IT & CIO REVIEW (Jul. 1, 2015), https://www.beckershospitalreview.com/healthcare-information-technology/8-epic-ehr-implementations-with-the-biggest-price-tags-in-2015.html [https://perma.cc/S5LY-7R5Z].

[92] *See* Schencker, *supra* note 7.

ments in IT infrastructure have an expectation that EHR systems should not only function, but function as promised and in a manner that should make clinical care easier and not harder.[93] As more and more providers spend more money implementing EHR systems per requirements under HIPAA and HITECH, their expectations for the functionality and ease of their EHR systems and responsiveness of EHR vendors increase, leading to a heightened litigious environment.

II. THE ECLINICALWORKS SETTLEMENT AND FRAUD AMONG EHR VENDORS

A. eClinicalWorks Settlement

It is with this backdrop of an increasingly litigious environment of the EHR industry that the DOJ announced its recent settlement with eCW, a leading EHR vendor,[94] for alleged violations of the FCA.[95] As news of the settlement spread across the health care industry, many have asked whether this is an indicator of what might be a new normal when it comes to EHR vendors, or if this is an isolated incident based on some specific and particularly egregious facts.[96]

The settlement resolved two alleged FCA violations: (a) that eCW paid kickbacks to certain customers in order to induce those customers to promote its product, and (b) that eCW obtained certification for its EHR software that resulted in payments to its customer-providers when the software, to the actual knowledge of eCW, did not comply with the requirements necessary for certification.[97] Although not addressed extensively in the federal government's press release about the settlement, the case initially arose out of complaints made by physicians, pharmacists, and nurses who used eCW software at the women's hospital at Rikers Island jail in New York City in 2010 and who alleged that the software was malfunctioning in a way that compromised patient safety.[98] Complaints regarding the software malfunctions were initially directed to Brendan Delaney, a former eCW employee, who worked on implementation of the EHR

---

[93] *Id.*

[94] *eClinicalWorks Holds Highest Market Share for Ambulatory Cloud-Based EHRs*, BECKER'S HEALTH IT & CIO REVIEW (Jan. 26, 2016), https://www.beckershospitalreview.com/healthcare-information-technology/eclinicalworks-holds-highest-market-share-for-ambulatory-cloud-based-ehrs.html [https://perma.cc/KC3E-R75N] (reporting that eClinicalWorks holds the highest market share of all cloud-based EHR vendors, which accounts for about ten percent of the market share).

[95] *See* Press Release, *supra* note 10.

[96] *See* Allen, *supra* note 12; *see also* Landi, *supra* note 14 ("Considering the implications of the fraud allegations, Bob Ramsey, an attorney who focuses on healthcare as a shareholder/partner at the Pittsburgh, Pa.-based law firm Buchanan, Ingersoll & Rooney, says the case should serve as a wake-up call to health IT vendors about the importance of being compliant with certification requirements.").

[97] *See* Press Release, *supra* note 10.

[98] *See* Allen, *supra* note 12.

system on Rikers Island and later at over thirty other hospitals.[99] Most of the fraud allegations initially related to patient safety issues, such as patient records that overlapped on computer screens causing confusion about a particular patient's diagnosis or prescribed drugs, errors within medication lists, and patients leaving jail without proper prescriptions or lab results.[100] The DOJ's complaint-in-intervention, however, emphasized false claims related to eCW's representations under the EHR Incentive Program as established under the American Recovery and Reinvestment Act of 2009.[101]

The EHR Incentive Program was created to spur more widespread adoption of EHRs and to incentivize Medicare and Medicaid participating providers (physicians and hospitals) to become "meaningful users" of certified EHR technology (CEHRT).[102] These incentives include both bonus payments in the initial years and then an assessment of penalties for those who fail to become "meaningful users" in later years.[103] Payments can be made under either the Medicare program or the Medicaid program, at the choice of the provider, and amounts are paid out in established time frames depending on the program.[104] The payments were maximized for those professionals who became eligible in 2011, but decreased in total payment amounts for those not becoming eligible until a later date.[105] The Medicare program requires eligible professionals to begin the incentive payments by 2014 and the Medicaid program allows eligible providers to start the program as late as 2016.[106] After the expiration of the incentive periods, eligible professionals who do not successfully demonstrate meaningful use will face payment adjustments to their Medicare reimbursements.[107]

---

[99] *Id.*

[100] *Id.*

[101] The HITECH Act was established under the American Recovery and Reinvestment Act of 2009 in Division A, Title XIII. American Recovery and Reinvestment Act of 2009, Pub.L. 111-5, 123 Stat. 115 (Feb. 17, 2009); United States' Complaint in Intervention at 1, U.S. *ex rel.* Delaney v. eClinicalWorks, LLC, No. 2:15-CV-00095-WKS (D. Vt. May 12, 2017).

[102] 42 U.S.C. § 300jj(1) (2009) (defining a "certified EHR technology" as "a qualified electronic health record that is certified pursuant to section 3001(c)(5) as meeting standards . . . applicable to the type of record involved"); United States' Complaint in Intervention, *supra* note 101, at 1.

[103] *EHR Incentive Programs*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/ehr-incentive-programs [https://perma.cc/KH7J-EMRY] (last visited Apr. 6, 2018) [hereinafter *EHR Incentive Programs*].

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Medicare and Medicaid EHR Incentive Program Basics*, CTRS. FOR MEDICARE AND MEDICAID SERVS., https://www.cms.gov/Regulations-and -Guidance/Legislation/EHRIncentivePrograms/Basics.html [https://perma.cc/HXL2-P2SB] (last visited Apr. 6, 2018).

One of the key features of being eligible for the incentive programs is adoption and meaningful use of CEHRT.[108] To determine what qualifies as CEHRT, the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) developed standards and other technical criteria that EHR software would be required to meet in order for EHR vendors to be able to market their products as certified under EHR Incentive Programs.[109] Under the certification program, organizations may seek certification status from an ONC-Authorized Certification Body (ONC-ACB) that will be responsible for certifying and monitoring CEHRTs during the initial period of certification in accordance with the standards adopted by CMS and ONC.[110] Once an EHR has been certified, it is then added to a database maintained by the ONC that lists all CEHRTs and other pertinent information regarding CEHRTs that are then eligible for incentive payments.[111] Given that adoption of a CEHRT is a key feature of the requirements for the EHR Incentive Program, it can be potentially very lucrative for an EHR company to become certified because providers that want to access the incentive payments can only do so through a CEHRT.[112]

The program has had huge success in getting providers to adopt EHRs—especially EHRs with the necessary capabilities to create greater efficiencies in the system, including e-prescribing capabilities.[113] CMS reported, "As of December 2017, more than 542,600 health care providers received payment for participating in the Medicare and Medicaid [EHR] Incentive Programs."[114] This strong participation has resulted in payments of over twenty-four billion under the Medicare program and over twelve billion under the Medicaid program.[115]

---

[108] 42 U.S.C. § 300jj-51 (2016).

