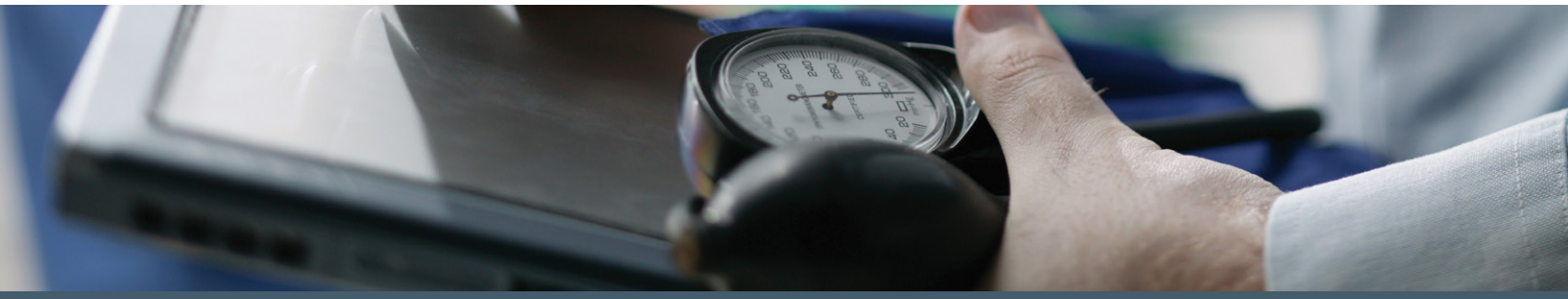
K&L GATES

QUI TAM QUARTERLY

EHR SYSTEMS: A STEP FORWARD FOR PATIENTS BUT A COMPLIANCE AND ENFORCEMENT MINEFIELD FOR HEALTH CARE PROVIDERS

By: Clifford C. Histed, Nora E. Becerra, and Cindy L. Ortega Ramos



Information is power, but the consequences of mismanaging information in the health care industry can be severe. Electronic Health Record (EHR) systems provide comprehensive real-time patient medical information in an electronic format that can be accessed instantly and securely by authorized users to promote management of diagnoses, medications, treatment plans, immunizations, and laboratory test results.

EHR systems have become widely used by health care providers in large part due to government initiatives such as the Health Information Technology for Economic and Clinical Health (HITECH) Act, which provided over US$35 billion in incentives to promote and expand the adoption and use of EHRs by eligible hospitals and providers.[1] As part of HITECH, CMS established an implementation plan for the rapid adoption and deployment of EHR systems. Commonly referred to as "meaningful use," the Medicare EHR Incentive Program contained specific requirements related to the use of EHR technology to improve the quality, safety, and efficiency of patient care. The EHR Incentive Program was transitioned to become one of the four components of CMS's Merit-Based Incentive Payment System (MIPS).[2]

Although the use of EHR systems by health care providers promises several benefits including improved patient care and decreased health care costs, system design issues and improper use of those systems have, in some cases, undermined the integrity of the health information and resulted in errors that may endanger patient safety and lead to serious regulatory risks. EHR systems have come under increased government scrutiny and have become one of the U.S. Department of Justice's (DOJ) priorities for health care-related enforcement due to the importance of these systems to the delivery of patient care and overall health care operations and their vulnerabilities to misuse. Accordingly, although EHR systems are an integral part of health care today, their functionalities and use have elevated risk for False Claims Act (FCA) and Anti-Kickback Statute (AKS) liability, and even criminal prosecution. Developers and users of EHR must remain well-informed about these risks and must be vigilant in managing them.

