

What's Next For DOJ's COVID Enforcement In Health Care

By **Mahnu Davar, Suneeta Hazra and Howard Sklamberg** (September 14, 2022)

The onset of the COVID-19 pandemic and the Jan. 31, 2020, public health emergency declaration that followed pushed those of us working in the life sciences and health care industries into uncertain waters.

Drug sample delivery, pharmaceutical industry educational programs, routine and COVID-19 related patient care visits, rollout of timely diagnostic and surveillance testing and personal protective equipment, and ongoing data collection in open or new clinical trials are just a sample of the issues that had to be addressed.

Business and patient care exigencies soon outpaced the capacity of state and federal regulators to react — the regulators themselves facing staffing shortages, difficult and unprecedented questions, and technological challenges.

Centers for Medicare and Medicaid Services policy statements, U.S. Food and Drug Administration draft guidances and town hall pronouncements, governors' emergency declarations and waivers, and trade and professional society self-regulatory guidance were issued and updated frequently.

Often, these regulatory changes were announced in podium policy or communicated in technical advisory meetings or private correspondence prior to being announced in formal guidance documents. The result was a patchwork of temporary policy pronouncements that bypassed traditional notice and comment procedures.

In this fast-changing ad hoc environment, the vast majority of health care and life sciences companies sought to serve the public health and to comply with regulators and the shifting regulatory landscape as best they could.

The uncertainty and fear caused by the COVID-19 pandemic however, created an environment vulnerable to fraud and unamenable to routine oversight. Now regulators, investigators and prosecutors have been working hard — and, in some eyes, overzealously — to uncover and punish such conduct.

As we enter the end of the third year of the COVID-19 pandemic, a few fraud-related enforcement trends and risks have emerged. These trends and risks include:

- Limited prosecutorial leniency despite new and sometimes unclear COVID-19-related regulatory requirements and guidance;
- Creative enforcement strategies to implement COVID-19-related enforcement goals and priorities;



Mahnu Davar



Suneeta Hazra



Howard Sklamberg

- Continued and potentially increased enforcement of fraud surrounding products that are important in fighting COVID-19; and
- Increased scrutiny of telecare reimbursement claims.

Limited Prosecutorial Leniency Despite New and Sometimes Unclear COVID-19-Related Regulatory Requirements and Guidance

We have already seen evidence in ongoing criminal and civil actions that the government often does not view the lack of clarity from regulators and policymakers as a bar to relying on pre-pandemic enforcement norms.

Thus, we predict that the private sector may have limited success arguing to the government that it made decisions contravening pre-pandemic norms to meet clinical needs in a shifting regulatory environment during an unprecedented pandemic. The government, whether it be the U.S. Department of Justice, FDA, U.S. Department of Health and Human Services or state attorneys general, may well bring charges regardless.

Additionally, health care fraud statutes have long statutes of limitations. In particular, the Federal Food, Drug and Cosmetic Act, False Claims Act, Medicare Fraud Statute and related laws generally have statutes of limitations ranging from five to 10 years.

While the compliance bar often observes that enforcement trails conduct by three to five years, the pandemic could extend this trail.

For example, undetected overbilling when hospitals and other providers were short-staffed during the pandemic or continued billing for certain types telehealth services after the expiration of insurer policy changes could create latent liability that may not be discovered by billing or compliance personnel — or CMS or private insurance auditors, for that matter — until years later.

In short, the window of time for health care and life sciences companies to evaluate compliance issues is starting to close, as motivated prosecutors or disaffected employees start reviewing companies' activities and conduct with fraud enforcement in mind.

Creative Enforcement Strategies to Implement COVID-19-Related Enforcement Goals and Priorities

Prosecutors are going to get more creative. With government leadership prioritizing COVID-19 fraud, line civil and criminal assistant U.S. attorneys and agency chief counsel's offices are continually evaluating ways to build cases they believe can show results and make a splash, and are increasingly relying on sophisticated data analytic tools to do so.

State attorneys generals' offices will also likely become more creative in bringing fraud cases, particularly for issues they believe the federal government is not adequately addressing.

At the same time, because of the significant uncertainty felt by everyone during the pandemic, particularly in the pre-vaccine phase, the government faces litigation risks if seeks to bring cases against good faith actors.

For example, it seems difficult to imagine charging physicians who in good faith distributed unused vaccines outside of the prescribed queues to avoid wastage due to expiration, yet at least one such case was brought by a local district attorney and promptly dismissed by the judge.