[109] *Certified EHR Technology*, CTRS. FOR MEDICARE & MEDICAID SERVS. [hereinafter *Certified EHR Technology*], https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Certification.html [https://perma.cc/K53P-WLXR] (last visited Apr. 6, 2018).

[110] 45 C.F.R. § 170.501 (2018); *see also* United States' Complaint in Intervention, *supra* note 101, at 6.

[111] *Certified Health IT Product List*, HEALTHIT.GOV (2017), https://chpl.healthit.gov/#/search [https://perma.cc/SA2Y-SLTL] (last visited Apr. 6, 2018).

[112] United States' Complaint in Intervention, *supra* note 101, at 6; *see Certified Health IT Product List*, *supra* note 111.

[113] *See* JAWANNA HENRY ET AL., ADOPTION OF ELECTRONIC HEALTH RECORD SYSTEMS AMONG U.S. NON-FEDERAL ACUTE CARE HOSPITALS: 2008–2015, ONC DATA BRIEF 35 (May 2016), https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php [https://perma.cc/UCN4-RNLF].

[114] *Data and Program Reports*, CTRS. FOR MEDICARE AND MEDICAID SERVS., https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/dataandreports.html [https://perma.cc/TWF7-D5Y5] (last visited Apr. 6, 2018).

[115] *Id.*; *see also EHR Incentive Program Summary*, CENTERS FOR MEDICARE AND MEDICAID SERVS., https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/December2017_MedicareEHRIncentivePayments.pdf [https://perma.cc/7BRB-24KF] (last visited Apr. 6, 2018).

Given the large sums of money the federal government is spending in connection with this program, it is unsurprising that any allegation regarding fraudulent practices conducted specifically to receive payment prompted the government's swift response.

Thus, in the DOJ's Complaint In Intervention in *United States ex rel. Delaney v. eClinicalWorks, LLC*,[116] the government focused its FCA liability claim on allegations that eCW manipulated its software to ensure that it would pass the certification test, enabling eCW to market its product to providers as meeting necessary certification requirements for purposes of securing the EHR incentive payments.[117] Specifically, the DOJ stated that eCW caused providers to submit false or fraudulent claims to the government because it:

> (a) [F]alsely attested to its certifying body that it met the certification criteria; (b) prepared its software in order to pass certification testing without meeting the certification criteria; (c) caused its users to falsely attest to using a certified EHR technology, when [eCW's] software could not support the applicable certification criteria in the field; and (d) caused its users to report inaccurate information regarding Meaningful Use objectives and measures in attestations to the [CMS].[118]

The most egregious claims that the government emphasized in the settlement agreement related to claims regarding the manner in which the eCW software was able to use so-called RxNorm codes[119] in connection with the e-prescribing capabilities of the software.[120] The government claimed that eCW first reviewed the standardized testing protocols that would be used by the applicable NCO-ACB, which identified the specific steps that an EHR vendor would be required to complete during the testing process.[121] eCW was thus aware that testing of the protocols for certification would require the identification and prescribing of sixteen specific drugs under the RxNorm requirement.[122] In order to meet certification requirements, the software should have

---

[116] United States' Complaint in Intervention, *supra* note 101, at 9.

[117] *Id.*

[118] *Id.* at 1–2.

[119] One of the certification requirements is that the software must be able to prescribe drugs electronically using the RxNorm codes set forth under the applicable protocols. *Id.* at 9. RxNorm is "a normalized naming system for generic and branded drugs; and a tool for supporting semantic interoperation between drug terminologies and pharmacy knowledge base systems." *Unified Medical Language System (UMLS)*, U.S. NAT'L LIBRARY OF MED., https://www.nlm.nih.gov/research/umls/rxnorm/overview.html [https://perma.cc/4WKN-B6NE] (last visited Apr. 6, 2018). The goal of utilizing RxNorm is to ensure that computers are using a normalized language to effectively communicate drug-related information. *Id.*

[120] Press Release, *supra* note 10.

[121] United States' Complaint in Intervention, *supra* note 101, at 7. Such protocols were publicly available in advance to EHR vendors so that the vendors could anticipate what protocols would be part of the test. Thus, reviewing the protocols alone was not anything nefarious or illegal. *Id.*

[122] *Id.* at 10.

been able to prescribe all pharmaceuticals based on utilization of RxNorm and not based on other pharmaceutical identifiers; but, for purposes of the specific certification test, only those specific sixteen drugs were to be tested.[123] Armed with such information, eCW representatives then "hardcoded"[124] the sixteen specific drug codes in order to assure that the software would pass the RxNorm portion of the test, even though the software itself was not able to prescribe drugs pursuant to the certification protocol.[125] eCW not only used this method for purposes of passing the test for the initial certification in 2013, but also used it on a retest in 2014.[126] Because eCW passed its initial tests and continued to pass tests related to RxNorm, its product was certified on July 24, 2013, and its certification was maintained during the initial certification period.[127] Despite eCW's awareness that its current methods did not comply with certification criterion, eCW did not make certification-conforming changes after receiving certification and continued to market and sell its product as a CEHRT.[128]

In addition to the issues related to the RxNorm codes, there were a number of other problems related to other aspects of certification that the complaint against eCW identified. These other problems included errors with patient education criterion, inadequate testing, unreliable version control, inability to create batch export reports,[129] inability to create accurate audit logs, inaccurate recording of diagnostic imaging orders, and unreliable performance of drug to drug and drug to allergy checks.[130] Key in connection with all of these errors,

---

[123] *Id.* It should be noted that eCW's software was not entirely without the capability to e-prescribe. While it was not transmitting the RxNorm codes in accordance with the certification requirements, it developed a work around in which the software either utilized proprietary drug identifiers as developed by private business partners or utilized National Drug Codes. *Id.* at 11. National Drug Codes are an identifier established by the Food and Drug Administration (FDA) under the Drug Listing Act of 1972, 21 U.S.C. § 360. Each drug product is "identified and reported using a unique, three-segment number, called the National Drug Code (NDC), which serves as a universal product identifier for drugs." *National Drug Code Directory*, U.S. FOOD AND DRUG ADMIN. (last visited Apr. 6, 2018), https://www.fda.gov/Drugs/InformationOnDrugs/ucm142438.htm [https://perma.cc/Z448-4TUM]. The FDA maintains a database of the NDC number that is assigned to each drug and using the numbers for purposes of enforcing the Federal Food, Drug, and Cosmetic Act. *Id.*

[124] United States' Complaint in Intervention, *supra* note 101, at 10 (noting that "rather than programming the capability to retrieve any code from the entire database of RxNorm codes, ECW simply typed the sixteen RxNorm codes necessary for testing directly into its software. . . . for the purpose of making its certification body believe it had implemented the RxNorm drug vocabulary and to pass certification testing").