To date, DOJ's EHR-related enforcement has been varied. From false certification, straightforward false claims submissions related to the EHR Incentive Program, to punishing conduct where EHR's clinical decision support features were corrupted and violated the AKS, these cases give rise to liability under the FCA. DOJ recovered more than US$1.8 billion in settlements involving health care fraud and false claims in fiscal year 2020 and has emphasized how "complex EHR-related fraud schemes remain a focus of the Department's work."[3] In public remarks to the Federal Bar Association last year, the former head of DOJ's Civil Division—the litigating component responsible for supervising FCA litigation and implementing FCA enforcement policies nationwide—told attendees that health care providers should anticipate ongoing scrutiny in relation to their use of and representations related to EHR systems.[4]

Enforcement Overview

EHR-related enforcement cases outlined below can be broken down into specific categories. The first category involves "straightforward" false statement or kickback cases. The second category involves cases that directly implicate specific functions of EHR systems that

end-users employ to enable or cause the false claims. The third category involves cases where certification of the EHR software was obtained through fraud and misrepresentation, and so implicate the functionality of EHR but not the manner in which their features are employed by the system's end users.[5]

"Straightforward" False Statement and Kickback Cases

DOJ criminal prosecutors have used traditional tools like the criminal false statement statute to combat EHR-related fraud schemes, and the FCA continues to be a familiar and particularly effective weapon against straightforward bribery schemes.

Joe White

In January 2014, a federal grand jury returned an indictment against Joe White.[6] Unlike the other cases discussed in this article, individual criminal liability was at play here.[7] White was the chief financial officer and administrator for Shelby Regional Medical Center (Shelby Regional) in Center, Texas and was responsible for overseeing the implementation of its EHR system.[8] He was also responsible for attesting that Shelby Regional met the meaningful use requirement[9] necessary to qualify for payments under the EHR Incentive Program.[10] For EHR Incentive Program attestations to be legitimate, the EHR must fulfill the meaningful use requirement in real time; however, because Shelby Regional's staff had only minimally used the EHR platform in real time, White instructed them to input data from paper records into the EHR for the sole purpose of meeting the meaningful use criteria.[11] Therefore, using the EHR software as a mere "fill in the blanks" report after providing the services, and receiving incentive payments based on the attestation that the meaningful use requirement was met constituted a false claim. This is the conduct to which White pleaded guilty—making false statements in the form of false EHR attestations—and for which he was sentenced to 23 months in federal prison.[12] He was also ordered to pay restitution in the amount of US$4,483,089.09 to the EHR Incentive Program.[13]

Athenahealth, Inc.

In October 2017, DOJ filed a complaint against Athenahealth, Inc. (Athena).[14] The complaint charged Athena with thirty-five counts of FCA violations tied to AKS violations. The alleged violations stemmed from three Athena marketing programs.[15] First, Athena gave prospective and current customers all-expense-paid trips, including to premium sporting events.[16] Second, it had a "client referral incentive program" that rewarded current customers for identifying potential customers with up to US$3,000 per physician that signed up as a new customer.[17] Lastly, Athena entered into "conversion deals"[18] in which competing companies would refer their clients to Athena in exchange for compensation.[19] By engaging in this behavior, Athena knowingly caused its clients to submit false claims for EHR Incentive Program payments resulting in the Medicare program paying millions of dollars in improper incentive payments. [20]

In January 2021, DOJ announced that Athena entered into a settlement agreement in which it agreed to pay monetary penalties in the amount of US$18.25 million.[21] Additionally, Athena agreed to separate and account for all the unallowable costs[22] and not charge them to any government programs.[23] Lastly, Athena agreed that the United States was entitled to recoup any overpayment plus interest and penalties as a result of the previously submitted unallowable costs.[24] In announcing the settlement, the U.S. attorney's office said DOJ "will aggressively pursue organizations that fail to play by the rules; EHR companies are no exception."[25]

These cases demonstrate that unlawful marketing schemes involving EHR systems in violation of the AKS and "delayed use" reporting fall squarely within the FCA. Failing to use EHR software in real time defeats the goals of the EHR Incentive Program, and therefore, providers should have clear training and systems in place to ensure that their EHR use meets current EHR Incentive Program requirements.[26] Additionally, EHR vendors need to understand that, regardless of how the payments are characterized, any program that offers remuneration (as broadly defined by the AKS) to current or potential customers for the referral of their business—even EHR system business—will be subject to intense scrutiny. The AKS applies in full force in these cases.

