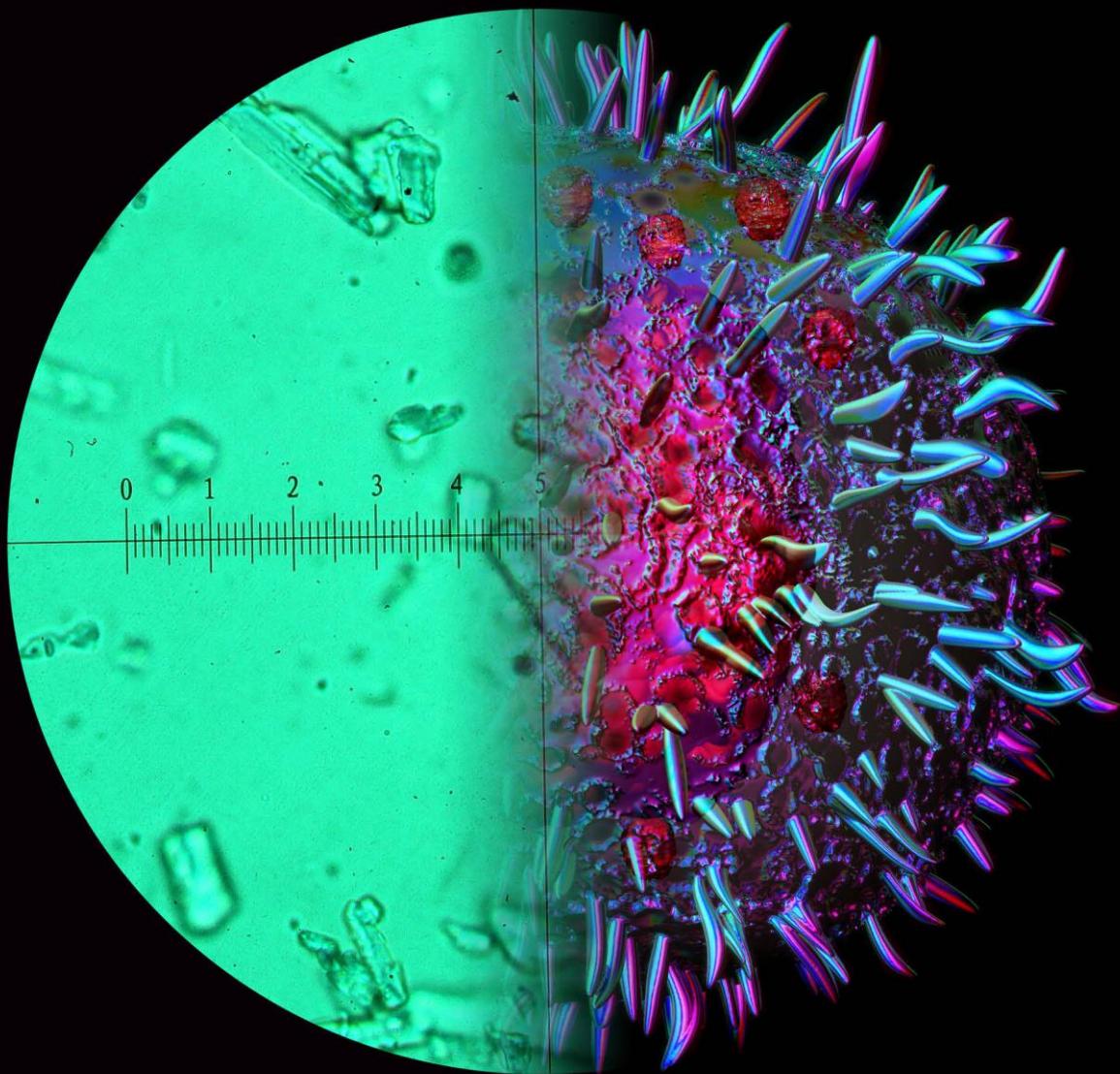


Deloitte.



