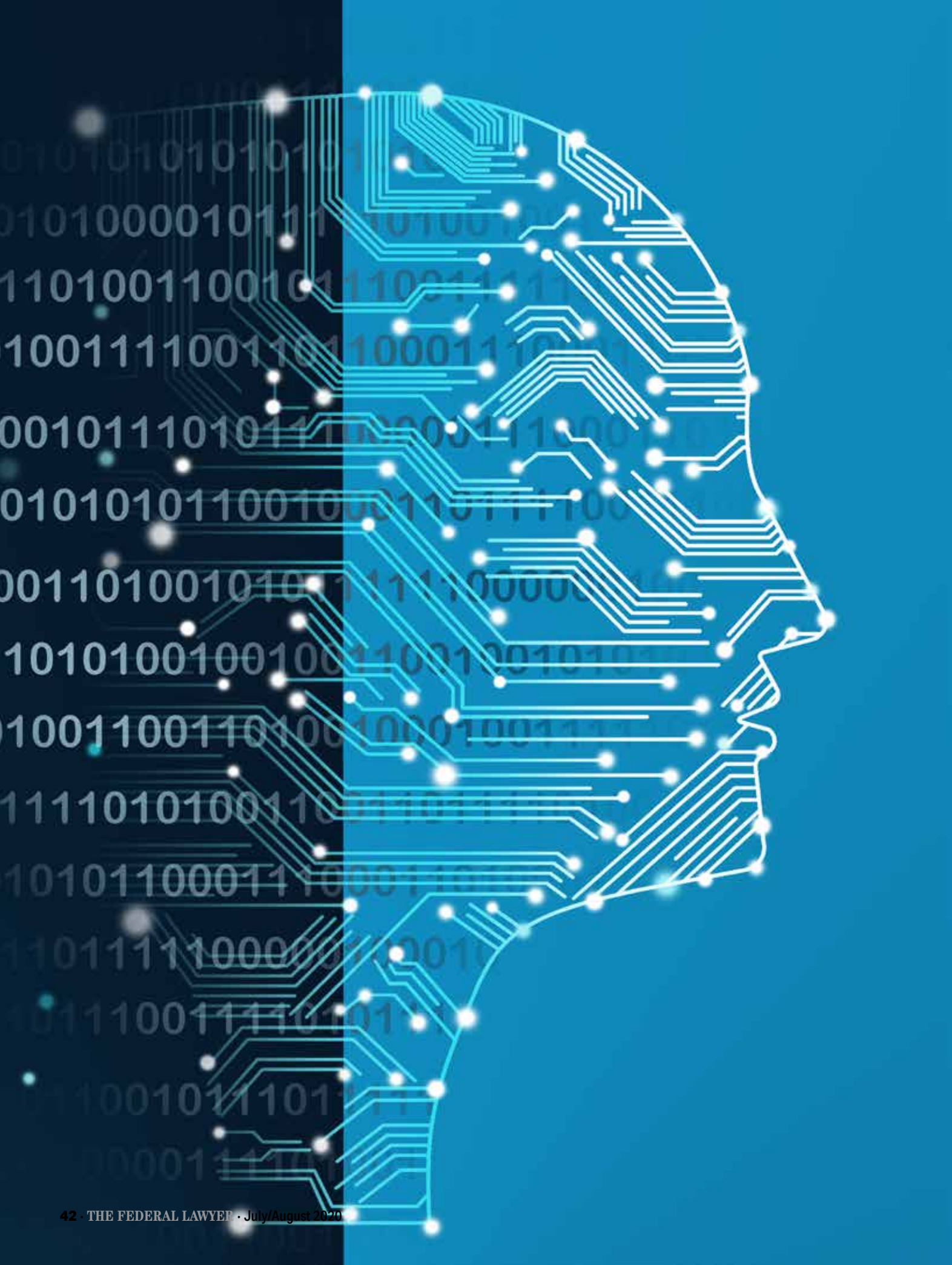

Big Data Makes Big Cases: How Data Analytics Is Shaping False Claims Act Enforcement

JASON MEHTA AND JENNIFER A. SHORT

As many practitioners have learned over the last few decades, the False Claims Act (FCA) is an emerging arsenal in the tool of government prosecutors. And whistleblower attorneys are taking notice and filing a large number of cases. Over the past decade, annual recoveries under the FCA have averaged more than $3 billion per year.[1] Equally impressive is the number of whistleblower actions entering the FCA pipeline—roughly 650 new *qui tam* matters are filed each year.