[125] *Id.*

[126] *Id.* at 10–11.

[127] *Id.*

[128] *Id.* at 16.

[129] To be certified, an EHR system must be able to create a set of export summaries of all patients in the database and the eCW software was unable to perform this function, which customers noted to eCW personnel. *Id.* at 14.

[130] *Id.* at 13–16.

and key for purposes of assuring that eCW had sufficient knowledge of its activity as required under the FCA,[131] was that eCW became aware of the issues—primarily via complaints from customers after experiencing errors with the product[132]—but failed to correct or rectify most, if any, of the problems until 2016, after eCW had come under investigation by the federal government.[133]

Unlike the claim regarding eCW's overt actions with the manipulation of the sixteen drug codes to facilitate passing the certification test, the remainder of the claims against eCW related to issues that could be considered problematic because they potentially compromised patient safety or created challenges for the customers in terms of work flow or efficiency in the delivery of care.[134] To the extent that the government was alleging that any inadequacies and technical challenges with the use of eCW's software were somehow fraudulent (as opposed to simply usual software bugs or glitches)[135] under the FCA, the government's allegations hinge on the fact that eCW was aware of the problems with the software and failed to rectify them. It is unrealistic and virtually impossible to claim that CEHRT software will be flawless and will always function in accordance with all the EHR Incentive Program's criteria at all times and with no flaws. Thus, it seems the government in the eCW complaint attempted to distinguish between situations in which the EHR vendor corrects any software bugs or flaws as soon as it is aware of such bugs or flaws versus a vendor that seems to be aware of the issues and consciously does nothing to remedy or fix the issues.[136] The latter is a necessary component of whether this behavior could be considered fraudulent. This distinction could be difficult to differentiate, and there seems to be little guidance from the eCW settlement agreement as to when an EHR vendor response might be adequate and when it could instead constitute fraud.

---

[131] To sustain a claim alleging violations of the FCA, one must prove that the entity alleged to have violated the FCA had "knowledge" of its actions, which includes deliberate ignorance, reckless disregard, and actual knowledge. *See* United States *ex rel.* Hutcheson v. Blackstone Medical, Inc., 647 F.3d 377, 380 (1st Cir. 2011).

[132] United States' Complaint in Intervention, *supra* note 101, at 12.

[133] *Id.* at 11–13, 15. It was noted in the complaint that eCW knew that it was under investigation at least by Dec. 23, 2016. *Id.* at 11.

[134] *See id.* at 12–16.

[135] It is quite common after software is released for either the company or users to discover certain errors or security bugs and then the company issues updates or "patches" to fix the errors. For example, within twenty-four hours of Apple releasing its new Mac operating system, Apple had discovered and released a software update to address a security bug in the system that would have allowed anyone to gain unauthorized and full administrator control into a Mac running the latest operating system without a password. *See* Mark Gurman, *Apple Releases Fix to Security Flaw in Mac Operating System*, BLOOMBERG NEWS (Nov. 28, 2017, 2:16 PM), https://www.bloomberg.com/news/articles/2017-11-28/apple-mac-operating-system-has-login-flaw-that-puts-data-at-risk [https://perma.cc/Y9FB-U5Y5].

[136] United States' Complaint in Intervention, *supra* note 101, at 11–15.

Similarly, the complaint also resolved allegations of violations of the AKS in connection with unlawful remuneration to customers who referred other customers or recommended eCW's products.[137] Specifically, the complaint alleged that eCW conducted a "referral program" that paid for referrals by one customer of another customer, a "site visit program" in which eCW paid current users to host other customers at their practice site to promote eCW's software, and a "reference program" that involved payments to current users to serve as references for prospective customers.[138] Lastly, the DOJ also alleged that eCW was paying physicians—both in cash and in kind—"consultant" or "speaker" fees to promote software.[139]

While these claims are referenced in the complaint, it is possible they were included at eCW's request to assure that no other FCA claims could be filed against eCW in connection with the conduct and to assure that neither the Office of Inspector General nor the DOJ could file any claims at a later time based on AKS violations for the same period.[140] It is not clear, however, whether the claims would be actionable if the FCA claim had instead been based solely on the AKS allegations and did not also involve the claims associated with the deliberate manipulation of the software under the EHR Incentive Program. For example, the complaint does not reference how many payments to physicians under any of the above-referenced programs resulted in referrals for software used by other customers that were then actually reimbursed by federal healthcare programs.[141] Certainly, there is evidence that eCW sought certification for the sole purpose of being able to seek payment under the EHR Incentive Program; thus, to the extent that payments were made to physicians with the intention of inducing those physicians to refer other providers to purchase eCW products for reimbursement under the EHR Incentive Program, it would seem that is a clear violation of the AKS.[142] It is not clear from the complaint, however, how successful such programs were and how many claims resulted from the remunerations or kickbacks paid.[143] This is an important distinction for purposes of contemplating application of the FCA to future cases involving EHR vendors because, unlike pharmaceutical products or medical devices,

---

[137] *Id.* at 17.

[138] *Id.* at 17–18.

[139] *Id.* at 18.

[140] Jonathan Cone et al., *Negotiating False Claims Act Settlements*, BRIEFING PAPERS (Feb. 2014), https://www.crowell.com/files/Negotiating-False-Claims-Act-Settlements.pdf [https://perma.cc/HW3Y-4CCG] (advising clients in connection with an FCA settlement to "negotiate the broadest possible release by writing the broadest definition of covered conduct").

[141] To sustain a claim under the AKS, one must eventually prove that the federal government made a payment under a federal healthcare program for a service that was rendered either due to or involving an illegal solicitation or receipt of remuneration. 42 U.S.C. § 1320a-7b (2012).

[142] *See id.*; United States' Complaint in Intervention, *supra* note 101, at 17–18.

[143] *See* United States' Complaint in Intervention, *supra* note 101, at 17–18.

