New Jersey Law Journal
STATEWIDE LEGAL AUTHORITY SINCE 1878
An ALM Publication
NOVEMBER 4, 2020 NJLJ.COM

DOJ and HHS-OIG's 2020 Health Care Fraud Takedown: Focus on 'Telefraud'

This year alone, many providers and patients transitioned to using telehealth platforms out of necessity. as with all areas of health care, expansion means increased risk for enforcement.

By Melissa L. Jampol, Amy Lerman and Elena M. Quattrone

Credit: H_Ko / Shutterstock.com

Utilizing telehealth platforms to deliver health-care services is an area of recent, rapid expansion. Since the worldwide spread of COVID-19, safe access to health-care services has been limited, and demand for telehealth services has surged. Alexander GC, *et al.*, *Use and Content of Primary Care Office-Based vs Telemedicine Care Visits During the COVID-19 Pandemic in the US*, JAMA Net Open (Oct. 2020) (number of telemedicine consultations increased thirty-fold to more than 35 million in 2020's second quarter). According to Epstein Becker Green's 2020 Telemental Health Laws **survey**, this year alone, many providers and patients transitioned to using telehealth platforms out of necessity. Regulators implemented measures to increase access to health care through telehealth, including waivers and other regulatory modifications related to professional licensure and use of telehealth technology, and in some cases amendments to existing and/or enacted new regulations focused on telehealth utilization.

Yet, as with all areas of health care, expansion means increased risk for enforcement. At the end of September, the U.S. Department of Justice (DOJ) and the U.S. Department of Health and Human Services (HHS) Office of Inspector General (OIG) demonstrated this point, announcing that in its 2020 "Takedown," 345 defendants across 51 judicial districts have been charged with allegedly submitting more than $6 billion in false and fraudulent claims to federal health-care programs and to private payors—$4.5 billion of which related to telehealth. **Press Release**, DOJ, "National Health Care Fraud and Opioid Takedown Results in Charges Against 345 Defendants Responsible for More than $6 Billion in Alleged Fraud Losses," (Sept. 30, 2020). While these enforcement actions actually occurred over numerous months preceding the press event (thus, the reference to a "takedown" is a misnomer), DOJ / HHS had not previously focused so sharply on enforcement activity involving telehealth providers. The 2020 Takedown warns the telehealth industry to pay attention to compliance infrastructures and efforts.

Indeed, Acting Assistant Attorney General Brian C. Rabbitt sent a warning by noting that the 2020

Takedown sent "a clear deterrent message and should leave no doubt about the department's ongoing commitment to ensuring the safety of patients and the integrity of health-care benefit programs, even amid a national health emergency."

The 2020 Takedown, which also targeted opioid distribution schemes, and fraud connected to substance abuse facilities, involved "telefraud" schemes that allegedly leveraged aggressive marketing and telehealth services. Alleged conspirators included telehealth company executives, owners of durable medicine equipment (DME) companies, genetic testing laboratories, pharmacies, medical practitioners, marketers, and business owners who OIG claims "scammed hundreds of thousands of unsuspecting patients in their homes." **Press Release**, OIG, "2020 National Healthcare Fraud Takedown," (Oct. 1, 2020). HHS-OIG Deputy Inspector General Gary Cantrell commented on the opportunities for fraud in the telehealth setting and how enforcement in this area remains a high priority, stating:

Unfortunately, bad actors attempt to abuse telemedicine services and leverage aggressive marketing techniques to mislead beneficiaries about their health care needs and bill the government for illegitimate services …. We will continue working with our law enforcement partners to hold accountable those who steal from federal health programs.

The schemes included in the 2020 Takedown are many, and the alleged perpetrators are diverse; however, the themes are familiar: companies utilizing allegedly aggressive marketing techniques to engage with consumers, and using purported kickbacks to encourage the ordering of medically unnecessary services by providers; specifically DME and genetic and other diagnostic testing, in some cases, where telehealth company executives allegedly paid providers to prescribe such services with brief or no interaction with patients.