Nevertheless, prosecutors are showing a willingness to apply a broader array of legal theories to implement the anti-fraud agenda. While there have no doubt been brazen instances of fraud — entities falsifying information to receive Paycheck Protection Act money, entities peddling unsafe or home-brewed therapeutics, etc. — the use of these tools, in the context of an emergency, can be overzealous.

In addition to the use of the typical health care fraud statutes including the False Claims Act, Anti-Kickback Statute and Stark Law, the government has used or may use other statutes, that are less often applied in the health care space, to prosecute alleged fraudulent activity related to COVID-19 products and services. These other statutes include (1) receipt of misbranded or adulterated medical devices or drugs, (2) Klein conspiracy, (3) the Travel Act, and (4) reverse FCA.

Receipt of Misbranded or Adulterated Medical Devices or Drugs

The FD&C Act presents a relatively low bar for committing a criminal violation, particularly for misdemeanors, which are punishable by up to one year in prison, and in some circumstances by fines of up to \$500,000.

For example, under the FD&C Act, a person may commit a misdemeanor if they receive an adulterated or misbranded medical device or drug, e.g., mislabeled, even unintentionally, and even without any knowledge the product is misbranded and without any intent to fraud or mislead, sends or offers to send the misbranded medical device or drug to another person.

Further, anyone who causes such activities to occur, even without knowledge or criminal intent, may also have committed a misdemeanor under the FD&C Act.

Although some judges have written that this strict liability application of the FD&C Act is unconstitutional or inapplicable in some settings,^[1] it remains a tool that the DOJ can wield or threaten to wield. The mere threat of its use can cause an individual or corporate defendant to accept a misdemeanor plea offer to avoid the expense of a trial or the risk of greater charges.

Of note, although the Public Readiness and Emergency Preparedness Act provides certain liability immunities against claims for damages relating to the manufacture, distribution, administration or use of drugs and medical devices used to combat COVID-19, the PREP Act does not provide immunity against federal enforcement actions brought by the federal government — whether civil, criminal or administrative.

Klein Conspiracy

It is a federal crime to conspire to commit any offense against, or to defraud, the U.S. government, including any U.S. government agency. This can include conspiring to interfere

with or impede a regulatory agency's ability to carry out its mission, and is often referred to as a Klein conspiracy after the tax evasion case *U.S. v. Klein* in the U.S. Court of Appeals for the Second Circuit in 1957.[2]

To establish a Klein conspiracy the prosecutor must prove that (1) the defendant entered into an agreement, (2) to obstruct a lawful function of the government, (3) by deceitful or dishonest means, and (4) committed at least one overt act in furtherance of the conspiracy.

The statute does not limit the method used to defraud, and the government does not need to suffer monetary loss. The prosecution only need demonstrate the conspirators intended to harm the federal government.

Moreover, it is often true that the recommended sentence, under the U.S. sentencing guidelines, for Klein conspiracies can be Draconian and sweep in a broad array of conduct and actors.

Thus, prosecutors often rely on it when a defendant's actions do not fit a typical false claims case, for example where the conduct did not easily result in the submission of a false claim or in monetary losses to the U.S. government.

Travel Act

The Travel Act criminalizes traveling, or using the mail or a facility — which includes the use of a cellphone, mail or email — in interstate or foreign commerce, for the purpose of furthering an unlawful activity, which includes certain offenses that would otherwise be state law violations.

The government must show that the defendant intended to facilitate the unlawful activity and performed or attempted to perform an act to facilitate it. The Travel Act is an attractive tool for prosecutors due to the ease in establishing federal jurisdiction.

Although originally enacted to combat organized crime, in recent years prosecutors have used it in federal health care fraud prosecutions. In April 2019, for example, seven health care providers in Texas were convicted under the Travel Act for paying \$40 million in bribes and kickbacks to medical providers in a fraudulent patient referral program.

Reverse False Claims

The reverse false claim provision of the FCA aims to penalize those who prevent the government from collecting what is owed to it.

A violation of the reverse false claims act provision occurs when a person knowingly makes, uses or causes to be used a false claim material to a monetary obligation to the government, and then knowingly conceals or improperly avoids or decreases an obligation to pay the government.

