

FEDERAL CIVIL ENFORCEMENT

Expert Analysis

## Health Care Companies Face New Opportunities But Old Legal Risks

BY WILLIAM HARRINGTON,  
ANNIE RAILTON  
AND COURTNEY ORAZIO

The federal False Claims Act (FCA) is likely already on the radar of health care companies doing business with the government: It is a powerful tool for the DOJ (or private whistleblowers standing in the DOJ's shoes) to seek recompense for false claims or false statements made in order to receive federal funds, authorizing treble damages and potentially sweeping penalties. It may not be top of mind during the current COVID-19 pandemic, but in fact the FCA has its origins in policing fraud in times of crisis. Consistent with that history, on March 20, 2020, Attorney General William Barr issued a press release underscoring the DOJ's focus on combatting COVID-19-related fraud, including fraudulent billing in violation of the FCA.

WILLIAM HARRINGTON and ANNIE RAILTON are partners at Goodwin in New York and COURTNEY ORAZIO is an associate in Boston.



William Harrington, Annie Railton, Courtney Orazio

As many companies potentially rush into the government contracting space to fill gaps in medical equipment and services, and even

As many companies potentially rush into the government contracting space to fill gaps in medical equipment and services, and even experienced contractors find themselves navigating uncharted (and evolving) waters concerning the provision of medical care, heightened risks under the FCA may follow.

experienced contractors find themselves navigating uncharted (and evolving) waters concerning the provision of medical care, heightened

risks under the FCA may follow. Below, we discuss some of those risks—in particular, those that may emerge due to a potential surge in telehealth services during this crisis—and steps that companies can take to mitigate potential FCA exposure as they provide critical goods and services in these uncertain times.

### The FCA's Application In Crises, Past and Present

Originally enacted in response to defense contractor fraud during the American Civil War, the FCA has long been used to police fraud in times of crisis.

As a recent example, in December 2018, the DOJ formed the Appalachian Regional Prescription Opioid

Force (ARPO) to combat the opioid epidemic. Just four months later, ARPO had already brought enforcement actions across 11 federal districts against at least 60 charged defendants for their alleged participation in illegally prescribing and distributing opioids. And two of the largest FCA recoveries in fiscal 2019 came from opioid manufacturers Insys Therapeutics and Reckitt Benckiser Group, which paid \$195 million and \$1.4 billion, respectively, to resolve criminal and civil claims against them.

Recent DOJ guidance underscores the heightened scrutiny and enforcement risk likely to result from the COVID-19 pandemic, and the unprecedented federal economic response to the crisis. On March 16, 2020, the National Whistleblower Center penned a letter to AG Barr, calling for the formation of a nationwide task force to investigate COVID-related fraud under the FCA. That same day, AG Barr issued a memorandum directing prosecutors to “prioritize the detection, investigation, and prosecution of all criminal conduct related to the current pandemic.” And on March 20, 2020, as noted above, AG Barr issued a press release reiterating the DOJ’s heightened focus on fighting COVID-related fraud, including against medical providers who fraudulently bill for tests and procedures in violation of the FCA.

### Potential Areas of FCA Risk In Light of COVID-19

With all that in mind, there are several areas of particular risk for companies involved in providing goods and services to aid in the response to

COVID-19. Among other things, companies must ensure compliance with rules and regulations concerning:

- Billing in the telehealth setting, or other scenarios when medical personnel do not actually see the patient;
- Licensing and credentialing requirements for providers;
- Privacy laws under the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and
- Pricing issues and representations by vendors concerning the efficacy of personal protective equipment (e.g., masks, gowns, gloves) and medical devices and equipment (e.g., ventilators).

---

Bearing in mind that the government will be scrutinizing telehealth services administered during and after the current crisis—especially those rendered by CARES fund recipients—companies should consider adopting strategies to mitigate potential FCA risk.

These risks may be especially acute for companies that receive funds through the Coronavirus Aid, Relief and Economic Security (CARES) Act, which was signed into law on March 27, 2020. Enforcement agencies will no doubt be paying close attention to how recipients use federal dollars they obtain—via contract, grant, or otherwise—as part of this \$2 trillion stimulus package. Given this, companies should take care to ensure that they accurately represent their qualifications for relief funds and that they comply with any regulatory requirements attached to those funds.