FCA and AKS Liability Arising From Specific EHR Functionality

DOJ has brought cases that directly implicate specific functions of EHR systems that end users employ to enable or cause false claims to be submitted to federal health care programs.

Practice Fusion, Inc.

In January 2020, DOJ filed a criminal information against Practice Fusion, Inc.[27] The information charged Practice Fusion with one count of conspiracy to violate AKS and one substantive violation of AKS.[28] The government alleged that Practice Fusion solicited and received kickbacks from pharmaceutical companies, including at least one major opioid company, in exchange for implementing clinical decision support (CDS) alerts in Practice Fusion's EHR software. The alerts were designed to increase prescriptions for the pharmaceutical companies' products.

In exchange for what Practice Fusion called "sponsorship payments," Practice Fusion allowed pharmaceutical companies to participate in the design and development of its CDS alerts, some of which did not reflect accepted medical standards.[29] Practice Fusion apparently promoted the anticipated financial benefit to the pharmaceutical companies that would result from increased sales of their products based on the CDS alerts, and indeed, over a five-year period, health care providers wrote numerous prescriptions after receiving CDS alerts that the drug companies participated in designing. Specific to opioids, Practice Fusion solicited a payment of nearly US$1 million from an opioid company to create a CDS alert that was designed with input from the opioid company's marketing department. Practice Fusion marketed its "CDS sponsorship" to the opioid company as a valuable return on investment resulting from physicians prescribing more opioids.[30]

Practice Fusion also caused health care providers to submit false claims for EHR Incentive Program payments by misrepresenting the data portability capabilities of its EHR software, giving rise to separate FCA allegations.[31] Specifically, Practice Fusion falsely represented that its EHR software met Office of the National Coordinator for Health IT (ONC) health IT certification requirements related to data portability when several versions of its software did not. Additionally, Practice Fusion disabled the data portability feature after it received ONC certification. In fraudulently obtaining ONC certification for its EHR products, Practice Fusion caused health care providers to falsely attest their compliance with EHR Incentive Program requirements necessary to receive incentive payments.[32]

Practice Fusion entered into a deferred prosecution agreement in which it agreed to undertake important remedial steps and to pay US$26 million in criminal fines and the forfeiture of criminal proceeds.[33] In separate civil settlements, Practice Fusion agreed to pay civil penalties of over US$118 million to settle multiple allegations of violations of the False Claims Act.[34] Christina Nolan, then U.S. attorney for the District of Vermont, said "Practice Fusion's conduct is abhorrent. During the height of the opioid crisis, the company took a million-dollar kickback to allow an opioid company to inject itself in the sacred doctor-patient relationship so that it could peddle even more of its highly addictive and dangerous opioids."[35] The recovery in relation to the criminal charges was the largest criminal fine in the history of the District of Vermont and required Practice Fusion to admit its wrongs.[36]

The Practice Fusion criminal and civil cases call attention to the responsibility that health IT developers have in creating clinical-decision and other health IT tools for

use by health care providers in the delivery of clinical care. These cases also highlight the dangerous influence that profit, not only by health IT developers but also by companies who sell products to health care providers, can have on the development of health IT tools. These cases are a stern warning to health care providers to question and thoroughly research EHR vendors and other health IT developers before working with them. Health IT developers should be cautious about marketing their EHR technology as a tool for health care providers to increase revenue and should consider their own AKS and FCA risk even though they do not submit claims to the federal government directly. Health care providers and EHR vendors should work closely with legal counsel to ensure that all compliance and enforcement risks are thoroughly considered.

Misrepresentations Concerning EHR Functionality

Some EHR-related enforcement cases have involved the functionality of EHR software itself and not the manner in which end users employed the software's features. These cases include those where EHR vendors obtained certification through fraud and misrepresentation.