While these figures have remained fairly steady since 2010, the statistics do not reveal the evolutionary changes in *who* is "blowing the whistle," *what* information they are bringing in support of their claims, and *how* the government is investigating and supporting FCA actions. The *qui tam* relator role is no longer reserved for the prototypical insider or disgruntled employee envisioned when Congress strengthened the FCA's whistleblower provisions in 1986. Increasingly, FCA cases are being filed by corporate relators who have filtered and analyzed vast swaths of data to identify their target defendants. The government, too, has pursued a number of initiatives in recent years that proactively use data analytics to identify problematic conduct in certain sectors. And, while data alone certainly is not sufficient to prove an FCA violation, it can be powerful supporting evidence of wrongdoing as well as the basis for large financial recoveries.[2]

This article looks at the use of data mining in FCA prosecutions, specifically *qui tam* cases, and highlights several high-profile fraud cases built on data. In light of these developments, the article also offers practical advice to those who do business with, or receive payments from, the government on how to use data mining to mitigate risk, encourage compliance, and—if necessary—defend against FCA liability.

Data Mining in Government Investigations

The concept of data mining is not new. For years, private industry has been using sophisticated algorithms and software to mine large sources of data to identify patterns and highlight trends.[3] The government has followed suit, most publicly and proactively in healthcare fraud initiatives, but also in investigating and prosecuting financial, procurement, and other types of fraud cases.

Using Healthcare Claims Data to Find Trends and Target Outliers

The U.S. government has a vast array of healthcare data available at its fingertips. Each time a healthcare provider submits a claim to Medicare or Medicaid, for example, the provider feeds dozens of pieces of information to regulators, including the patient's name and date of birth, the place and date of service, the current procedural terminology (CPT) code that describes the service provided, and the supporting diagnosis code. Electronic Health Record (EHR) systems have the capacity to collect even more information that can become subject to government inquiries and oversight.

The government routinely looks to healthcare claims data to identify patterns of potential fraud and to substantiate (or disprove) allegations of fraudulent billing. Indeed, the Department of Health and Human Services (HHS) Office of Inspector General (OIG)—the federal agency most directly tasked with overseeing the Medicare program—prides itself on its data analytics team. In its own words,

"OIG uses Data Driven Decision Making to produce outcome focused results."[4] Further, OIG notes that it "leverages sophisticated data analysis to identify and target potential fraud schemes and areas of program waste and abuse."[5]

Through the Medicare Fraud Strike Force, an initiative that began in 2007, HHS-OIG joined forces with the FBI and the Department of Justice (DOJ) to leverage the available data in pursuing nationwide and industrywide healthcare fraud schemes.[6] The stated goal of the Strike Force (now one component of the Health Care Fraud Prevention and Enforcement Action Team, or HEAT) was to "shift[]from a 'pay and chase' approach toward fraud prevention" in healthcare.[7]

One of the most far-reaching examples of the use of data mining occurred in 2015, when the government examined the billing practices of compound pharmacies on an industrywide basis. Compound pharmacies were targeted for investigation due to an atypical and aberrant spike in billing to the TRICARE program, as identified in government reporting. The government used a panoply of data tools to identify "outlier" pharmacies and providers—that is, providers whose prescribing and fulfilling patterns stood out relative to their peers. Investigators looked at trend analyses, top-billing pharmacies, and pharmacies with relatively few prescribers responsible for large numbers of claims. After flagging more than $1 billion in suspect pharmaceutical claims, DOJ pursued and recovered tens of millions in FCA payments from the most egregious offenders.[8]

More recently, the government has used its data assessment capabilities to support DOJ's opioid initiative, announced by then-Attorney General Sessions in 2018. In an oft-repeated speech, Attorney General Sessions proudly promoted the Opioid Fraud and Abuse Detection Unit, a new data analytics program that focuses on opioid-related healthcare fraud. In his words, this unit uses data and data-mining techniques to "tell us important information—who is prescribing the most drugs, who is dispensing the most drugs, and whose patients are dying of overdoses."[9]

The results—with respect to opioid cases in particular—have been staggering, and the effort is ongoing. In June 2018, more than 600 individuals were arrested on charges related to an estimated $2 billion in false billing for opioid prescriptions.[10] The following year, opioid manufacturer Insys Therapeutics reached a settlement regarding its role in the national crisis and agreed to pay $195 million to resolve a number of FCA actions that had been filed against it.[11] Shortly thereafter, in July 2019, Reckitt Benckiser Group paid $1.2 billion to settle both criminal and civil charges stemming from its marketing of an opioid treatment drug.[12] And in January 2020, an electronic health records vendor reached a $118.6 million settlement with the federal government and several states to resolve FCA charges that it had solicited and accepted kickbacks from opioid and other pharmaceutical companies in exchange for embedding "alerts" in the records software that were designed to encourage and increase unnecessary prescriptions.[13] Government officials have noted the importance of data analytics to these enforcement efforts.[14]