Under the microscope
Making sense of today's health care
enforcement landscape

As the primary tool for fighting fraud against US government programs, the civil False Claims Act ("FCA") has been leveraged effectively by government organizations and "relators," or non-government whistleblower plaintiffs, since its passage in 1863. In the modern era of health care reform, FCA enforcement efforts have expanded significantly, opening up potentially new areas of liability and risk for health care and life sciences organizations and making it challenging for many of those organizations to keep up.

Addressing those FCA risks is a matter of connecting the what, why, and how of today's busy health care fraud and abuse enforcement landscape. In this point of view, we look at the types of cases being brought by the government and then turn our attention to risk mitigation through effective compliance programs. But first, let's review some of the events leading to the current state of enforcement.

Recent trends in enforcement activity

During the federal fiscal year 2017, settlements and judgments under the FCA led to the recovery of \$3.7 billion. Of that amount, more than half—\$2.4 billion—came from the health care industry. This amount reflects only recoveries by the federal government, and individual states have had additional recoveries under parallel state false claims act statutes for false Medicaid claims. Since strengthening the provisions of the FCA in 1986, Department of Justice ("DOJ") recoveries under the FCA total more than \$56 billion.¹

There is no sign of this activity slowing down anytime soon. One reason is heightened scrutiny of providers billing the Medicare fee-for-service program and organizations involved with Medicare Advantage plans. Another is a rise in the number of relators pursuing cases under the FCA. Coordination between civil and criminal divisions is also on the rise.

Data analytics plays a role as well. The Centers for Medicare and Medicaid Services ("CMS") reviews clinical data with increasing frequency and sophistication to reveal anomalies that point to potential improper payments.² And the Department of Health and Human Services' Office of Inspector General ("OIG") is expanding its use of data analytics to investigate allegations of fraud, waste, and abuse. Private plaintiffs and their law firms are also increasingly using data mining to identify potential claims.

Finally, it's worth noting that most FCA actions are filed under *qui tam* provisions of the FCA, under which a whistleblower receives up to 30 percent of the recovery. This creates an incentive for people to report violations of the FCA, and a growing number of *qui tam* suits are moving forward into litigation even when the government declines to formally intervene in the matter.

The upshot of these trends is that health care fraud remains a top priority of the federal government. "This government," said US Attorney General Jeff Sessions during his confirmation hearing, "must improve its ability to protect the United States Treasury from waste, fraud, and abuse."³

Current issues

With that, let's turn our attention to some current developments, beginning with the biggest health care fraud FCA ruling in recent years: the *Escobar* decision.

Implied certification. In 2016, the US Supreme Court affirmed the so called "implied certification" theory of FCA liability, under which a contractor's claim is legally false if it violates an underlying statute, regulation, or contract term material to payment—even if the claim form or submission itself is factually accurate. The Supreme Court's decision in *Universal Health Services v. US ex rel Escobar* addressed the question of whether

¹ Department of Justice Office of Public Affairs press release December 21, 2017.

² "Targeted Probe and Educate (TPE)," Centers for Medicare and Medicaid Services, August 14, 2017, <https://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Medical-Review/Targeted-Probe-and-EducateTPE.html>, accessed December 6, 2017.

³ Domenico Montanaro, "Watch Live: Jeff Sessions' Attorney General Confirmation Hearing," National Public Radio, January 10, 2017, <https://www.npr.org/2017/01/10/509039636/watch-live-jeff-sessions-attorney-general-confirmation-hearing>, accessed December 6, 2017.

the submission of a claim in and of itself implies that the underlying items or services were provided in compliance with applicable terms of payment.⁴

The answer, according to the court, is yes—sometimes. For implied certification to exist, the claim must make specific representations about the goods and services provided in addition to requesting payment. It also must fail to disclose noncompliance with a material statutory, regulatory, or contractual requirement to the extent that the non-disclosure ends up making the representations made misleading. Moreover, the claimant has to know that the underlying statutory or regulatory provision is material to the government's payment decision.