EHR systems, in and of themselves, are not necessarily reimbursable under federal healthcare programs[144]—although some courts have allowed reimbursement to be inclusive of items that may be part of other payments.[145] Regardless, due to the unique nature of EHRs and the unique nature of the EHR Incentive Program's involvement in the eCW case, the viability of an AKS claim as the basis for an FCA claim against EHR vendors more generally remains somewhat untested despite this settlement agreement resolving such claims.

B. Fraud Among EHR Vendors

Some might examine the eCW settlement agreement and related FCA allegations as simply one egregious example of blatant deception, given the knowing and deliberate act of hardcoding the software for the purpose of receiving certification under the EHR Incentive Program.[146] Many in the EHR Vendor industry have been rightly concerned, however, about what the case means for the purpose of trying to determine what might or might not constitute fraud in the EHR context and what it means for other vendors.[147] While the "hardcoding" allegations were about a specific incident, many of the other allegations

---

[144] Pharmaceutical drugs are directly reimbursed by the Medicare program under Medicare Part D, and many states include prescription drugs as covered by certain Medicaid programs. *See How to Get Drug Coverage*, MEDICARE.GOV (last visited Apr. 6, 2018) https://www.medicare.gov/sign-up-change-plans/get-drug-coverage/get-drug-coverage.html [https://perma.cc/2VYN-KQ35] (describing Medicare's prescription drug coverage and how to enroll); *see also Prescription Drugs*, MEDICAID.GOV (last visited Apr. 6, 2018) https://www.medicaid.gov/medicaid/prescription-drugs/index.html [https://perma.cc/7XEV-K7L2] (noting that pharmacy coverage is an option benefit, but that all states provide coverage in some form). Medical devices are perhaps more akin to pharmaceutical products because the products themselves are reimbursed under some federal healthcare programs. *See* United States *ex rel.* Hutcheson v. Blackstone Medical, Inc., 647 F.3d 377, 394 (1st Cir. 2011) (describing that medical devices are part of the calculation of the diagnosis-related group that Medicare pays a hospital for a particular service, although the devices are not separately itemized or reimbursed at cost).

[145] *Blackstone Medical, Inc.*, 647 F.3d at 394. (finding that even though the hospitals and physicians may not have submitted claims that directly reimbursed the specific medical devices, that "[w]e cannot say that, as a matter of law, the alleged misrepresentations in the hospital and physician claims were not capable of influencing Medicare's decision to pay the claims" because "[t]he intricacies of the DRG system do not alter the clear language of the Provider Agreement and the Hospital Cost Report Forms.").

[146] In its defense, eCW responded to allegations about the specific charges related to RxNorm codes by stating that it was an inadvertent error that was corrected upon discovery. A representative of eCW wrote, "The failure to include RxNorm codes in electronic prescriptions was completely inadvertent on the part of eClinicalWorks, as our software used RxNorm codes in other parts of the system, such as in C-CDAs. We gained nothing by not including the codes, which are available for free from the National Library of Medicine. We resolved this issue as soon as we learned of it." *See* Landi, *supra* note 14.

[147] *See id.* (discussing a healthcare attorney saying this case should serve as a wake-up call to health IT vendors about compliance).

related to eCW's failure to immediately correct known issues.[148] EHR vendors watching this case were left wondering what the eCW case means for purposes of fixing known bugs or glitches within the software. How soon after a problem is discovered does a software error need to be corrected? Is there time to see if other issues arise? Might some of the issues be related to specific systems because of legacy software? How often must software be updated? Are some glitches okay and some not? Will issues that cause patient safety problems be seen as more important or less important than issues that cause financial injuries like improper billing?

Certainly, there are myriad questions, but not necessarily a lot of guidance or answers to those questions from the eCW settlement agreement. One can see the potential for these types of issues to bleed over into other areas, even other applications of the FCA. On August 24, 2016, three hospitals in the state of New York settled Medicaid fraud charges alleging that they failed to pay known overpayments within the sixty days required to remit known overpayments.[149] Under amendments to the FCA enacted as part of the Affordable Care Act,[150] the FCA now makes it a false claim to retain any known overpayments for a period of greater than sixty days.[151] In the New York case, a software glitch in the hospitals' billing system caused the erroneous billing of 444 claims to the Medicaid program during 2009 and 2010.[152] The three hospitals were notified by an individual employee about the software glitch, thus putting the hospitals on notice of the possibility of erroneous billing.[153] While the hospitals eventually remitted the overpayments, the remittance trickled in over a period of two years (from 2011 to 2013) rather than within the sixty days that is required pursuant to the FCA.[154] The employee who had alerted the hospitals to the known error had been fired, and he eventually became the *qui tam* relator in the case.[155]

While this particular FCA action was directed at the hospitals, one could see how this exact scenario could equally implicate an EHR vendor. Imagine that instead of an employee discovering the glitch and informing appropriate executives within the company, an employee at the EHR vendor discovers a

---

[148] *See* United States' Complaint in Intervention, *supra* note 101, at 11–16.

[149] *See* Kane *ex rel.* United States v. Healthfirst, Inc., 120 F.Supp.3d 370, 383 (S.D.N.Y 2015); *see also* Jonathan Stempel, *New York City Hospitals Settle Medicaid Repayment Fraud Charges*, REUTERS (Aug. 24, 2016, 12:25 PM), https://www.reuters.com/article/us-new-york-hospitals-settlement/new-york-city-hospitals-settle-medicaid-repayment-fraud-charges-idUSKCN10Z2KC [https://perma.cc/W7LT-GW88].

[150] Patient Protection and Affordable Care Act, 42 U.S.C. § 1301 (2012).

[151] 31 U.S.C. § 3729(a)(1)(G) (2012) ("[K]nowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government.").

[152] *See* Stempel, *supra* note 149.

[153] *Id.*

[154] *Id.*

[155] *Id.*

similar glitch that is causing thousands of dollars in overpayments to the Medicare or Medicaid programs, or both. Assume that the employee notifies executives at the EHR vendor, but the executives are concerned about the damages that an announcement about the error might have on the company's reputation and realize that fixing the error would be time intensive and expensive. The executives therefore decide to get one of their current coders to work on a patch, which they will release in about six months—during the summer months when everyone is on vacation and fewer people will take notice of the patch. Could the employee at the EHR vendor file an FCA claim alleging that the vendor failing to notify any customers of the known software error and that not correcting the error until several months after the fact constitutes a false claim?[156]

Indeed, once one begins to review existing claims against EHR vendors, especially those claims between provider-customers and the vendor based on breach of contract, many of the allegations arise out of failure on the vendor's part to deliver the product in the manner in which it was promised; or, said another way, the failure of the software to perform as desired and anticipated.[157] To the extent that a software issue is the cause of, or contributes to, a situation in which a provider submits claims that are false, fraudulent, or a misrepresentation of the services actually provided, the EHR vendor is not only potentially liable in a direct claim against the provider, but also potentially exposed to FCA actions. This liability, however, must be premised on all factors necessary to sustain an FCA claim, including "knowledge" on the part of the vendor, claims submitted to federal healthcare programs, and claims that are material to the government's decision to pay the claim.[158]

The challenge remains, however, to determine at what point a glitch in the software or known bug or error in the coding turns from simply common and necessary software maintenance to fraudulent practices. Are any of the lawsuits against the existing vendors examples of such neglect or lack of attention that vendors' lack of action has transitioned into fraud? Where does the line between fraud and inattention fall, and does the eCW settlement agreement give vendors—or even *qui tam* relators—guidance on that question?