Beyond Healthcare—Use of Data in Other Enforcement Contexts

The government is making increasing use of data mining to aid enforcement in areas other than healthcare, too. In the wake of the 2008 financial crisis, for example, DOJ created a Financial Fraud Enforcement Task Force that, among other things, examined government-backed housing loans and default information to pursue FCA and other charges against some of the country's largest mortgage lenders.[15] The effort led to nearly $2 billion in recoveries in 2016 alone. DOJ also has warned that it is using data analytics in securities and market manipulation investigations and prosecutions.[16]

In a similar vein, in November 2019, DOJ launched a Procurement Collusion Strike Force (PCSF), which focuses on potential antitrust violations by government contractors.[17] In announcing the Strike Force, the assistant attorney general specifically noted: "The Strike Force will work on ways to improve our use of data analytics programs to identify potential 'red flags' of collusion in government procurement data. Many investigative agencies individually have made great strides on this front, and the PCSF will serve to facilitate collaboration and the sharing of best practices between these agencies."[18] Although the PCSF is driven by criminal antitrust concerns, its creation was no doubt driven by the criminal cases *and* civil FCA settlements that DOJ reached with a number of South Korean companies that had engaged in bid-rigging on Department of Defense fuel supply contracts.[19]

In addition to putting companies on notice that the government is using data analytics to investigate areas of potential fraud, DOJ officials have noted that companies within target industries can use similar analytical approaches to monitor their compliance internally:

> Whereas we are able to identify indicators and anomalies from market-wide data, companies have better and more immediate access to their own data. For that reason, if misconduct does occur, our prosecutors are going to inquire about what the company has done to analyze or track its own data resources—both at the time of the misconduct, as well as at the time we are considering a potential resolution.[20]

Data Analytics in Individual FCA Investigations and Prosecutions

Government investigators and attorneys also routinely examine datasets on a more defendant- or case-specific level to test whether allegations of fraud are consistent with the data. These inquires also help develop evidence that can be used either in settlement discussions or at trial. Once more, the Medicare claims data, which is available to DOJ attorneys and law enforcement agents, provides the most familiar examples. For instance, a DOJ attorney might ask whether the Medicare claims data reveals a pattern or concentration of referring or prescribing physicians for reimbursable lab tests or pharmaceuticals. Does the patient population for the service or testing make sense clinically, or does the data suggest that the services were medically unnecessary?[21] Did a provider routinely use a higher reimbursement code in its billing when a less expensive service was likely used (a practice known as "upcoding")?[22]

Even where the government does not have the necessary data at its fingertips, it may seek data from a target company via subpoena or Civil Investigative Demand. For example, a company selling commercial items through a General Services Administration (GSA) schedule contract might be asked to provide sales and pricing data for both its government and private sector sales so that investigators can query whether the company complied with discount disclosure requirements and the contract's pricing requirements.[23]

Data comes into play again after the government's investigation substantiates a suspected FCA violation and the question of potential damages arises. Medicare claims data, for example, can reveal how much was actually paid on a set of allegedly false claims. Likewise, sales data can be used in a GSA pricing case to determine how much

the government may have overpaid for commercial items because of an asserted failure to comply with the contractual pricing formula. And, although a detailed discussion is beyond the scope of this article, the use of statistical sampling to support FCA liability and damages claims remains an active and controversial subject among practitioners in this area.[24]

Whistleblowers' Use of Data to Bring Cases

The government is not alone in using data to identify potential FCA violations and develop cases. Whistleblowers and their counsel are using information creatively to find and file *qui tam* actions. These cases are not based on an individual's insider knowledge of a company's practices, but on a strategic analysis of available data. The "whistleblower" in these cases might be a competitor company, an industry advisor, or even an entity created for the purpose of identifying potential FCA actions. This phenomenon has been around for a while—in 1996, an entity named Health Outcomes Technology mined publicly available Medicare and Medicaid claims data to file FCA claims against nearly a hundred hospitals that showed up as outliers in the numbers of complex pneumonia cases being billed.[25]

