COMMENTARY

Fraud, Access, and the Future of Telemedicine

Jacob T. Elberg, JD, and Eli Y. Adashi, MD, MS

On July 20, 2022, the Department of Health and Human Services, Office of Inspector General (HHS-OIG), issued a Special Fraud Alert warning healthcare providers of increased fraudulent activity surrounding telemedicine companies. The Alert marks a further escalation of a multi-year effort by the Department of Justice (DOJ) and the HHS-OIG to crack down on multi-billion dollar fraud cases involving telehealth companies. It is the objective of this Commentary to place the HHS-OIG Special Fraud Alert in the context of enforcement efforts by the DOJ and HHS to stem the recent growth in telehealth fraud resulting from the COVID-19 pandemic. Taken together, it is apparent this is a critical moment in the evolution of telehealth and it is crucial to strike a proper balance between effective regulation and enforcement on the one hand, and access to care on the other. (J Am Board Fam Med 2023;00:000–000.)

Keywords: **COVID-19, Fraud, Health Services Accessibility, Pandemics, Telemedicine, United States Department of Health and Human Services**

On July 20, 2022, the Department of Health and Human Services, Office of Inspector General (HHS-OIG), issued a Special Fraud Alert warning health care providers of increased fraudulent activity surrounding telemedicine companies.[1] The Alert marks a further escalation of a multi-year effort by the Department of Justice (DOJ) and the HHS-OIG to crack down on multi-billion-dollar fraud cases involving telehealth companies. It is the objective of this Commentary to place the HHS-OIG Special Fraud Alert in the context of enforcement efforts by the DOJ and HHS to stem the recent growth in telehealth fraud resulting from the COVID-19 pandemic. Taken together, it is apparent this is a critical moment in the evolution of telehealth and it is crucial to strike a proper balance between effective regulation and enforcement on the 1 hand, and access to care on the other.

The HHS-OIG Alert is the first to be focused specifically on educating health care providers on the possibility that they may be recruited, perhaps unknowingly, to engage in unlawful arrangements. Though acknowledging that schemes have taken a variety of forms and involved a wide range of fraudulent billing, including for unnecessary medications, durable medical equipment, and genetic testing, the HHS-OIG warns that Telemedicine Companies have been enlisting health care providers to prescribe items and services that are medically unnecessary, potentially violating the Anti-Kickback Statute in addition to other statutes. As such, these relationships expose health care providers to potential criminal, civil, or administrative liability, including OIG exclusion. The Alert seeks to educate health care providers regarding "suspect characteristics" and urges them to "exercise caution and use heightened scrutiny when entering into arrangements with Telemedicine Companies that have 1 or more of the suspect characteristics." These characteristics include the practitioner not having sufficient contact with or information from the patient to meaningfully assess medical necessity, the Telemedicine Company only furnishing items and services to Federal health care program beneficiaries and not accepting other insurance, or the Telemedicine Company only furnishing 1 product

This article was externally peer reviewed.
Submitted 8 February 2023; revised 18 May 2023; accepted 25 May 2023.
This is the Ahead of Print version of the article.
From the Associate Professor of Law and Director of the Center for Health & Pharmaceutical Law, Seton Hall University School of Law, Seton Hall University, Newark, NJ (JTE); Professor of Medical Science, Former Dean of Medicine and Biological Sciences, Brown University, Providence, RI (EYA).
Funding: None.
Conflict of interest: None.
Corresponding author: Jacob T. Elberg, JD, Associate Professor of Law and Director of the Center for Health & Pharmaceutical Law, Seton Hall University School of Law, Seton Hall University, One Newark Center, Newark, NJ 07102 (E-mail: jacob.elberg@shu.edu).

or a single class of products, thus restricting the practitioner's treating options.[1]

HHS-OIG issued the Alert the same day that the DOJ announced charges against 36 defendants across the country for alleged involvement in more than $1.2 billion in fraudulent billing, much of it committed through telemedicine.[2] These charges followed announcements by the DOJ in 2019, 2020, and 2021 of billions of dollars in fraudulent claims arising out of telehealth. Telemedicine has arguably become the most significant focus of the DOJ and HHS's enforcement efforts over the past 3 years.

Notably, on the same day that the HHS-OIG issued the Alert, the DOJ announced charges involving the $1.2 billion in fraud and the Centers for Medicare & Medicaid Services (CMS) and the Center for Program Integrity announced that it took administrative actions against 52 health care providers involved in similar schemes. Administrative actions require a lower threshold in terms of knowledge that the conduct is unlawful, and are consistent with the message of the OIG Alert that the government is concerned that health care providers who do not set out to engage in wrongdoing are being unknowingly pulled into fraudulent schemes involving telehealth.