---

[156] *See* 31 U.S.C. § 3729(a)(1)(G) ("[K]nowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government. . . ."). It does not seem that a *qui tam* relator could in fact sustain an FCA claim for knowingly causing another entity to conceal "or knowingly and improperly avoid[ing] or decreas[ing] an obligation to pay or transmit money or property to the Government," known as a "reverse false claim." Indeed, there is no "causes to" language in the second half of subsection G, but it seems it would fit squarely into the idea that the software vendor's action of not correcting the error is causing another to make or use a false record or statement material to an obligation to pay or transmit money.

[157] *See* Landi, *supra* note 14.

[158] 31 U.S.C. § 3729.

III. FALSE CLAIMS ACT LIABILITY FOR EHR VENDORS

Jeffrey Smith, vice president of policy at American Medical Informatics Association, has stated,

> [The eCW case] really highlights how benign glitches can have far-reaching impacts to patient safety. I imagine every single CIO out there understands this notion very well, because while we suffer through computer glitches and little hiccups on smartphones—in healthcare, a glitch can be the difference between life and death. . . . And, I anticipate that the $155 million that the government is getting is only the beginning.[159]

In the years since the enactment of HIPAA and HITECH, the informatics side of healthcare has enjoyed a relatively liability free existence due not only to contracting practices such as hold-harmless provisions and indemnification clauses, but also the complication of human error as an intervening or contributory factor in negligence and general legal doctrines such as the learned intermediary doctrine.[160] As provider usage and reliance on EHR systems has increased, however, there has also been a marked rise in the prevalence of claims not only medical malpractice claims from patients, but breach of contract claims from customers and providers.[161]

Given this increased use and reliance on electronic systems is primarily the result of the $24 billion that the federal government spent incentivizing providers to join the digital age, the eCW settlement agreement is perhaps less surprising than it may first appear. While the bulk of FCA claims are against providers and suppliers that contract directly with federal healthcare programs, the DOJ has great financial success[162] with FCA claims premised on the inducement-of-fraud theory against entities such as pharmaceutical companies and device manufacturers.[163] Based on the eCW case and the alleged fraud under the settlement agreement, it is likely that the use of the FCA to address fraud

---

[159] *See* Landi, *supra* note 14.

[160] *See supra* notes 80–82 and accompanying text.

[161] *See* Landi, *supra* note 14.

[162] This Article references monetary success because it is undisputed that the largest settlement amounts under the FCA have been achieved through settlement agreements with pharmaceutical companies for AKS violations or promotion of drugs for off-label use. *See* Settlements & Judgments, *supra* note 37. Whether such settlement amounts have been successful in deterring pharmaceutical companies or their executives from certain illegal behaviors is not necessarily clear, however. Regarding a successful drug that is still protected by an existing patent—thus providing the pharmaceutical company the opportunity to effectively set the price of the pharmaceutical at any price that it desires—a pharmaceutical company might be willing to pay any associated fees, penalties, or settlement amounts because the benefits from the illegal behavior outweigh the assessment of fines and penalties. *See* Krause, *supra* note 41, at 404–05. Thus, for certain drugs that might be extremely marketable across a large population, the risk of entering into a settlement for illegal activity might simply be viewed as a "cost of doing business." *See id.* at 429 (quoting William N. Sage, *Fraud and Abuse Law*, 282 JAMA 1179, 1180 (1999)).

[163] *See* Kwok, *supra* note 27, at 215.

and misrepresentation in the EHR industry will continue. While FCA cases against pharmaceutical companies and medical device manufacturers can serve as good examples for EHR vendors and what they might come to expect, the distinctions and unique characteristics of EHR vendors and the EHR industry relative to the pharmaceutical industry and its practices make it unlikely that the government will have as much success with application of the FCA against EHR vendors as with pharmaceutical companies.

A. Distinctions Between Pharmaceutical Companies and EHR Vendors

It is undisputed that even with fewer FCA cases alleged against pharmaceutical manufacturers,[164] the amount that the government has been able to recover—inclusive of reimbursement of overpayments, penalties, and treble damages—against pharmaceutical companies has been unprecedented.[165] Thus, even with fewer total cases implicated by the FCA, the pharmaceutical industry continues to have a massive impact on the total recovery amount under the FCA.[166] It further demonstrates the DOJ's consistent efforts to utilize the FCA to enforce the country's increasingly complex healthcare regulatory scheme by targeting not just hospitals, physicians, and other providers who contract directly with the Medicare and Medicaid programs, but also those large ancillary providers and suppliers, such as pharmaceutical companies or medical device manufacturers. Although EHR vendors and pharmaceutical companies share some characteristics that demonstrate some common liability concerns under the FCA, there are many distinctions between these two types of health care entities that will distinguish EHR vendors from pharmaceutical companies, making the monetary success for FCA claims against EHR vendors less likely.

First, as mentioned above, much of the ability to achieve large settlements against pharmaceutical manufacturers is attributable to two unique aspects of pharmaceutical sales: (a) name-brand drugs, when first introduced in to the

---

[164] Hospitals, clinics, and single providers account for the largest individuals/entities that entered into settlements to resolve FCA allegations, which amounted to approximately $585 million. *2016 Year-End Health Care Compliance and Enforcement Update—Providers*, GIBSON DUNN & CRUTCHER LLP (Feb. 15, 2017), https://www.gibsondunn.com/2016-year-end-health-care-compliance-and-enforcement-update-providers/ [https://perma.cc/SJ2W-BB4F].