In the Medicaid and Medicare context, the government may use the reverse false claim provision to pursue health care providers who identify, or should have identified through reasonable diligence, a Medicaid or Medicare overpayment and, with either intentional or reckless disregard, fail to repay it within the allotted 60 days.

Continued and Potentially Increased Enforcement Focus on Fraud Related to Products That are Important to the Fight Against COVID-19

We expect the government will continue to investigate and bring charges against actors who the government determines may be or are marketing or selling COVID-19-related medical products through fraudulent means, regardless of whether the product falls under an FDA enforcement discretion policy or emergency use authorization, or EUA. This scrutiny will likely increase if the conduct or product poses a high public health risk.

At the pandemic's start, the FDA moved fairly quickly to establish enforcement discretion policies and EUAs to permit the distribution and import of medical products that could be used to combat COVID-19 but did not meet applicable FDA requirements. Although the FDA has ended some of these policies and EUAs, most are still in force, albeit in amended form.

In tandem, the FDA has pursued administrative compliance and enforcement actions against products and actors that the FDA asserts did not fully comply with its enforcement discretion policies and EUAs, while the DOJ has charged cases of fraud and apparent fraud for the same conduct.

For example, beginning in early 2020, the DOJ has brought civil and criminal cases against manufacturers, distributors and importers who fraudulently represented respirators as being N95s approved by the National Institute for Occupational Safety and Health.

DOJ enforcement related to the sale and distribution of fraudulent N95 respirators and other important COVID-19 related products, e.g., COVID-19 tests, will likely be an area of continued scrutiny.

Additionally, the DOJ's ongoing focus on clinical trial fraud and data integrity is likely to expand to include individuals and entities operating under the FDA's COVID-19 enforcement discretion policies for clinical trials, which relaxed certain record-keeping standards, recognized the use of telehealth technologies to replace in-person investigator-subject visits, and allowed for a more streamlined approach to deviation documentation and reporting by sponsors.

Eventually, the FDA will rescind its COVID-19 enforcement policies and EUAs. Products no longer covered by an enforcement discretion policy or EUA would in most cases be misbranded or adulterated under the FD&C Act if they did not comply with standard applicable FDA requirements.

If the FDA's administrative remedies are not sufficient to prevent the manufacture and distribution of noncompliant FDA-regulated products at such time, we would not be surprised to see an uptick in civil and criminal cases.

Increased Scrutiny of Telecare Reimbursement Claims

The pressure on providers to make up for profit losses from closed clinics, patient reluctance to go to the doctor's office in-person and staffing shortages during the early days of the pandemic have had the potential to put undue pressure on billing compliance programs.

Further, early and successful adoption of waiver-based approaches during the pandemic created a market expectation and demand for telemedicine services and for insurance reimbursement of such services.

Many new medical practices and entities providing telehealth-based services, such as those

involved in supervising at-home COVID-19 testing for clinical care or as part of data collection in COVID-19 therapeutics clinical trials, have flourished.

Many of these practices and entities, however, can exist only in large part thanks to temporary COVID-19 policies that have allowed new diagnostic testing technologies to be shipped to patient homes, purchased in pharmacies and supervised through remote monitoring technologies.

Reimbursement for these visits must also be made in accordance with certain pandemic-era policy clarifications and waivers from CMS, state public health regulators and private insurance plans.

What are the enforcement consequences for these practices and entities when state and federal public health emergency declarations and associated policies end?

With billions of dollars of fraud in the Medicare and Medicaid system prior to the pandemic, and estimates of potentially tens of billions of dollars in fraud related to PPP loans and other COVID-19 related financial incentive programs, it is a virtual certainty that state and federal regulators and auditors will scrutinize reimbursement claims sent by medical systems, diagnostics laboratories and other organizations set-up to perform telecare services.

Already, in July, the HHS Office of Inspector General announced it had been conducting dozens of investigations of fraud schemes involving companies that purported to provide telemedicine services.[3]

In the announcement, the HHS OIG includes a list of suspect characteristics of telemedicine arrangements that, together or separately, could suggest fraud or abuse.

These suspect characteristics are, in short:

- The telemedicine company identifies or recruits purported patients by advertising free or low out-of-pocket cost items or services.
- The physician does not have sufficient contact with or information about the patient to meaningfully assess medical necessity.
- The practitioner receives volume-based compensation.
- The telemedicine company furnishes products or services only to patients who are federal health care beneficiaries.
- The telemedicine company falsely or incorrectly claims to not furnish any products or services to federal health care beneficiaries.