A more recent example of data-driven relators is Integra Med, a data analytics firm based in Austin, Texas, which filed a number of *qui tam* actions in various jurisdictions based on the company's analysis of Medicare claims data.[26] Integra Med described itself as a company that "specializes in using statistical analysis to uncover and prove fraud."[27] In its more recent cases, Integra Med indicated that it analyzed Medicare inpatient claims data from 2011 through 2017 to determine statistical abnormalities and potential areas of fraud.[28] Intriguingly, courts that have analyzed Integra Med's role as a relator have acknowledged that the company is not "a prototypical FCA relator in that it had no insider relationship with Defendants," but found that fact "is not enough to bar its suit."[29]

While Integra Med has been able to allege statistical variances in its billing analysis, it has been seemingly unable to convince the government to intervene in either of its two recent healthcare data mining cases. And, Integra Med has not fared much better on its own. Courts in both Texas and California have recently stymied Integra Med's ability to pursue these theories on their own—generally finding that data analysis by itself is not enough to overcome the federal pleading standards required for fraud cases.[30] The implicit suggestion, therefore, seems to be that data analysis alone is insufficient to bring a case past the motion to dismiss hurdle. Successful relators will likely need more than just simply data metrics—they will need data plus information related to scienter and the actual quintessential "who, what, where, when, and why" of the alleged fraud scheme.

Another illustrative example of the pioneering use of data is a series of nearly a dozen FCA cases filed by the National Health Care Analysis (NHCA) Group. The founder of the NHCA Group, John Mininno, made a series of explosive allegations prior to filing any of these *qui tam* suits in an article titled "Medicare Scammers Steal $60 Billion a Year. This Man Is Hunting Them."[31] In the article, Mininno was described as a "big-data entrepreneur,"[32] and he recalled that when the Centers for Medicare & Medicaid Services made healthcare data available to the public, he viewed it as "a massive business opportunity," specifically with regard to *qui tam* suits.

In total, the approximately dozen NHCA lawsuits named 38 defendants and purportedly implicated "more than 73 million prescriptions written by hundreds of thousands of different physicians for millions of different Medicare beneficiaries."[33] DOJ ultimately moved to dismiss the lawsuits, alleging that the relator's investigations were without merit and were "contrary to the public interest."[34] While DOJ was mostly successful in dismissing these suits, at least one of these matters is still pending.[35]

The effect of the NHCA lawsuits remains to be seen, but it seems to bolster the findings of the Integra Med cases—data mining, by itself, will not be sufficient to whet the government's interest to intervene in a FCA case. Nonetheless, it seems likely that future relators will continue exploring the contours of data mining and buttressing data with other, more quintessential "whistleblower" evidence.

Limitations on Data Mining

Any discussion on the use of data mining and its ability to affect government FCA prosecutions must necessarily include a conversation on data's limitations. While the ability to mine millions of rows of data is no doubt impressive and revolutionary, it is not the be-all, end-all panacea to rooting out alleged fraud. We highlight three particular limitations of data.

First, data by itself does not necessarily prove any material falsity. For example, when a physician is an outlier in the number of procedures ordered, there is nothing inherently false in the ordering of those procedures. After all, someone always needs to be the number one performer or biller. Similarly, when a bank underwrites more FHA-backed loans that default compared to other banks, that data alone does not prove that anything false occurred that would trigger liability under the FCA.

While this idea—that data mining does not necessarily prove falsity—is intuitive, the temptation to overly extrapolate meaning into data is a concern. Very often, in the course of advocacy, lawyers (on all sides) impute meaning into statistical variations. While most statistics students can detect the difference between correlation and causation in a purely analytical method, lawyers often blur these distinctions in the context of advocacy. Therefore, while this might be an obvious point, it is an important one—data is often a starting point for an investigation rather than a defining conclusion of an investigation.

Second, and related to the first point, data analytics generally do not provide direct evidence of FCA scienter (knowledge, actual or reckless disregard). In this respect, the FCA punishes only those actions that are made "knowingly." Mere mistakes or negligence is not actionable under the FCA. Thus, for example, even when a physician submits false claims, these claims are not necessarily actionable. Further, certain patterns that might be apparent in the context of data mining could simply be the result of repeated innocent mistakes. Therefore, data should not necessarily be used to prove scienter.

Nonetheless, when other evidence—either direct or circumstantial—supports the knowledge and falsity elements of an FCA claim, the data can provide powerful supporting and consistent evidence. Further, if the data was available to a defendant but it did not look at or analyze its own conduct, the defendant's intent might be questioned. For example, if the problem or issue was known in the industry as a risk area, or if the defendant was required by contract or regulation to track its compliance, then a failure to do so might be construed as deliberate ignorance. Therefore, data can be used to buttress scienter evidence, but it is often used as just that—buttressing evidence, rather than being definitive conclusory evidence.