But for the government to deny payment under these circumstances, it has to satisfy a "demanding" test of materiality—it is has to prove that the agency would not have paid had it known the facts. It is no longer enough for the government to simply point to language in a statute or regulation that makes compliance a "condition of payment." For instance, if the agency has a history of paying similar claims—or paying a particular defendant—despite knowing about the violations, that would be strong evidence that the conditions were not material. Lower courts are beginning to apply these new standards—not always in consistent ways—making this an area that providers should continue to monitor carefully.

The 60-day Rule. Under the Affordable Care Act, health care providers that receive an overpayment of Medicare or Medicaid funds must report and return amounts to which they are not entitled within 60 days of identification.⁵ CMS elaborated on that provision for Medicare Parts A and B via a final rule it published in February of 2016. According to the rule, a claim under Medicare Parts A and B is an identified overpayment once the amount of the overpayment has been quantified.⁶ But should a provider fail to exercise "reasonable diligence" through and conduct an investigation in the face of "credible information" of a potential overpayment, the 60-day period will begin to run at the time that the provider learns of the potential overpayment, and the retention of an overpayment under such circumstances may constitute reckless disregard or deliberate ignorance, which could trigger liability under both the 60-day Rule and the FCA.

According to the 60-day Rule, when providers have a sufficient factual basis to conclude that they may have received overpayments, they should investigate to determine whether they have in fact received an overpayment. That investigation may also involve in certain circumstances taking probe samples of claims to look for errors. Should errors be found, providers need to determine the full scope of the error, which may require further sampling and extrapolation. What if the provider has good reason to conclude an overpayment has occurred, but fails to investigate it? In that case, the provider could be at risk that DOJ or a private whistleblower will seek substantial penalties under the "reverse false claims" provisions of the False Claims Act, as well as civil monetary penalties under the CMS 60-day Rule.

The Part C/D Overpayment Rule. CMS issued a separate rule governing overpayments under Medicare Parts C and D in 2014.⁷ UnitedHealthcare filed an action under the Administrative Procedure Act in January 2016 seeking to set aside the Part C/D Overpayment Rule on the grounds that it violates the requirement of "actuarial equivalence" under the Medicare Act and that it violates the meaning of the ACA Overpayment Statute by providing that a provider has "identified" an overpayment not only when it has "actual knowledge" of an overpayment, but when it "should have identified" the overpayment—in effect a negligence standard that is lower than the FCA's intent standard.⁸ Eventually, the courts will have to decide whether "identified" means actual knowledge, negligence or something closer to the FCA "reckless disregard" standard.

⁴ Universal Health Services, Inc. v. United States ex rel. Escobar, 136 S. Ct. 1989 (2016).

⁵ 42 USC. § 18001 et seq. (2010).

⁶ 42 C.F.R. § 401.301 et seq. (2016).

⁷ 42 C.F.R. § 417, 422, 423, et al. (2014)

⁸ *UnitedHealthcare Insurance Company et al v. Price et al*, Case No. 1:16-cv-157(D.D.C.).

Objective falsity. FCA suits based on challenges to medical necessity or quality of care have become common. They impact potentially any type of provider. Most affected in recent FCA actions are providers of long-term care, therapy, inpatient hospital, and home health services—not to mention physicians themselves.

Suppose two medical experts disagree about whether a procedure is medically necessary. Is that enough to show falsity under the FCA?

In two recent cases, the courts decided it isn't, concluding that there must be further evidence to establish an objective falsehood.⁹ Otherwise, providers "would be subject to potential FCA liability anytime the government could find a medical expert who disagreed with the certifying physician's clinical judgment."¹⁰ As for what qualifies as "further evidence," the courts pointed to false or fraudulent documentation or withholding important information about the patient's condition from the certifying physicians.