[165] *See* Settlements & Judgments, *supra* note 37; *see also* Press Release, *supra* note 32 (noting the largest settlement in FCA history with GlaxoSmithKline LLC (GSK) pleading guilty and paying $3 billion ($1 billion to resolve criminal charges and $2 billion to resolve civil charges) to resolve criminal and civil liability arising from illegal activity related to several of its pharmaceutical products). This amount stands in contrast to a total of $4.7 billion that was collected for the entire year 2016, which was the third highest annual recovery in the history of the FCA. *See* Press Release, United States Dep't of Justice, Justice Department Recovers Over $4.7 Billion from False Claims Act Cases in Fiscal Year 2016 (Dec. 14, 2016), https://www.justice.gov/opa/pr/justice-department-recovers-over-47-billion-false-claims-act-cases-fiscal-year-2016 [https://perma.cc/7462-6NC4].

[166] *See* Settlements & Judgments, *supra* note 37.

market, are almost always "on patent," meaning that the drugs and their manufacturing processes or ingredients, or both, are protected as intellectual property rights thus limiting the possibility of competing products for a time;[167] and (b) once approved for a specific use, drugs can be used for other off-label uses in a physician's medical judgment.[168] Thus, during the period that a particular pharmaceutical is protected from competition,[169] the pharmaceutical company is effectively the only seller on the market and it is during the time that most of the profit is generated from the drug—and the company's expenses are recouped.[170] A pharmaceutical company is limited in its promotion of its product through certain restrictions on advertising and misbranding of drugs,[171] but there are no prohibitions against physicians, in their medical judgment, prescribing a drug for any use, not simply the labeled use.[172] Therefore, it is possible for a pharmaceutical company to generate profits not just based on the use for which a drug was approved, but for any number of off-label uses.[173] To the extent a drug can be prescribed for more uses, the customer base widens, and

---

[167] To encourage innovation and creation of new drugs, federal law enables pharmaceutical manufacturers to file for patent protection for certain aspects of a drug, including its active ingredients, the process of its manufacturing, etc. *See* Benjamin N. Roin, *Unpatentable Drugs and the Standards of Patentability*, 87 TEX. L. REV. 503, 507–08 (2009).

[168] *See* Sandra H. Johnson, *Polluting Medical Judgment? False Assumptions in the Pursuit of False Claims Regarding Off-Label Prescribing*, 9 MINN. J.L. SCI. & TECH. 61, 61–62 (2008).

[169] In addition to patent law, there are other protections under the Food and Drug Administration that would also protect the time for which a drug manufacturer has to promote its drug. *See* Rongxiang Liu, *Pharma's Strategies on Fighting Generics and Healthcare Reform*, 3 BIOTECH. & PHARMACEUTICAL L. REV. 26, 32 (2010) ("Title I also provides an incentive to Pharma for innovations, which is the right of exclusivity. The exclusivity period for an innovative brand drug is the time period in which no ANDA can be approved, regardless the status of the patent protecting the brand drug. Therefore, Pharma's exclusivity is independent of, but runs in tandem with, patent protection.").

[170] *See* Roin, *supra* note 167, at 507–08.

[171] *See* Krause, *supra* note 41, at 405–06 (describing that while there is no direct prohibition against promotion of a drug for an off-label use, there are FDA regulations that restrict advertising in a way that effectively prohibits promotion of an off-label use).

[172] *See id.* at 405 (citing United States v. Caronia, 703 F.3d 149, 153 (2d Cir. 2012)); Citizen Petition Regarding the Food and Drug Administration's Policy on Promotion of Unapproved Uses of Approved Drugs and Devices, 59 Fed. Reg. 59,820 (Nov. 18, 1994) (quoting 1982 FDA Drug Bulletin stating that "once a [drug] product has been approved for marketing, a physician may prescribe it for uses or in treatment regimens of patient populations that are not included in approved labeling"). It should be noted that while there are no prohibitions, prescribing a drug for a purpose other than its approved purpose pursuant to its label under the FDA could expose the physician to medical malpractice or other negligence or wrongful death claims to the extent that such use is not medically appropriate or supported by sufficient medical evidence. *See* BARRY R. FURROW ET AL., HEALTH LAW: CASES, MATERIALS AND PROBLEMS, 366–77 (7th ed. 2013) (noting that prescribing a drug for an off-label use can be used as an affirmative defense, but does not always successfully dismiss a medical malpractice claim).

[173] *See* Johnson, *supra* note 168, at 70–71.

the possibility of greater profits increases due to the wider distribution of the drug.[174] Thus, even though it might be illegal for a pharmaceutical company to promote a drug for off-label use, it may nevertheless be financially advantageous for the company to do so because the penalties and fines that the company might pay for the illegal activity may still dwarf the potential profits that can be gained through the wider distribution of the drug while still on patent.[175] While there is some ambiguity in the area of what "promotion" might actually be illegal, the government has been relatively successful under the FCA in garnering large settlements against pharmaceutical manufacturers for various activities implicating promotion of their drugs, including violations of the federal AKS.[176]

Interestingly, at first glance, the eCW case seems to have a number of similarities to these cases against pharmaceutical companies that could lead one to believe that application of the FCA to EHR vendors would be strikingly similar to its application to pharmaceutical companies. Much like the actions of drug companies to promote a particular product for off-label use during the small window in which the product is protected from competition, eCW was alleged to have undertaken knowingly fraudulent action during the very narrow window in which it could become certified under the EHR Incentive Program.[177] Because of the incentive payments and the possibility of customers' insistence upon the purchase of software that met necessary certification requirements during that time, eCW was motivated to take whatever actions necessary to ensure robust sales to all of these new users entering the market. Indeed, eCW generated over $320 million in annual revenue in 2014 and stated that it anticipated 15–20 percent growth.[178]

---

[174] Elizabeth Richardson, *Health Policy Brief: Off-Label Drug Promotion*, HEALTH AFFAIRS, 3–4 (June 30, 2016), https://www.healthaffairs.org/do/10.1377/hpb20160630.920075/full/ [].

[175] *Id*. at 2.

[176] *See* Krause, *supra* note 41, at 417–18. Note that while Krause argues that the FCA has been a hugely profitable tool for the federal government against drug companies, she argues that a recent opinion raising First Amendment challenges to advertising and marketing off-label use may disrupt application of the FCA against drug companies for the promotion of off-label use because of the inconsistency between application of the FCA versus protections under the First Amendment. *Id*. at 418–19. This Article is not making a determination that the FCA is an appropriate tool to combat promotion of off-label use, but simply recognizes that the federal government uses the FCA to combat the promotion of off-label use and that has been highly successful in its monetary recovery efforts. Likewise, any analysis in this Article about the likelihood of the federal government, through the DOJ, utilizing the FCA for purposes of combatting abuses in the EHR industry that impact patient safety should not be construed to be a conclusion regarding the appropriateness of the FCA for this purpose.