Shutterstock

### A Closer Look at FCA Risk In Connection With Telehealth

Of the areas identified above, telehealth in particular has garnered attention in light of widespread distancing efforts. President Trump even touted its utility in a recent briefing. The federal government has expanded coverage and reduced barriers to telehealth services in response to the COVID-19 pandemic—but with increased access (and perhaps also increased funding) may come increased risks. Companies should be cognizant of those risks, and how to mitigate them, especially as practitioners that traditionally rely on in-person visits (e.g., primary care physicians, therapists, dermatologists, and other specialists) enter the telehealth arena for the first time.

Historically, the U.S. Centers for Medicare and Medicaid Services (CMS) has restricted coverage of telehealth services—including limiting its applicability to patients in more remote locations, requiring that a provider be licensed in the state where the patient is located, and requiring that the provider and patient have an existing relationship at the time of service. But on March 13, 2020, in response to the COVID-19 pandemic, the U.S. Department of Health and Human Services (HHS) waived each of these requirements. As a result,

health care providers may now be reimbursed under Medicare for providing covered telehealth services to Medicare patients located in their homes, regardless of where the patient is located, regardless of where the provider is licensed, and regardless of what (if any) relationship exists between the provider and patient prior to the time of service. But by its terms, HHS's waiver applies "*only to the extent necessary*," as determined by CMS, to (1) "ensure that sufficient health care items and services are available to meet the needs of individuals enrolled in the Medicare, Medicaid, and CHIP programs," and (2) to reimburse providers who "*furnish such items and services in good faith*, but are unable to comply with one or more of these requirements as a result of ... the 2019 Novel Coronavirus ... pandemic" "*absent any determination of fraud or abuse*."

On March 17, 2020, the OIG also announced that—for the time period that the COVID-19 public health emergency is effect—health care providers will not face administrative sanctions for reducing or waiving any cost-sharing obligations that federal health care program beneficiaries may owe for telehealth services, such as copayments, coinsurance, and deductibles. Ordinarily, such routine reductions or waivers could implicate the Anti-Kickback Statute—a frequent source of alleged FCA violations. For free or reduced-cost telehealth services furnished during the COVID-19 public health emergency, however, OIG "will not view the provision of [those] services alone to be an inducement or as likely to influence future referrals." But nothing in the OIG's statement

otherwise relieves providers of their responsibility to only bill for services performed and to comply with applicable laws related to claims submission and cost reporting.

Finally, also on March 17, OIG's OCR division similarly announced that, in its "enforcement discretion," it will not impose penalties for noncompliance with HIPAA against covered health care providers in connection with the good faith provision of telehealth services during the COVID-19 public health emergency. As a result, providers may offer telehealth services via non-public-facing platforms such as FaceTime, Skype, and Facebook Messenger. Health care providers are nonetheless encouraged to inform patients that the use of such non-HIPAA compliant third-party applications may introduce privacy risks.

Despite expanded coverage and increased access to telehealth services in response to the COVID-19 pandemic, however, questions and risks remain. For example, where and when should providers apply waivers or reduce cost-sharing obligations in this rapidly-changing situation, and how can providers determine what services qualify as "necessary" to "meet the needs" of Medicare beneficiaries. While CMS has not limited "necessary" services to the treatment of COVID-19 itself, CMS's announcement does not identify what specific services will, in fact, be deemed "necessary." Companies must also still be cognizant of other applicable federal and state laws, including those related to establishing the requisite physician-patient relationship and obtaining informa-

tion sufficient to make a diagnosis or treatment recommendation in order to issue a prescription via telehealth.

Bearing in mind that the government will be scrutinizing telehealth services administered during and after the current crisis—especially those rendered by CARES fund recipients—companies should consider adopting strategies to mitigate potential FCA risk, which may include:

- Documenting the rationale for decisions concerning CARES relief funds, including government guidance or regulation(s) being relied on for a particular decision;
- Updating internal policies and procedures, especially if entering telehealth as a new business line, or deviating from preexisting practices due to COVID-19 circumstances;
- Keeping careful records that establish the medical necessity for all services rendered;
- Training (or re-training) the company's billing team on key FCA issues; and
- Closely monitoring waivers and reductions of cost-sharing obligations, and new patient relationships, to reduce the risk that steps taken post-pandemic could be viewed as potential kickbacks.

Finally, in addition to internal measures, companies should also be diligent in monitoring CMS and OIG guidance, and should promptly revise their policies and procedures as necessary to comply with that guidance in these uncertain and unprecedented times.