Use of statistical sampling. Statistical sampling involves collecting a subset of a population of interest, drawing a statistical inference from it, then extrapolating that inference across the larger population. It is a technique that has been used quite often by the government at times to quantify amounts of overpayments. More recently, there have been efforts to use statistical sampling to prove liability. The 60-day Rule specifically accepts sampling and extrapolation as a permissible way of identifying and quantifying overpayments.

Although sampling is an accepted approach for certain types of fraud cases, courts are likely to scrutinize its statistical validity, especially for liability purposes. Most often, the key issue driving the extrapolated results when employing sampling techniques is the error rate. Getting this right requires careful analysis of complex medical records and codes. Additional factors when employing sampling techniques include selecting a sampling methodology that holds up along multiple dimensions including size, randomness, and representativeness of the sample data.

But even the most meticulous sampling may fail to settle concerns about due process and reliability. The challenge is that human judgment doesn't always line up with a mathematical model. A prognosis of life expectancy for a hospice admission, for example, is inherently uncertain. The exact role of statistical sampling in liability scenarios is something courts have yet to determine and will be the subject of ongoing litigation.

Other recent developments

Medicare advantage. Recently, the government has begun to intervene in cases involving Medicare Advantage ("MA") plans—both against MA plans and against providers. Areas of interest include false risk adjustment data and false certifications of the accuracy of claims.

Meaningful use payments. In May 2017, DOJ announced a settlement agreement in a case against a vendor or electronic health record ("EHR") software alleging that the vendor causes its customers to submit false claims for meaningful use payments by filing false certifications of compliance with requirements the CMS EHR Incentive Program.

⁹ Samantha P. Kingsbury and Laurence Freedman, "Another Court Agrees That A Difference Of Opinion On Medical Necessity Is Insufficient to Show Falsity Under the False Claims Act," *Health Law & Policy Matters*, February 14, 2017, <https://www.healthlawpolicymatters.com/2017/02/14/another-court-agrees-that-a-difference-of-opinion-on-medical-necessity-is-insufficient-to-show-falsity-under-the-false-claims-act/>, accessed December 6, 2017.

¹⁰ Bill Myers, "Judge Strikes Down Government Effort To Split The Difference Between Experts," *Provider*, April 5, 2016, <http://www.providermagazine.com/news/Pages/2016/0416/Judge-Strikes-Down-Government-Effort-To-Split-The-Difference-Between-Experts.aspx?PF=1>, accessed December 6, 2017.

Individual accountability. Recently, the DOJ reiterated its commitment to use FCA and other civil remedies against individuals responsible for corporate wrongdoing.¹¹ The policy applies even where the individual does not have the ability to pay the judgment. The purpose of this policy is to prevent corporations from failing to stem health care fraud by approaching payments as a cost of doing business. Underscoring that commitment, the past few years have seen a number of notable multimillion-dollar settlements and judgments involving individuals in life sciences and health care companies.

Non-intervened cases. Government intervention remains key to health care *qui tam* fraud recoveries. But the government intervenes in only a minority of cases filed, and historically—when the government decided not to intervene—the relator generally chose not to pursue the case on his or her own. That is starting to change, however, with a noticeable trend in non-intervened cases moving into active litigation with the relator and relator's counsel.

Other developments. Other types of health care fraud—while not necessarily novel—continue to be enforced through the FCA. One area is drug pricing. Another one is kickbacks, where FCA cases continue to be filed involving such issues as below—and above—market rent, payments for sham services, sham speaker arrangements, and many different kinds of fee waivers. Cases involving Stark Law (physician self-referral) violations are also common. Further, the FCA's per-claim penalties have dramatically increased, roughly doubling between 2015 and 2017.¹²

Responding to government actions and *qui tam* cases

In light of all that's happening in the enforcement landscape, how should organizations respond to a government action or a non-intervened *qui tam* case today?

