wiley

ALERT

DOJ Health Care Fraud Takedown and FCA Working Group Signal New Era of Enforcement and Compliance Risks

July 8, 2025

On July 2, 2025, the U.S. Department of Justice (DOJ) and the Department of Health and Human Services (HHS) jointly announced the next phase of the Administration's "Whole-of-Government" approach to fighting health care fraud: the formation of the DOJ-HHS False Claims Act (FCA) Working Group. The announcement comes only days after DOJ touted the largest health care fraud enforcement action in its history, alleging more than $14 billion in fraudulent activity and charging 324 defendants. DOJ and HHS's strengthened partnership aims to enhance the government's response to health care fraud, refine enforcement priorities under the FCA, and foster collaboration between DOJ and HHS in identifying fraud and protecting federal health care programs. With health care fraud in DOJ's crosshairs and enforcement priorities set, companies should evaluate their Compliance programs to ensure they keep pace with the government's tactics.

DOJ-HHS Working Group

The FCA is a potent tool that DOJ uses to recover funds paid out due to fraud. The statute imposes civil liability on any person who knowingly presents a false claim for payment of government funds or makes a false statement that is material to a claim for payment of government funds. The FCA also enables private whistleblowers (or "relators") to file *qui tam* actions on behalf of the government and receive a share of any money recovered in the litigation.

Authors

Brandon J. Moss
Partner
202.719.7554
bmoss@wiley.law

Kathleen Cooperstein
Special Counsel
202.719.4043
kcooperstein@wiley.law

Corey J. Hauser
Associate
202.719.4436
chauser@wiley.law

Isaac J. Wyant
Associate
202.719.4705
iwyant@wiley.law

Practice Areas

Civil Fraud, False Claims, *Qui Tam* and Whistleblower Actions

Health Care

Health Care Risk Management and Regulatory Compliance

Oversight, Investigations & White Collar Enforcement

White Collar Defense & Government Investigations

While DOJ and HHS have a history of collaborating in FCA investigations, this new Working Group formalizes that partnership and expands the list of represented contingencies. The new Working Group includes the HHS Office of General Counsel, the Centers for Medicare & Medicaid Services (CMS) Center for Program Integrity, the Office of Counsel to the HHS Office of Inspector General (HHS-OIG), and DOJ's Civil Division, with representatives from U.S. Attorney's offices. The inclusion of CMS and HHS officials demonstrates the importance the Working Group is placing on soliciting feedback directly from HHS and CMS program operators.

The Working Group's announcement also outlined priority enforcement areas, including:

- *Medicare Advantage*. The Working Group will focus on fraud and abuse in Medicare Advantage plans, also known as Medicare Part C, which often involve allegations of upcoding, improper diagnosis submissions, and other fraudulent activity designed to recoup additional reimbursements. Given that Part C now accounts for over 50% of all reimbursement claims, it is unsurprising that the Working Group placed this enforcement target at the top of its list.
- *Drug, Device, and Biologics Pricing*. This includes improper arrangements involving discounts, rebates, service fees, formulary placement, and price reporting.
- *Barriers to Patient Access*. A newer priority, DOJ and HHS will be looking to bring enforcement actions targeting violations of network advocacy requirements and other practices that impede patient access to care.
- *Kickbacks*. The Working Group will target illegal kickbacks related to drugs, medical devices, durable medical equipment, and other federally reimbursed products.
- *Defective Medical Devices*. Continuing the prior Trump Administration's focus on patient harm, DOJ and HHS will aggressively pursue investigations and claims against manufacturers and sellers of materially defective medical devices that impact patient safety.
- *Electronic Health Record (EHR) Manipulation*. DOJ will investigate and prosecute manipulation of EHR systems that "drive inappropriate utilization of Medicare-covered products and services."

Notably, the Working Group plans to "maximize" collaboration between the agencies to efficiently drive new investigative leads by marshaling HHS and HHS-OIG reports and by using "enhanced data mining." In addition to triggering criminal health care fraud actions, like those in the recent record-setting Takedown, data analytics is rapidly becoming a leading source of original FCA actions. It was deployed quite successfully to target Paycheck Protection Program (PPP) fraud in the post-COVID era, and here, it appears that the government is poised to expand its utility to health care fraud. This collaboration is likely to lead to an increase in original actions by DOJ under the FCA.

Finally, continuing DOJ's recent emphasis on expediting investigations, the Working Group aims to "maximize cross-agency collaboration to expedite ongoing investigations in these priority areas and identify new leads, including by leveraging HHS resources through enhanced data mining and assessment of HHS and HHS-OIG report findings." The cross-functional group will also advise on whether HHS should suspend payments under

42 C.F.R. § 405.370 or whether DOJ should move to dismiss a relator's *qui tam* complaint under 31 U.S.C. § 3730(c)(2)(A). Despite DOJ rarely exercising its power to dismiss *qui tam* complaints, Deputy Assistant Attorney General Brenna E. Jenny told American Health Law Association attendees that the Working Group will assess "early whether novel legal theories are viable and supported by leadership." This sentiment could signal DOJ's willingness to dismiss meritless whistleblower complaints and ensure drawn-out FCA investigations don't harm operations.