Greenway Health, Inc.

In February 2019, DOJ filed a complaint against Greenway Health, LLC (Greenway).[37] The complaint alleged that Greenway falsely obtained EHR Incentive Program certification, misrepresented the capabilities of its Prime Suite EHR (Prime Suite), and paid kickbacks to users who recommended its product.[38] Specifically, the government alleged that Greenway falsely obtained EHR Incentive Program certification for Prime Suite by concealing the fact that it failed to meet certain requirements for certification.[39] Additionally, Greenway's failure to meet certification requirements prevented health care providers using Greenway's EHR from meeting the requirements for

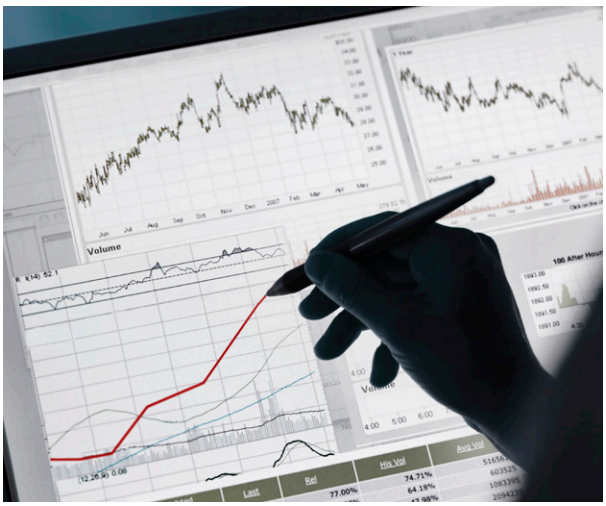
government incentive payments by incorrectly calculating the percentage of office visits for which its users distributed clinical summaries.[40]

Greenway agreed to pay US$57.25 million to settle the allegations.[41] In announcing the settlement, the government said, "This resolution demonstrates the department's continued commitment to pursue EHR vendors who misrepresent the capabilities of their products, and our determination to promote public health while holding accountable those who seek to abuse the government's trust."[42] As part of the settlement, Greenway also entered into a five-year corporate integrity agreement requiring Greenway to retain an outside entity to assess its quality control and compliance systems and to review Greenway's arrangements with healthcare providers to assure AKS compliance.[43]

eClinicalWorks, LLC

In May 2015, DOJ filed a complaint against eClinicalWorks, LLC (ECW) alleging that it misrepresented its software capabilities and paid US$392,000 in kickbacks to customers who promoted its product.[44] ECW allegedly failed to satisfy ONC certification criteria and made false statements in obtaining certification by concealing that its software did not comply with certification requirements.[45] As a result of its actions, ECW caused health care providers to submit false claims for federal incentive payments based on the use of ECW's software.[46]

The DOJ announced in 2017 that ECW would enter a settlement to resolve the allegations.[47] ECW was required to pay the government US$155 million to settle allegations concerning its misrepresentation of software capabilities and US$392,000 in kickbacks that ECW paid to customers who promoted its product.[48] The settlement includes a five-year corporate integrity agreement requiring ECW to retain an Independent Software Quality Oversight Organization to assess its software quality control systems, among other things.[49]



These cases further emphasize why health care providers should thoroughly evaluate EHR vendors and their products prior to entering into arrangements for the development or provision of EHR. If the EHR software does not meet EHR Incentive Program certification requirements, the health care providers using such EHR cannot attest to EHR Incentive Program compliance, as doing so will create potential FCA liability for any resulting claims. These cases further enforce that EHR vendors are not outside of the scope of the FCA and AKS.

Key Takeaways

EHR design, implementation, and certification attestation are a compliance and enforcement minefield for health care providers and administrators. In order to avoid impediments to high-quality patient care, disruptive and costly investigations, and potentially devastating enforcement actions, consider these important key takeaways:

Vigilance for instances of potential noncompliance is key, and due diligence of EHR system vendors and arrangements are now a key component of any fulsome compliance program.