Planning. For counsel of health care and life sciences organizations confronted with allegations or evidence of potential false claims, the immediate priority is unchanged: Conduct an internal investigation. This includes interviewing witnesses (delivering Upjohn warnings to employees), and collecting and reviewing documents. Because FCA matters often require technical expertise, in-house counsel also may decide it's necessary to retain outside advisers, such as external counsel, consultants, or forensic accountants.

An effective investigation includes plans for all relevant fronts. One, of course, is government action. Another is the potential for other litigation. If a publicly-traded entity is involved, there may be shareholder lawsuits. If there are debt covenants, a settlement may have an impact on a covenant calculations. The investigating team must take bondholders and rating agencies into account. Relationships with customers, physicians, and payers all require consideration. Media and public relations teams will need a dedicated strategy of their own.

To carry out a financial analysis of the potential exposure, the investigation team must include people who thoroughly understand a variety of subject matters, including billing and coding, medical necessity, documentation standards, and fair value among others. They'll also need to understand the population to be inspected, along with the inspection periods, well enough to field tough questions from regulators. Another important qualification is the ability to compile a thorough and credible financial report.

Common mistakes. Investigators need to avoid a number of common errors. Underestimating the size of the allegation is an important one. So is a too-slow initial response, creating missed opportunities for taking appropriate action. Organizations sometimes give too little consideration to privilege and document preservation, the amount of time an investigation can take, and the effect it can have on morale.

¹¹ "Acting Assistant Attorney General Kenneth A. Blanco of the Criminal Division Speaks at the American Bar Association 27th Annual Institute on Health Care Fraud," US Department of Justice, May 18, 2017, <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-kenneth-blanco-criminal-division-speaks-american-bar>, accessed December 6, 2017.

¹² <https://www.gpo.gov/fdsys/pkg/FR-2016-06-30/pdf/2016-15528.pdf>

Another potential mistake is not engaging outside advisers early enough. Testifying experts, for instance, need time to formulate their opinions and calculate potential FCA damages and penalties. They also need to critique the opposing side's damages methodology, assumptions, and calculations, and prepare for rebuttal testimonies. Another key participant is the external auditor. While not part of the investigation itself, auditors require lead time to assess management's conclusions about the impact of any findings on an organization's system internal controls and the organization's financial statements.

Consultants can take on many roles from beginning to end. They can help collect and analyze data and run analyses and calculations related to damages. They also can work with counsel on case strategy, arguments, depositions, and interviews. It is critical to retain consultants who have the needed subject matter specialization and are accustomed to working in investigation and dispute contexts. To avoid losing important legal protections, organizations should see to it that consultants work under attorney-client privilege.

Prevention through compliance programs

Compliance programs must be designed and implemented to satisfy the government, in a tangible way, and demonstrate the organization is taking compliance seriously. Additionally, in a non-intervened *qui tam* suit, a company's program will often have to withstand the scrutiny of an expert witness who may be called to give an opinion about whether the company has an *effective* compliance program.

Analyzing the maturity of an organization's compliance program can help an organization set priorities as it enhances that program over time. There are three stages in the evolution of compliance programs:

Foundation



A foundational program focuses on basic compliance using the technology solutions the organization has already. The program includes an inventory of compliance policies plus basic training to maintain compliance with laws, rules, and regulations. Risk management is mostly reactive and focused on historical data, with some risk assessments plus compliance monitoring and testing.

Modernization



A modernized program is more extensive. Compliance policies are new and refreshed, with updated requirements (linked to laws, rules, and regulations) and internal controls. Metrics help with monitoring and reporting. Training and communications integrate into daily business activities and relationships. A refined compliance risk governance structure has the support of the board and senior management. This type of program shows that team members are knowledgeable about compliance. To regulators, it also provides transparency plus evidence of the program's adequacy.

Value creation



The value-creating program is the most sophisticated of all. It uses real-time data to analyze risk against key metrics, taking upcoming regulatory changes into account. Predictive analytics help with reporting, capacity and resource planning, and other decisions. The view of risk rolls up to the enterprise level. Overall, the program aims squarely at improving efficiency and outcomes.