- The telemedicine company furnishes only one product or class of product, which, the HHS OIG noted, could limit the practitioner's treatment options.
- The telemedicine company does not expect physicians to follow-up with the patient.[4]

While these factors are not exhaustive, they can be used as a road map for companies now working to identify current or past potential compliance gaps that were created by exigent circumstances and the use of new telemedicine technologies.

For example, many providers relied on third-party turn key telemedicine technology consultants and providers to manage the technological and administrative details of telehealth. The OIG and DOJ are likely interested in the extent to which providers have exercised appropriate oversight over care quality and billing accuracy and compliance.

Steps Health Care and Life Sciences Companies Should Take Right Now

Provider and clinical laboratory risk assessment plans for 2022 should include a sophisticated review of compliance with CMS and state telehealth and billing related waivers, including a look at technical billing software issues such as auto billing, resolution of current procedural terminology coding blanks and use of miscellaneous codes, and identification of referring provider national provider identifiers.

Additional scrutiny and review of such information is particularly warranted in states where telehealth was highly restricted prior to the pandemic. As noted, the OIG's indicia of potential fraud and abuse should also be considered in any provider compliance review of telehealth billing and implementation.

Life science product companies should similarly review and confirm their compliance with applicable FDA policies and EUAs during the pandemic, including applicable policies and EUAs relating to sale, distribution and use of their products, including those relating to the diagnosis, cure, mitigation, treatment or prevention of COVID-19, including laboratory testing services, and to distribution of drug samples.[5]

Clinical trial sponsors and related entities such as clinical research organizations would also be wise to confirm that their clinical trial activities during the pandemic complied with all FDA requirements and guidance, including the FDA's enforcement discretion policies for clinical trials during COVID-19.

All entities in the health care and life sciences space should closely scrutinize any indications of potential fraud or other criminal violations.

Additionally, many laws and regulations affecting the health care and life sciences industries did not change during the pandemic, and so health care and life sciences companies should also take care to confirm they continued to comply with those requirements despite the exigencies of the COVID-19 pandemic.

The pandemic has been a time of immense change and uncertainty, and the health care and life sciences industries, as well as its regulators, should be commended for the overall composure with which they have addressed and are addressing its exigencies.

Moreover, certain industry and regulator practices that began during the pandemic will, for the better, likely continue into the foreseeable future. However, as the dust begins to settle, the government will continue to aggressively scrutinize COVID-19-related practices for noncompliance and potential fraud.

All things considered, there is no better time than the present for health care and life science companies to confirm their compliance with applicable rules and policies in place throughout the pandemic.

Mahnu Davar, Suneeta Hazra and Howard Sklamberg are partners at Arnold & Porter.

Arnold & Porter associate Elizabeth Carney and senior associate Tyler Scandalios contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See, e.g., *U.S. v. DeCoster*, 828 F.3d 626 (8th Cir. 2016) (Beam, J., dissenting).

[2] *United States v. Klein*, 247 F.2d 908 (2d Cir. 1957).

[3] Additionally, on September 7, 2022, HHS OIG issued a report, titled "Medicare Telehealth Services During the First Year of the Pandemic: Program Integrity Risks," assessing the program integrity risks associated with Medicare telehealth services and identifying ways to safeguard Medicare from fraud, waste, and abuse related to telehealth. In conducting a study underlying the report, HHS OIG determined that the billing of 1,714 providers for telehealth services during the first year of the pandemic poses a high risk to Medicare (although HHS OIG stopped short of stating that any particular provider was engaging in fraudulent or abusive practices). The full report is available through <https://oig.hhs.gov/oei/reports/OEI-02-20-00720.asp>.

[4] The full HHS OIG Special Fraud Alert is available at <https://oig.hhs.gov/documents/root/1045/sfa-telefraud.pdf>.

[5] Although not discussed in-depth in this article, FDA issued a temporary COVID-19 policy loosening certain FDA requirements governing distribution of drug samples. Accordingly, health care practitioners, pharmaceutical manufacturers and distributors, pharmacies, and other entities working with drug samples should reconcile internal recordkeeping approaches with pre-pandemic state and federal laws requiring sample traceability, inventory management, and audits. Reporting times for significant theft, loss, recordkeeping falsification, and other issues related to drugs samples have not changed under federal or state law.