Health Care Fraud Takedown

In addition to the DOJ-HHS announcement, and as predicted by panelists during Wiley's June 17 webinar, DOJ dropped its annual health care fraud takedown last week, moving on hundreds of targets simultaneously in a coordinated operation substantially larger than any of the previous years' enforcement actions. The Takedown showcases the usual variety of telehealth, kickback, and pharmacy shortage schemes to which industry players have grown accustomed over the last decade. Consistent with the Administration's stated priorities, DOJ enforcement appears to be shifting its weight towards schemes with some connection to international influences (like the four Pakistani defendants charged with $703 million of fraud using AI-generated patient consults to justify phony prescriptions) and novel technologies (such as the allegedly unnecessary amniotic skin grafts that generated a slew of indictments across Arizona and Nevada). But don't be fooled into thinking DOJ is content to run the same plays over and over. This Takedown also features many less traditional charges extending beyond simple billing fraud.

One defendant is the Chief Financial Officer of a software company that enabled patients, providers, and labs to connect seamlessly; however, DOJ alleges that it also created the infrastructure for telemedicine fraud by facilitating kickbacks and unnecessary insurance claims.

A hospital now faces civil liability for its doctors' alleged failure to "adequately" inform patients on the heart transplant list about their conditions. At the same time, a group of skilled nursing facilities reportedly agreed to pay over $6 million to resolve allegations that they omitted information about transactions with "related organizations" in their cost reports. In another instance, a lab owner, an office manager, and a compliance officer were charged criminally because (in addition to other allegations) they rewarded patients attending substance abuse treatment with gift cards for continued attendance. This list is just a small sampling of the myriad fact patterns falling under the ever-widening umbrella of "health care fraud."

The grand finale of last week's criminal Takedown, titled "Operation Gold Rush," meets the Administration's policy goals of shutting down transnational criminal organizations (TCOs) and prioritizing large-scale fraud against U.S. interests. The targets comprise a conglomerate of Russian-directed agents operating out of the United States, Estonia, and the Czech Republic, setting the stage for a high-stakes cross-border event. Twelve individuals have been arrested, including four extradited from Estonia, and seven apprehended at border crossings trying to flee the United States. All told, the intended loss tops $10.6 billion, making this the largest charged loss amount in health care fraud history. Encrypted messaging services, cryptocurrency exchanges, and layers of phony entities and bank accounts were all part of the scheme, according to DOJ.

Takeaways

At bottom, these two significant announcements signal increased attention to practical health care fraud enforcement in the new Administration. The Health Care Fraud Takedown highlights how recent reports of the Fraud Section's demise have been greatly exaggerated. As part of the "Whole of Government Approach," the Section continues to pursue health care fraud aggressively. Likewise, the DOJ-HHS Working Group aims to reprioritize and refocus civil health care fraud enforcement under the FCA. This formalized partnership could lead to an increase in original actions filed by DOJ, marking a return to the highs seen at the end of the first Trump Administration.

Those operating in the health care space should expect scrutiny of their Medicare Advantage billing, network adequacy, and patient access practices. They should also review their arrangements related to drug, device, and biologic pricing, to include discounts and rebates, and ensure that these arrangements do not expose them to civil or criminal liability.

This is also a good time for companies to review compliance policies and practices to ensure they are appropriately tailored to health care enforcement priorities. And remember, *priority* should not be read restrictively. The government will continue to pursue a broad range of health care fraud. While deterrence is always the ultimate objective of every compliance program, early detection is an increasingly close second as the Administration continues to emphasize and incentivize affirmative self-disclosure. On the criminal side, DOJ's updated Corporate Enforcement Policy provides a clear path to declination if misconduct is disclosed promptly and the company cooperates and effectively remediates. For civil matters, the Justice Manual includes "Guidelines for Taking Disclosure, Cooperation and Remediation into Account in False Claims Act Matters," which establishes a path for companies that disclose false claims, cooperate, and take remedial action to avoid damage multipliers.

Finally, with a specific call for more *qui tam* actions in the DOJ-HHS announcement, companies should continue to have appropriate mechanisms in place for employees and third parties to report perceived issues. Once raised, compliance teams should be prepared to respond quickly and investigate allegations. Given the government's renewed focus on data culling, compliance officers should also examine and potentially implement internal data analytics tools to detect potential fraud before a whistleblower comes forward.