An interesting aspect of value-creating programs is their emphasis on talent. They look for people with advanced data and analytics competencies. And the hiring techniques they use are specifically designed for compliance risk management.

A compliance risk framework

Compliance can be expensive. For that reason, management teams, boards, and audit committees are bound to ask about the value that the organization receives from its compliance program. Here's where a compliance framework makes sense. People need a basis for comparison, and this framework provides it by offering a standard set of elements, including:

	Governance involves board or compliance committee oversight of the compliance and ethics program, including sponsorship of a culture of integrity. Executive leadership is committed to, and supports the value of, ethics and compliance. Structures and processes support the compliance organization itself.
	Policies and procedures include formal policies, procedures, and related controls, all of which address business and risk appetite in mitigating compliance risk. Protocols drive the screening of new hires and employees in positions of authority.
	Risk assessment and regulatory change uses a defined strategy to regularly surface and respond to risks. It also includes an integrated regulatory change management program.
	Monitoring and testing take place on a well-defined schedule based on risk assessment results. Point-in-time testing assesses both program design and operating effectiveness. Ongoing monitoring programs keep track of business performance and risk indicators.
	Measurement and reporting uses technology to display dashboards of risk concentrations, breaches, and other indicators.
	Risk mediation uses protocols to surface issues. Employee reporting and case management systems capture, prioritize, and assign accountability.
	Regulatory interaction and coordination rely on protocols to communicate with regulators. Identified stakeholders interact with regulators, including during examinations and in communicating exam outcomes. They give an enterprise-wide view of examination activities.
	Communication, awareness, and training take place at both the enterprise level and within the lines of businesses. Business and/or regulatory changes are communicated in a timely way. "Speaking up" programs exist for employees to safely voice questions and concerns.

On top of these eight basic elements are four enabling ones:

			
People with the appropriate qualifications manage the compliance program against legal, policy, and ethical risks.	Processes facilitate the execution of the compliance program in an integrated and cost-effective way.	Technology helps to prevent, detect, and respond to compliance and ethics breaches. It also efficiently supports the compliance program.	Analytics create actionable insights that direct the future of the compliance program—strategically, operationally, and tactically.

Bringing it all together

Despite shifting reform policies and a change in administration, health care enforcement and compliance continue to receive strong support in Washington. Authorities and relators alike are pursuing new avenues to surface fraud and abuse.

For organizations in the health care and—increasingly—life sciences industries, the logical course is to stay aware of recent developments and evaluate their significance to the business. A structured program of ongoing compliance is an effective way to take this knowledge and put it to work at mitigating risk. At the same time, a strong compliance framework provides ways to keep management, investors, regulators, and other stakeholders informed and engaged.

Let's talk:

Steven Stanton

Managing Director
Forensic
Deloitte Financial Advisory Services LLP
sstanton@deloitte.com
+1 202 220 2120

Robert J. Cepielik

Partner
Forensic
Deloitte Financial Advisory Services LLP
+1 215 299 5212
rcepielik@deloitte.com

Katherine A. Lauer

Partner
Latham & Watkins LLP
+1 858 523 5451
katherine.lauer@lw.com

Daniel Meron

Partner
Latham & Watkins LLP
+1 202 637 2218
daniel.meron@lw.com

This article contains general information only and Deloitte and Latham & Watkins LLP are not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte and Latham & Watkins are shall not be responsible for any loss sustained by any person who relies on this presentation.

About Latham & Watkins LLP

Latham & Watkins LLP is a leading global law firm dedicated to working with clients to help them achieve their business goals and overcome legal challenges anywhere in the world. The firm has earned considerable market recognition based on a record of landmark matters and a unified culture of innovation and collaboration. From a global platform of offices covering the world's major financial, business and regulatory centers, the firm's lawyers help clients succeed. For more information, visit www.lw.com.

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.