Third, we caution that that relators, in particular, need to be

cautious about over-reliance on publicly available data. As the above case examples of Integra Med and NHCA prove, data alone often is insufficient to whet the government's appetite for intervention. But, more fatally, it is possible that courts will subsequently find that pure data analysis is insufficient to overcome the FCA's public disclosure bar. As a general matter, the FCA's public disclosure bar prohibits relators from pursuing FCA cases where their information has already been publicly disclosed. While the threshold for a public disclosure bar was reduced under the amendments as part of the Affordable Care Act, the bar nonetheless does still preclude relators from pursuing cases unless they can show that they have "materially added" to publicly disclosed information. It remains an open question whether data mining publicly available data will be sufficient to overcome the public disclosure bar's requirements.

Practical Compliance Tips for All Attorneys

In light of the government's and relators' focus on data analysis, potential target companies and their counsel should consider adapting their practices and incorporating compliance measures to reflect and protect against this new wave of cases. Below are several practical tips to get ahead of the curve.

First, as a threshold matter, understand the emergence of data-driven analysis. By recognizing that regulators are increasingly harnessing and using the power of data to identify outliers, healthcare providers and contractors can begin the process of undertaking proactive steps to ensure maximum compliance and reduce their risk.

Second, to the extent it is not done already, take measures to collect and store relevant data. On the defense side, while most healthcare providers are already collecting some data, it is a best practice to ensure that clients have a system in place to capture as much relevant data as possible. Information is power. On the relator side, attorneys should be asking their clients about what data they might have and how that data might illustrate—or even prove—the allegations.

Third, all attorneys should educate their clients about the need to teach downstream employees about the importance of data collection and data analysis. One of the most critical pieces to harnessing and leveraging the power of data is to educate employees about the importance of accurate data collection. This means teaching physicians, for example, to accurately collect data from patient encounters. It means teaching billers and coders about including all relevant fields, even if those fields might not ultimately be billed. Most practices start—with good reason—at proper collection of claims information; however, a best practice is to collect not only claims information but also relevant fields on patients' clinical records (e.g., medications, imaging studies, lab reports), as well as other external data (e.g., prescriptions, financial information.)

Fourth, attorneys should appreciate the importance of data cleanliness. Just like most clinicians understand the importance of cleanliness in the operating room, so too must healthcare providers understand the importance of cleanliness in data. Remember the adage of "garbage in, garbage out." Unless the healthcare data is accurate when entered, the data cannot be relied upon afterwards. Therefore, providers must constantly clean or scrub data to ensure that it is accurate, correct, consistent, relevant, and not corrupted. And, relator attorneys who mine this data should be careful that the data they are searching is reliable, accurate, and up to date. Nothing is more harmful to a case than relying on antiquated or inadequate information.

Fifth, compliance counsel using data to build a case for their clients must always remember that the data is only as good as the query. To get a meaningful understanding of data to build a successful defense, compliance counsel needs to have access to the right data and query this data correctly. Looking at a million fields of data doesn't mean much—it means only something in context. Thus, a best practice is to start at the end: ask what information is ultimately wanted. If counsel wants to know what providers are billing the most procedures, for example, they would need to focus on billing data. If counsel is interested in suspicious kickback arrangements, they would need to review billing data in concert with financial data. Similarly, relator counsel should make sure that, when mining their clients' own data for purposes of bringing forth a case, the counsel are using proper queries designed to get the right results.

In addition to the above, healthcare providers need to take care to comply with data privacy obligations under the Health Insurance Portability and Accountability Act (HIPAA) and many state statutes.[36] Remember that HIPAA's protections and mandates apply to aggregated data just like they apply to individual patient files. Therefore, follow the HIPAA security requirements—such as authentication protocols and control over access to protect the data.[37] One best practice is to consider housing a de-identified dataset. The benefit is that it removes the patient identifiers and, therefore, might be exempt from HIPAA's mandates. As such, this might allow for easier access in manipulating and analyzing the data.