EHR is a complex subject. Vigilance and stamina are required of health care practitioners and administrators to remain compliant. Providers should question and research EHR vendors thoroughly before making any commitment to work with them. Scrupulously vetting EHR manufacturers, vendors, and their software systems, including the "incentives" EHR vendors and manufacturers might provide, is key to avoid AKS issues in the future. EHR vendors should not market their software as a "health services increase tool," engage in incentive programs, or attempt marketing schemes that go back to incentives or referral payment.

For an additional layer of protection, providers should inquire into EHR vendor's and manufacturer's compliance programs and whether their software meets all of the government's requirements. Similarly, providers should employ qualified compliance staff and insist on competence and dedication from those hired. Establishing a compliance program or committee to oversee EHR's use can be a favorable factor if ever faced with an investigation.

The DOJ expects health care providers to engage in constant internal monitoring and expects them to self-report when something goes wrong. DOJ and the U.S. Department of Health and Human Service's message in this respect are clear and unmistakable. Therefore, the design, implementation, monitoring, and continuous improvement of your compliance program is nonnegotiable because your business could depend

on it. On that note, it is important to know that cooperation upon investigation is highly valued by the DOJ and considered when opposing a sanction.

Financial and reputational costs of noncompliance related to EHR systems are significant.

Providers should be aware that whistleblowers and relators are everywhere. Every patient, former patient, employee, former employee, or competitor can become a whistleblower or relator in search of a payday. This is important to note given that whistleblowers and relators have powerful legal and investigative tools and powerful financial incentives to use them. Similarly, it is crucial to understand that criminal prosecution is possible and that the government is eager to use its punitive tools under the right circumstances.

Providers and EHR vendors should work closely with their legal counsel to ensure a thorough diligence, compliance, and risk assessment of any business decision they would like to explore regarding the use, design, and functionality of EHR.

Our Health Care Fraud and Abuse group routinely assists providers and health care corporations with legal advice regarding FCA, Anti-Kickback Statute, and Stark Law compliance, including internal compliance reviews, transactional due diligence, external and internal investigations, and general strategic considerations. The group is specifically well-versed in handling EHR-related compliance and enforcement issues.

Endnotes

[1] The HITECH Act is part of the larger American Recovery and Reinvestment Act, an economic stimulus plan designed to, in part, improve the nation's health care delivery system by digitizing all patient records. *See* American Recovery and Reinvestment Act of 2009, H.R. 1, 111th Cong. (2009–2010), **www.congress.gov/bill/111th-congress/house-bill/1**.

[2] *See* Off. of the Nat'l Coordinator for Health Info. Tech., *Meaningful Use*, HealthIT.gov (Oct. 22, 2019), **https://www.healthit.gov/topic/meaningful-use-and-macra/meaningful-use.**

[3] Press Release, U.S. Dep't of Just., Justice Department Recovers Over $2.2 Billion from False Claims Act Cases in Fiscal Year 2020 (Jan. 14, 2021), **https://www.justice.gov/opa/pr/justice-department-recovers-over-22-billion-false-claims-act-cases-fiscal-year-2020**.

[4] David M. Maria & Trevor T. Garmey, *DOJ Civil Division Highlights False Claims Act Priorities for 2020*, *The Nat'l L. Rev.* (Mar. 30, 2020), **https://www.natlawreview.com/article/doj-civil-division-highlights-false-claims-act-priorities-2020**.

[5] While outside the scope of this article, there has also been EHR-related litigation concerning health care providers' failure to provide access to EHR records from individuals or their authorized representatives. Although the monetary penalties pale in comparison to the AKS and FCA penalties, the cases and underlying conduct are still relevant, and diligence is required to avoid this kind of liability. *See, e.g.*, Resolution Agreement, *U.S. Dep't of Health* & Hum. Servs. v. Hous. Works Inc. (July 22, 2020), **https://www.hhs.gov/sites/default/files/housing-works-signed-ra-cap.pdf**; Press Release, U.S. Dep't of Health & Hum. Servs., OCR Settles OCR Resolves Twentieth Investigation in HIPAA Right of Access Initiative with $80,000 Settlement (Sept. 10, 2021).