[177] United States' Complaint in Intervention, *supra* note 101, at 9.

[178] Dan Primack, *The Software 'Unicorn' That Will Never Go Public*, FORTUNE (Feb. 13, 2015), http://fortune.com/2015/02/13/the-software-unicorn-that-will-never-go-public/ [https://perma.cc/8GAK-VWHE].

Despite these similarities, there seems to be more divergences than parallels between these two sectors of the health care industry, which might indicate a different application of the FCA. Unlike the existing patent structure for pharmaceuticals, the facts of the eCW case and the urgency that created incentives for software companies like eCW to seek certification status are finite in time.[179] The specific facts of the eCW case, wherein the false claim was tied to federal monies paid under the EHR Incentive Program, make it not entirely unlikely that other software companies could face similar allegations for the next few years as the monies are paid out, but make it virtually impossible that such allegations and activities are actionable on a long term basis once the program is over. This should not be read to mean that the eCW case will stand as the lone FCA case, but that future cases will have to rely more closely on some of the other allegations of the settlement agreement for purposes of sustaining claims.[180] For example, the original FCA allegations against eCW related more so to patient safety concerns caused by eCW's failure to properly maintain its software and allegations of AKS violations arising out of payments made to physicians to promote eCW's software.[181] Because of the nature of the "hard-coding" allegations,[182] these other avenues were not explored in as great of depth and it is not entirely clear what else would be necessary to prove an FCA case not premised on EHR incentive payments. Certainly, to satisfy the "knowledge" requirement under the FCA, it would be necessary to show what an EHR vendor knew about flaws or glitches in its product, when it knew, its reaction (or lack of reaction), and how such glitches affected claims made to the federal government. Unlike a pharmaceutical company that has clear incentives to promote off-label products in order to expand the market for buyers or to generate greater profits, the incentive for an EHR vendor to ignore or delay software malfunctions is not as transparent. As these types of nuances and complexities emerge, it appears less and less likely that EHR vendor liability under the FCA will closely resemble application of the FCA against pharmaceutical companies.

In addition to some of the structural distinctions between the nature of the claims themselves, the market for EHRs and the market for pharmaceuticals is exceedingly diverse. One of the consistent challenges for the DOJ in trying to consider how to corral drug companies' marketing and promotion activities is weighing the balance between punishing the manufacturer enough to potentially curb behavior without the punishment having residual effect on the patients

---

[179] *See* EHR Incentive Programs, *supra* note 103 (noting that payments under the program only run through 2021 and payments that are being made on an ongoing basis are only for purposes of complying with later stage obligations related to meaningfully using CEHRT—not simply the purchase of CEHRT).

[180] United States' Complaint in Intervention, *supra* note 101, at 11–17.

[181] *Id.* at 13.

[182] *See id.* at 9–10.

who need access to the products.[183] An effective deterrent for drug companies might simply be to require the company to remove the product from the market or exclude the company from federal health care programs, thus preventing the manufacturer from generating any profits from the sales.[184] While this certainly might help to curb illegal behavior, it could be potentially devastating for consumers who are taking the pharmaceutical and need it to treat their particular condition. Thus, most enforcement tools against pharmaceutical manufacturers come in the form of fines and penalties.[185]

EHR products, on the other hand, are vast and many.[186] The federal government estimates that "684 health IT developers supply certified health IT to 354,395 ambulatory primary care physicians, medical and surgical specialists, podiatrists, optometrists, dentists, and chiropractors," and "82% have 2014 certified edition technology."[187] While there is some market consolidation, there is no shortage of products on the market from which customers may choose. Thus, to the extent that the DOJ might levy such high penalties or fines so as to bankrupt an EHR vendor, it may be an inconvenience to its customers to switch to a new platform, but it would not be challenging for such customer to find a new vendor, nor would it be entirely uncommon.[188] Indeed, under the Corporate Integrity Agreement that eCW entered into as part of its settlement agreement with the DOJ, eCW was required to offer to all of its customers the option of switching to another EHR vendor without assessing any penalties or service charges.[189] In a report following the settlement, about one third of eCW cus-

---

[183] *See* Lise T. Spacapan & Jill M. Hutchison, *Prosecutions of Pharmaceutical Companies for Off-Label Marketing: Fueled by Government's Desire to Modify Corporate Conduct or Pursuit of a Lucrative Revenue Stream?*, 22 ANNALS HEALTH L. 407, 421 (2013).

[184] *Id.* at 419.

[185] It should be noted that this challenge is part of what led to the drafting of the Yates Memo and the increased emphasis on trying to prosecute executives who have created a culture of compliance with companies. Memorandum from Sally Quillian Yates, Deputy Attorney Gen., on Individual Accountability for Corporate Wrongdoing to All U.S. Attorneys, (Sept. 9, 2015), https://www.justice.gov/archives/dag/file/769036/download [https://perma.cc/H2MC-XSZ6].

[186] *See* QUICK STATS, *supra* note 8.

[187] *Id.* Although there are many vendors, just five vendors supply 2014 certified technology to sixty percent of all providers.

[188] *See* Farringer, *supra* note 7, at 971. Ironically, an article in *Becker's Health IT & CIO Review* from 2014 noted a comment that Girish Navani, Chief Executive Officer and cofounder of eCW, made in 2013 stating that more than half of eCW's new clients came from another vendor. *See* Helen Gregg, *50 Things to Know About Epic, Cerner, MEDITECH, McKesson, athenahealth and Other Major EHR Vendors*, BECKER'S HEALTH IT & CIO REV. (July 14, 2014), https://www.beckershospitalreview.com/healthcare-information-technology/50-things-to-know-about-epic-cerner-meditech-mckesson-athenahealth-and-other-major-ehr-vendors.html [https://perma.cc/53SE-H4TZ].