Conclusion

The emergence of data analytics is changing business as usual across all industries, and the government healthcare enforcement space is no exception. By understanding the government and relators' focus on data analytics, and by implementing practical suggestions to use data as both a proactive compliance tool and a reactive defense, relators can better present their arguments, and healthcare clients can better defend themselves during the inevitable inquiry. ⊙

Jason Mehta is a partner at Bradley Arant Boult Cummings, LLP in Tampa, Fla. Jennifer A. Short is a partner at KaiserDillon, PLLC in Washington, D.C. Mehta and Short are both former assistant U.S. attorneys who prosecuted healthcare and procurement fraud matters under the False Claims Act. They now advise individuals and corporations in civil and criminal investigations and litigation.

Endnotes

[1]*See Justice Department Recovers over $3 Billion from False Claims Act Cases in Fiscal Year 2019* (Jan. 9, 2020), https://www.justice.gov/opa/pr/justice-department-recovers-over-3-billion-false-claims-act-cases-fiscal-year-2019.

[2]*See, e.g., United States Settles False Claims Act Allegations Against Jacksonville-Based Fertility* (Apr. 10, 2015), https://www.justice.gov/usao-mdfl/pr/united-states-settles-false-claims-act-allegations-against-jacksonville-based-fertility ("This case was developed by proactively mining healthcare reimbursement data. In mining through this data, the Center was identified as a top biller of fertility related treatments. In addition, through this data mining, government investigators were able to determine that the Center

had billed for services allegedly rendered by Dr. Fox – the owner of the practice – even when he was out of the country."); *see also Four Area Hospitals Pay Millions to Resolve Ambulance Swapping Allegations* (Oct. 4, 2017), https://www.justice.gov/usao-sdtx/pr/four-area-hospitals-pay-millions-resolve-ambulance-swapping-allegations ("Among the tools instrumental to the settlement were those provided by HHS-OIG's Chief Data Office, Consolidated Data Analysis Center (CDAC). CDAC provides HHS-OIG and its law enforcement partners with best practices, consultancy and skills development in data mining, predictive analytics and data management and modeling in support of fraud prevention and recovery.").

[3]*See, e.g., International Educational Data Mining Society,* http://www.educationaldatamining.org/; Bernard Marr, Forbes, *How Big Data and Analytics Are Transforming the Construction Industry* (Apr. 19, 2016), https://www.forbes.com/sites/bernardmarr/2016/04/19/how-big-data-and-analytics-are-transforming-the-construction-industry/#1dadc10933fc; Dan Patterson, TechRepublic, *How Nonprofits Use Big Data to Change the World* (Feb. 8, 2017), https://www.techrepublic.com/article/how-nonprofits-use-big-data-to-change-the-world/.

[4]*HHS-OIG Semi-Annual Report to Congress,* Oct. 1, 2018–Mar. 31, 2019, https://oig.hhs.gov/reports-and-publications/archives/semiannual/2019/2019-spring-sar.pdf.

[5]*See HHS-OIG Justification of Estimates for Appropriations Committees for Fiscal Year 2019,* https://oig.hhs.gov/reports-and-publications/archives/budget/files/2019budget.pdf.

[6]*Fact Sheet: The Health Care Fraud and Abuse Control Program Protects Consumers and Taxpayers by Combating Health Care Fraud* (Feb. 26, 2016), https://www.justice.gov/opa/pr/fact-sheet-health-care-fraud-and-abuse-control-program-protects-conusmers-and-taxpayers.

[7] *Id.*

[8]*See, e.g., United States Settles False Claims Act Allegations Against Compound Pharmacy Owner For $4.25 Million* (Oct. 21, 2016), https://www.justice.gov/usao-mdfl/pr/united-states-settles-false-claims-act-allegations-against-compound-pharmacy-owner-425 ("This case was developed through an initiative to track and prosecute compound pharmacies that submitted millions of dollars in improper claims to the TRICARE program. The government estimates that up to $2 billion of tainted and unnecessary compound prescriptions had been submitted to and paid by the government. In the Middle District of Florida, the government has recovered almost $70 million in fines and penalties over the past 18 months.").

[9]*Attorney General Sessions Delivers Remarks Regarding Trump Administration's Response to Opioid Epidemic* (Mar. 22, 2018), https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-trump-administrations-response-opioid-epidemic.

[10]*See National Health Care Fraud Takedown Results in Charges Against 601 Individuals Responsible for Over $2 Billion in Fraud Losses* (June 28, 2018), https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-601-individuals-responsible-over ("In many cases, doctors, nurses, and pharmacists take advantage of people suffering from drug addiction in order to line their pockets. These are despicable crimes. That's why this Department of Justice has taken historic new steps to go after fraudsters, including hiring more prosecutors and leveraging the power of data analytics.").