[6] *See* Indictment, United States of America v. Joe White, No: 6:14cr-00005-JDK-JDL, Eastern District of Texas (Jan. 22, 2014) [hereinafter *Indictment*].

[7] White submitted the attestation for Shelby Regional purporting to be the director of nursing and assistant administrator without having authority to do so. *See* Indictment Count I at ¶ 5.

[8] *Id.* at 5 ¶ 20, White, No: 6:14cr-00005-JDK-JDL.

[9] To receive incentive payments, Shelby Regional was required to meet all required objectives: (1) Computerized provider order entry; (2) Record demographics; (3) Maintain up-to-date problem list of current and active diagnoses; (4) Maintain active medication list; (5) Maintain active medication allergy list; (6) Report vital signs and chart changes; and (7) Record smoking status for patients 13 years or older. Indictment at ¶ 27.

[10] *Id.* at ¶ 20.

[11] *Id.* at ¶¶ 7–9.

[12] Press Release, U.S. Dep't of Just., Former Shelby County Hospital CFO Sentenced in EHR Incentive Case (June 17, 2015), **https://www.justice.gov/usao-edtx/pr/former-shelby-county-hospital-cfo-sentenced-ehr-incentive-case**.

[13] *Id.*

[14] First Amended Complaint, *United States of America ex el. Sanborn v. AthenaHealth, Inc.*, No. 1:17-cv-12543-GAO (D. Mass. Dec. 22, 2017).

[15] *Id.*

[16] *See* Complaint in Intervention at ¶¶ 4, 37–50, Athena, No. 1:17-cv-12543-ADB; No. 1:17-cv-12125-ADB (Jan. 25, 2021).

[17] *Id.* at ¶¶ 5, 51–61.

[18] "Conversion deals" are agreements entered into with competing companies that have decided to discontinue their service or product and agree to refer their clients to another competitor in exchange for compensation for each successful converted customer.

[19] See Complaint in Intervention at ¶¶ 6, 62–69, Athena, No. 1:17-cv-12543-ADB; No. 1:17-cv-12125-ADB (Jan. 25, 2021).

[20] Id. at ¶ 70.

[21] Settlement Agreement, Press Release, U.S. Dep't of Just., Athenahealth Agrees to Pay $18.25 Million to Resolve Allegations that It Paid Illegal Kickbacks, (Jan. 28, 2021), **https://www.justice.gov/usao-ma/press-release/file/1361181/download**.

[22] The settlement agreement defines unallowable costs as: "All costs . . . incurred by or on behalf of Athena, its employees, and its agents in connection with: (1) the matters covered by this Agreement; (2) the United States' audit(s) and civil and any criminal investigation(s) of the matters covered by this Agreement; (3) Athena's investigation, defense, and corrective actions undertaken in response to the United States' audit(s) and civil and any criminal investigation(s) in connection with the matters covered by this Agreement (including attorney's fees); (4) the negotiation and performance of this Agreement; and (5) the payment Athena makes to the United States pursuant to this Agreement." See Settlement Agreement, **https://www.justice.gov/usao-ma/press-release/file/1361181/download**.

[23] Press Release, U.S. Dep't of Just., Athenahealth Agrees to Pay $18.25 Million to Resolve Allegations that It Paid Illegal Kickbacks, (Jan. 28, 2021), **https://www.justice.gov/usao-ma/pr/athenahealth-agrees-pay-1825-million-resolve-allegations-it-paid-illegal-kickbacks**.