[189] Mike Miliard, *One-Third of eClinicalWorks Customers Prepping to Switch EHR Vendors, KLAS Says*, HEALTH CARE IT NEWS (July 28, 2017, 10:01 AM), http://www.healthcare

tomers stated that they were planning on changing to a different vendor, but of that one third, only 4 percent stated that their reason for switching was due to the settlement agreement with the DOJ.[190] What this likely means is that the large vendors like eCW have sufficient revenue and customer base that they are likely able to absorb any fines or penalties that may be assessed,[191] and that any similar actions taken against smaller companies would have little impact on customers and access to EHR products, even if it meant that the EHR product was no longer available.[192]

Lastly, the potential profit margins of these two industries are also unique and distinct. While perhaps certain aspects of an EHR system could be patentable, which could set a particular EHR product apart from other similar products, the entire goal of the EHR Incentive Program and the "meaningful use" regulations under HITECH is to create uniformity and consistency among EHR systems.[193] Thus, unlike pharmaceutical companies whose goal is to create a new drug that can, for at least a time, enjoy patent protection and thus limited competition, an EHR vendor seeking certification is required under law to create a product that by its nature will have nearly identical features to other products on the market.[194] Certainly, there will be means by which vendors can distinguish their products from other products based on appearance, ease of use, integration with other systems, or customization for certain specialties, but as it relates to core functions, the EHR systems must all be able to perform the same functions. Thus, not only are there hundreds of competitors in the same market, but the distinctions that a vendor can create to make its product superior to other products is somewhat limited. These limitations will then lead to less price variation because there is less of an ability for a vendor to tout their product as so far superior to other products that it would warrant a drastically increased

---

itnews.com/news/one-third-eclinicalworks-customers-prepping-switch-ehr-vendors-klas-says [https://perma.cc/DXM5-L382].

[190] *Id.*

[191] eCW stated on its website that it had added more than 3,750 providers in the third quarter, reported revenue of $130 million, and stated that eCW "is now the second most widely used EHR in the country." *See* Press Release, eClinicalWorks, eClinicalWorks Announces Strong Sales Growth, Adding Over 3,750 Providers in Third Quarter and Reporting $130 Million in Revenue (Oct. 6, 2017), https://www.eclinicalworks.com/announcesstrongsales growth/ [https://perma.cc/FH4P-P2EQ].

[192] Tom Sullivan & Jessica Davis, *Not Just Epic and Cerner: Hospitals Have Several EHR Options If They Abandon eClinicalWorks*, HEALTH CARE IT NEWS (June 1, 2017, 12:28 PM), http://www.healthcareitnews.com/news/not-just-epic-and-cerner-hospitals-have-several-ehr-options-if-they-abandon-eclinicalworks [https://perma.cc/EW38-NEXV].

[193] Marsha R. Gold et al., *Obtaining Providers' 'Buy-In' and Establishing Effective Means of Information Exchange Will Be Critical to HITECH's Success*, 31 HEALTH AFF. 514, 518 (2012), https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.2011.0753 [https://perma.cc/NX3Y-R7W5].

[194] *See generally* Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 75 Fed. Reg. 44590 (July 28, 2010) (codified at 45 C.F.R. pt. 170).

price compared to other vendors.[195] So, while many EHR vendors have experienced relatively high profit margins, such profits will never be able to compare to the margins that can be generated in the pharmaceutical context, given the distinctions in the market place.[196] Thus, recovery in the EHR area is much more likely to resemble FCA recovery amounts for hospitals or other providers, but not necessarily similar to amounts recoverable in the pharmaceutical context.

Despite that, on its face, the eCW complaint-in-intervention looks as though it is right out of the DOJ playbook for FCA application against pharmaceutical companies.[197] It seems unlikely, however, that the eCW case will set off widespread application of FCA actions against EHR vendors in a manner similar to the pharmaceutical industry. The EHR Incentive Program will have limited long-term use and, outside of this program, these two sectors seem too disparate and unique to be able to draw conclusions as to one based on application of the FCA under another. It seems unlikely that EHR vendors will continue to enjoy the limited liability that has existed since the advent of EHRs into the market, and certainly this is likely not the last we will hear from *qui tam* relators or the federal government about EHR systems. What these cases will look like in the future, however, and what their effect on the market will be generally has yet to be seen.

CONCLUSION

According to HealthIT.gov,

> The main goal of health IT is to improve the quality and safety of patient care. The promise of fully realized EHRs is having a single record that includes all of

---

[195] HealthIT.gov, a government sponsored website to assist providers and professionals with transitioning to an EHR, provides advice on how to select a vendor on its "Frequently Asked Questions" page, and also provides several comparison tools so that a consumer can compare functionalities in the Vendor Evaluation Matrix Tool, meaningful use capabilities under the Vendor Meaningful Use Compare Tool, and pricing under the Vendor Pricing Template. U.S. Dep't of Health & Human Servs., *Frequently Asked Questions*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/frequently-asked-questions/425#id93 [https://perma.cc/3MGP-8PVP] (last visited Mar. 29, 2018). Thus, with these tools, vendors are unlikely to create a product that strays too far from a competitor's product or set a price too much higher than other pricing unless there is a clear way to distinguish your product from another product.

[196] It is acknowledged that the availability for patent protection in the pharmaceutical context is because of the high research and development costs associated with getting a drug to market and the necessary incentives that must be created to induce companies to incur such costs in the beginning stages of a new product. EHR systems do not have similar research and development costs or lengthy approval processes equivalent to the FDA approval process. The period during which drugs are patent protected, however, has often enabled drug companies to not just recoup their expenses, but generate profits far exceeding any related expenses. This is not a commentary on whether those systems are providing proper incentives, but merely recognizing distinctions between the industries.

[197] *See generally* United States' Complaint in Intervention, *supra* note 101.

> a patient's health information: a record that is up to date, complete, and accurate. This puts providers in a better position to work with their patients to make good decisions.[198]

As the health care industry works to implement EHRs to achieve these goals, both EHR vendors and customers are experiencing the inevitable growing pains of trying to figure out healthcare delivery in the new age of electronics.

After two decades of working together to implement new systems, it seems that the responsibility that EHR vendors have in the health care delivery system may finally be starting to be recognized—both for its benefits and for its faults. While EHR vendor liability in medical malpractice and breach of contract claims has already increased, the eCW settlement agreement represents the first of its kind utilizing the FCA to combat fraudulent activity in the EHR industry.[199] Based on the unique facts of the eCW case, the settlement may not serve as a predictor of the filing of hundreds of similar FCA claims under the EHR Incentive Program in the same way that the DOJ has used the promotion of off-label use and the AKS against pharmaceutical companies. However, it should stand as a cautionary tale to the EHR industry regarding FCA liability more generally. Many of the claims in the eCW complaint highlight some of the activities and behaviors of EHR vendors that the DOJ might deem suspect, even outside the context of the EHR Incentive Program. While the facts of eCW may stand alone, the DOJ is putting vendors on notice to the expectations of the government when it comes to correcting known errors, performing necessary maintenance, assuring software functions appropriately, and ensuring that EHRs do not compromise patient safety. EHR vendors should not dismiss eCW as an isolated incident, but heed the warnings about the potential for FCA liability in the future.

---

[198] *Why Adopt EHRs*, *supra* note 66.

[199] *See* Press Release, *supra* note 10.