[11]*Opioid Manufacturer Insys Therapeutics Agrees to Enter $225 Million Global Resolution of Criminal and Civil Investigations* (June 5, 2019), https://www.justice.gov/opa/pr/opioid-manufacturer-insys-therapeutics-agrees-enter-225-million-global-resolution-criminal?utm_medium=email&utm_source=govdelivery.

[12]*Justice Department Obtains $1.4 Billion from Reckitt Benckiser Group in Largest Recovery in a Case Concerning an Opioid Drug in United States History* (July 11, 2019), https://www.justice.gov/opa/pr/justice-department-obtains-14-billion-reckitt-benckiser-group-largest-recovery-case.

[13]*Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigation* (Jan. 27, 2020), https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0.

[14]*See, e.g.,* Byron Tau and Aruna Viswanatha, *Investigators Use New Strategy to Combat Opioid Crisis: Data Analytics,* Wall Street Journal (Aug. 26, 2019), https://www.wsj.com/articles/investigators-use-new-strategy-to-combat-opioid-crisis-data-analytics-11566811803.

[15]*See, e.g., Wells Fargo Bank Agrees to Pay $1.2 Billion for Improper Mortgage Lending Practices* (Apr. 8, 2016), https://www.justice.gov/opa/pr/wells-fargo-bank-agrees-pay-12-billion-improper-mortgage-lending-practices; *Manhattan U.S. Attorney Sues And Settles With JPMorgan Chase For $614 Million For Fraudulent Mortgage Lending Practices* (Feb. 4, 2014), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-sues-and-settles-jpmorgan-chase-614-million-fraudulent-mortgage.

[16]*See, e.g.,* Dan Mangan, *Federal prosecutors, Commodity Regulators Broaden Market Manipulation Probe Beyond Precious Metals Trades,* CNBC (Sept. 18, 2019), https://www.cnbc.com/2019/09/18/federal-prosecutors-regulators-broaden-market-manipulation-probe.html (noting government's use of data to detect "spoofing" in commodities trading).

[17]*Assistant Attorney General Makan Delrahim Delivers Remarks at the Procurement Collusion Strike Force Press Conference* (Nov. 5, 2019), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-procurement-collusion-strike.

[18]*Id.*

[19]*Three South Korean Companies Agree to Plead Guilty and to Enter into Civil Settlements for Rigging Bids on United States Department of Defense Fuel Supply Contracts* (Nov. 14, 2018), https://www.justice.gov/opa/pr/three-south-korean-companies-agree-plead-guilty-and-enter-civil-settlements-rigging-bids.

[20]*Deputy Assistant Attorney General Matthew S. Miner Delivers Remarks at the 6th Annual Government Enforcement Institute* (Sept. 12, 2019), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-delivers-remarks-6th-annual-government.

[21]*See, e.g., Millennium Health Agrees to Pay $256 Million to Resolve Allegations of Unnecessary Drug and Genetic Testing and Illegal Remuneration to Physicians* (Oct. 19, 2015), https://www.justice.gov/opa/pr/millennium-health-agrees-pay-256-million-resolve-allegations-unnecessary-drug-and-genetic.

[22]*See, e.g., Careall Companies Agree to Pay $25 Million to Settle False Claims Act Allegations* (Nov. 12, 2014), https://www.justice.gov/opa/pr/careall-companies-agree-pay-25-million-settle-false-claims-act-allegations (resolution of charges that defendant submitted upcoded claims for home health services).

[23]*See, e.g., Informatica Agrees to Pay $21.57 Million for Alleged*

False Claims Caused by Its Commercial Pricing Disclosures (May 13, 2019), https://www.justice.gov/opa/pr/informatica-agrees-pay-2157-million-alleged-false-claims-caused-its-commercial-pricing (allegations that defendant provided misleading information in GSA contract negotiations, resulting in overcharges to the government).

[24]https://southerncalifornialawreview.com/2018/03/01/statistical-sampling-used-prove-liability-false-claims-act-healthcare-fraud-note-milene-vega/.

[25]*See, e.g., Rhode Island-Based Hospital to Pay $400,000 to Settle Health Care Fraud Allegations* (Oct. 17, 2002), https://www.justice.gov/archive/opa/pr/2002/October/02_civ_599.htm. The government investigated the relator entity's allegations hospital-by-hospital and reached settlements with most over a number of years before intervening in the *qui tam* case. The slimmed-down lawsuit itself suffered from procedural issues that eventually caused it to be dismissed.