Although the DOJ and HHS noted increased levels of fraud involving telemedicine before the COVID-19 pandemic, loosened telehealth regulations in response to the pandemic have afforded telemedicine companies with increased opportunities for fraudulent conduct. A 2021 McKinsey & Company analysis projected that as much as $250 billion may be spent annually on telehealth in the future.[3] A year later, telehealth utilization had stabilized at a level 38 times higher than before the pandemic.[3] As health care delivery has continued to shift toward telehealth, CMS allowed telehealth coverage for a number of Current Procedural Terminology (CPT) codes permanent in the 2021 physician fee schedule final rule, while leaving open the question of how restrictive telehealth regulations will be as the COVID-19 pandemic eases.[4] The continued flood of publicity surrounding telemedicine fraud and the billions of dollars lost threatens to curtail what would otherwise likely be a continued expansion of telehealth flexibility to the benefit of both patients and health care providers.

This is an area where data analytics provide a substantial opportunity for government regulators to identify potential misconduct in the early stages and address it before financial losses are out of hand. It is striking that millions of dollars in fraud have been committed involving telehealth prescriptions by individual physicians before a government regulator has intervened. Viewed in this light, the HHS-OIG efforts at educating health care providers are praiseworthy, but unlikely to reach a large number of health care providers. These efforts should be paired with a system capable of immediately identifying individual physicians engaged in telehealth and ensuring that they are aware of the concerns expressed in the OIG Alert. HHS and DOJ have dramatically improved their data analysis capabilities over the past decade, and should put them to use here to prevent, in addition to prosecute fraud involving telehealth.[5] It is an area particularly ripe for data analytics through which regulators can quickly identify unusual telemedicine prescribing—data analytics can quickly and automatically identify prescriptions written by providers who lack a preexisting relationship with the patients; health care providers having numerous prescriptions filled, lab tests run, or DME provided by entities with which they have no preexisting relationship; patients using entities without a preexisting relationship or geographic connection, to name just a few potential warning signs. Of course, these warning signs are not automatically indicia of fraud—for example, patients may be geographically disconnected for legitimate reasons or may be having a legitimate initial encounter with a new provider—but can quickly and inexpensively identify for investigators billing in need of additional review. While data analytics is not a panacea when it comes to telemedicine fraud and may be less able to identify other issues of fraud and abuse in telemedicine, such as billing for services not performed or inadequately performed, it has potential to help combat many of the most significant issues raised by telemedicine.

Regulators should also consider going a step further. While telehealth offers a critical opportunity for care and it is appropriate that the government avoid requiring prior approval before patients use telehealth services, it would not meaningfully interfere with patient care to require physicians to certify that they have read and understood telehealth regulations and the associated risks before they begin engaging in the practice. Such education—which need be no more onerous than certifying that they have read the Alert—would benefit both providers and government finances, saving health care providers from unknowingly becoming involved in what may be a career-ending relationship, and the

government from losing additional money to fraud. Where health care providers fail to heed warnings, the education will provide crucial evidence enabling the DOJ to prove that the health care providers were not unwitting participants but knowing coconspirators. Telehealth offers tremendous opportunities for improving the practice of medicine and the provision of care for health care providers and patients alike. Unfortunately, as currently regulated, telemedicine also provides substantial opportunities for criminals who seek to capitalize on the vast amount of money in health care and the system's laudable preference for access to treatment over safeguards. With proper systems in place, fraud prevention need not come in the form of restricted telehealth access. The future of telehealth stands at a crossroads—the treatment gains from the practice are continually being threatened by press releases announcing billion dollar losses. Now is the time to take action so that telehealth can be seen as an opportunity and not as a vulnerability in the evolving practice of medicine.

To see this article online, please go to: http://jabfm.org/content/00/00/000.full.

References

1. Department of Health and Human Services, Office of Inspector General. Special Fraud Alert: OIG alerts practitioners to exercise caution when entering into arrangements with purported telemedicine companies. Accessed July 20, 2022. Available at: https://oig.hhs.gov/documents/root/1045/sfa-telefraud.pdf.
2. United States Department of Justice. Justice department charges dozens for $1.2 billion in health care fraud. Accessed July 20, 2022. Available at: https://www.justice.gov/opa/pr/justice-department-charges-dozens-12-billion-health-care-fraud.
3. McKinsey & Company. A quarter-trillion-dollar post-COVID-19 reality? July 9, 2021. Available at: https://www.mckinsey.com/industries/healthcare/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality.
4. Centers for Medicare & Medicaid Services. CY 2021 Medicare physician fee schedule final rule. January 1, 2021, 85 Fed. Reg. 84472, federalregister.gov.
5. United States Department of Justice and Department of Health and Human Services. Health care fraud and abuse control program FY 2021. Available at: https://oig.hhs.gov/publications/docs/hcfac/FY2021-hcfac.pdf.