[24] *Id.*

[25] *Id.*

[26] The Medicare EHR Incentive Program (commonly referred to as meaningful use) transitioned to CMS's MIPS as part of the Medicare Access and CHIP Reauthorization Act (MACRA). *See* Off. of the Nat'l Coordinator for Health Info. Tech., *Meaningful Use*, HealthIT.gov (Oct. 22, 2019), **https://www.healthit.gov/topic/meaningful-use-and-macra/meaningful-use.**

[27] *See* Criminal Information, *United States of America v. Practice Fusion, Inc.*, No. 2:20-cr-00011 (D. Vt. Jan. 27, 2020).

[28] *Id.*

[29] *See* Press Release, U.S. Dep't of Just., Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations (Jan 27, 2020), **https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0.**

[30] *Id.*

[31] *See* Criminal Information, *United States of America v. Practice Fusion, Inc.*, No. 2:20-cr-00011 (D. Vt. Jan. 27, 2020); *see also* Deferred Prosecution Agreement, *United States of America v. Practice Fusion, Inc.*, No. 2:20-cr-00011-wks (D. Vt. Jan. 27, 2020).

[32] *Practice Fusion, Inc.*, No. 2:20-cr-00011; see also Press Release, U.S. Dep't of Just., Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations (Jan 27, 2020), **https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0.**

[33] *See* Criminal Information, United States of America v. Practice Fusion, Inc., No. 2:20-cr-00011 (D. Vt. Jan. 27, 2020); see also Deferred Prosecution Agreement, United States of America v. Practice Fusion, Inc., No. 2:20-cr-00011-wks (D. Vt. Jan. 27, 2020).

[34] See Press Release, U.S. Dep't of Just., Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations (Jan 27, 2020), **https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0**.

[35] *Id.*

[36] *Id.*

[37] *See* Complaint, *United States v. Greenway Health, LLC*, No. 2:19-cv-00020 (D. Vt. Feb. 06, 2019).

[38] *Id.* at ¶ 5.

[39] *Id.* at ¶ 6.

[40] *Id.* at ¶ 83.

[41] Press Release, U.S. Dep't of Just., Electronic Health Records Vendor to Pay $57.25 Million to Settle False Claims Act Allegations (Feb. 6, 2019), **https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-5725-million-settle-false-claims-act-allegations**.

[42] *Id.*

[43] *Id.*

[44] *See* Complaint, *United States v. eClinicalWorks*, No. 2:15-cv-00095-wks (D. Vt. May 1, 2015).

[45] *See* Complaint in Intervention, *eClinicalWorks*, No. 2:15-cv-00095-wks (D. Vt. May 12, 2017); More specifically, the government alleged that *eClinicalWorks* modified its software by "hardcoding" only the drugs codes required for testing, it did not accurately record user actions in an audit log, and that it failed to satisfy data portability requirements intended to permit healthcare providers to exchange information between different EHR software. *Id.* ¶ 44.

[46] *Id.* at ¶ 87.

[47] Press Release, U.S. Dep't of Just., Electronic Health Records Vendor to Pay $155 Million to Settle False Claims Act Allegations (May 31, 2017), **https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations**.

[48] *Id.*

[49] *Id.*

Authors

Clifford C. Histed

Partner

Chicago
+1.312.807.4448
clifford.histed@klgates.com

Cindy L. Ortega Ramos

Associate

Chicago
+1.312.807.4322
cindy.ortega@klgates.com

Nora E. Becerra

Associate

Chicago
+1.312.807.4222
nora.becerra@klgates.com

Members of our team are regular contributors to Triage: Timely Conversations for Health Care Professionals, a podcast created by K&L Gates to inform our clients and friends of the firm about the latest developments in health law.

Subscribe to Triage through **Apple Podcasts**, **Google Podcasts**, and **Spotify** to have our episodes delivered directly to you as they become available.

Learn more about our Health Care Fraud and Abuse practice at klgates.com/Health-Care-Fraud-and-Abuse-US-Practices.

22952