[26]*See, e.g., U.S. ex rel. Integra Med Analytics LLC v. Baylor Scott & White Health*, 17-CV-0886 (W.D. Tex.), and *U.S. ex rel. Integra Med Analytics LLC v. Providence Health Services*, 17-CV-01694 (C.D. Cal.).

[27]*U.S. ex rel. Integra Med Analytics LLC v. Baylor Scott & White Health,* 17-CV-0886 (W.D. Tex.), Doc. No. 11, § 11.

[28]*Id. a*t § 25.

[29]*U.S. ex rel. Integra Med Analytics LLC v. Providence Health Services*, 2019 WL 3282619, at *5 (C.D. Cal. July 16, 2019).

[30]In the Integra Med action in the Western District of Texas, the court dismissed the complaint in full at the motion to dismiss phase finding a public disclosure bar. Integra Med has appealed. In the Central District of California action, the court was similarly dismissive and mostly dismissed the case. On a narrow ground, the court allowed Integra Med to proceed to discovery, but the defendants are currently pursuing an interlocutory appeal to the Ninth Circuit, and the action is currently stayed. *U.S. ex rel. Integra Med Analytics LLC v. Providence Health Services*, 17-CV-01694 (C.D. Cal.).

[31]*See* J.C. Herz, *Medicare Scammers Steal $60 Billion a Year. This Man Is Hunting Them,* https://www.wired.com/2016/03/john-mininno-medicare/.

[32]*Id.*

[33]*See* The United States' Mot. to Dismiss Relator's Second Am. Compl. at 1, *U.S. ex rel. Health Choice Grp., LLC v. Bayer Corp.,* No. 5:17-CV-126-RWS-CMC (E.D. Tex. Dec. 17, 2018), ECF No. 116; The United States' Mot. to Dismiss Relator's Second Am. Compl. at 1, *U.S. ex rel. Health Choice Alliance, LLC v. Eli Lilly & Co.,* No. 5:17-CV-123- RWS-CMC (E.D. Tex. Dec. 17, 2018), ECF No. 192; United States of America's Mot. to Dismiss Relators' First Am. Compl. at 1, *U.S. ex rel. Miller v. AbbVie, Inc.,* No. 3:16-CV- 2111-N (N.D. Tex. Dec. 17, 2018), ECF No. 52; United States' Mot. to Dismiss at 1, *U.S. ex rel. CIMZNHCA, LLC v. UCB, Inc.,* No. 3:17-CV-00765-SMY (S.D. Ill. Dec 17, 2018), ECF No. 63; United States' Mot. to Dismiss Relators' Compl. at 1, *U.S. ex rel. Carle v. Otsuka Holdings Co.,* No. 17-CV-00966 (N.D. Ill. Dec. 17, 2018), ECF No. 30; United States' Mot. to Dismiss Relators' Compl. at 1, *U.S. ex rel. SCEF, LLC v. AstraZeneca PLC,* No. 2:17-CV-01328-RSL (W.D. Wash. Dec. 17, 2018), ECF No. 15; United States' Mot. to Dismiss at 1, *U.S. ex rel. SMSF LLC v. Biogen Inc.,* No. 1:16-cv-11379-IT (D. Mass. Dec. 17, 2018), ECF No. 52; United States' Mot. to Dismiss at 1-2, *U.S. ex rel. SAPF LLC, v. Amgen Inc.,* No. 2:16-CV-05203-GJP (E.D. Pa. Dec. 17, 2018), ECF No. 18; United States' Mot. to Dismiss at 1-2, *U.S. ex rel. SMSPF LLC v. EMD Serono Inc.,* No. 2:16-cv-05594-TJS (E.D. Pa. Dec. 17, 2018), ECF No. 23; United States' Mot. to Dismiss Relator's First Am. Compl. at 1, *U.S. ex rel. NHCA-TEV LLC v. Teva Pharm. Prods. Ltd.,* No. 2:17-cv-02040-JD (E.D. Pa. Dec. 17, 2018), ECF No. 30.

[34]*See supra* note 33.

[35]In *U.S. ex rel. CIMZNHCA, LLC v. UCB, INC.,* No. 3:17-cv-00765-SMY-MAB, 2019 WL 1598109, at *4 (S.D. Ill. Apr. 15, 2019), the district court denied DOJ's motion to dismiss a finding that the government's stated purposes for moving to dismiss were arbitrary and capricious. This finding has been appealed to the Seventh Circuit Court of Appeals and remains pending.

[36]The Health Insurance Portability and Accountability Act of 1996 (HIPAA) P.L. No. 104-191, 110 Stat. 1938 (1996).

[37]45 C.F.R. Parts 160, 164.