Among the cases included in the **2020 Takedown** are:

• *Middle District of Florida* – 29 defendants charged in schemes to defraud insurance programs, totaling $584 million. In one case, the CEO of two telehealth companies pled guilty to soliciting kickbacks and bribes from DME suppliers in exchange for encouraging telehealth providers to order unnecessary DME. DOJ alleges that in some cases, the providers never spoke to the patients for whom they prescribed DME.

• *Southern District of Georgia and District of South Carolina* – In "Operation Rubber Stamp," a collaboration between the Southern District of Georgia and the District of South Carolina, more than $1.5 billion in allegedly fraudulent billings to government health-care programs were identified, and charges filed against multiple defendants. In Georgia, the cases involved telehealth company executives who allegedly paid providers to order unnecessary DME, pain medications, and genetic and other diagnostic testing, often with either no or little patient interaction, which were purchased by health-care entities, and submitted to Medicare for reimbursement. Similarly, in South Carolina, providers were charged with conspiracies involving more than $100 million dollars in false and fraudulent billings, allegedly for signing prescriptions over a web-based platform, often without meeting or speaking to patients. Charges were also filed against individuals and a corporation that allegedly used offshore call centers and telehealth to bill hundreds of millions of dollars of medically unnecessary DME to government payors.

• *Northern District of Illinois* – Seven defendants were charged with allegedly defrauding insurance programs out of $205 million. In one case, a physician, licensed in 17 states, worked for more than 10 telehealth companies, and allegedly paid his friends to sign telehealth orders in his name for medically unnecessary genetic testing and DME. The scheme allegedly resulted in $145 million in false claims billed to Medicare, and approximately $54.6 million paid by Medicaid.

• *Eastern District of Pennsylvania* – Six defendants were charged for their alleged roles in schemes to defraud insurance programs out of $27 million. In one case, a telehealth company owner pled guilty to soliciting illegal kickbacks and bribes in exchange for medically unnecessary orders for DME and cancer genetic testing.

Prior to the 2020 Takedown, telehealth enforcement was unique due to the nuances of health-care delivery through this modality. For instance, implementing regulations that align with technological advancements in telehealth has been challenging for many jurisdictions. Additionally, each U.S. jurisdiction features different rules for health-care delivery that are required for reimbursement, such as establishing the provider-patient relationship, the types of services

available for coverage (e.g., behavioral health services, primary care), and the types of modalities that may be used, which all impact acceptable delivery of care, and federal and state enforcement risk.

With telehealth now a DOJ and HHS-OIG enforcement priority, stakeholders must carefully navigate the complex regulatory regime that governs the delivery of telehealth services.

Key factors to consider when operating in this space to limit enforcement risk include:

• *Defining appropriate scopes of services offered via telehealth.* Consider what services can reasonably be offered via telehealth to best serve the patient. Similarly, consider staffing needs and whether there are licensure or scope of practice considerations that must be addressed before providers deliver services using the telehealth platform.

• *Understanding and ensuring compliance with state law requirements governing the virtual environment.* Each jurisdiction has its own separate and distinct laws and guidance regarding the delivery of care via virtual platform. Be cognizant of these laws and guidance, especially with regard to establishing provider-patient relationships, remote prescribing, and claims submission and reimbursement.

• *Creating the appropriate structure for the telehealth model.* Each jurisdiction also has its own rules regarding prohibitions on the corporate practice of medicine (or other health-care professions), under which licensed professionals may only be employed by professional entities. Decisions about who is providing the telehealth services may require the creation of professional corporations in various states so as to lawfully deliver these services.

• *Being mindful of claims submission and reimbursement considerations.* In response to COVID-19, both government and private payers have allocated more resources for telehealth, but providers may have to meet certain requirements specific to that payer related to documentation, coding, or even the electronic platform used in order to qualify.

• *Following changes in the loosened professional licensure requirements in response to COVID-19.* Since a national public health emergency was declared in March 2020, federal and state authorities loosened regulatory requirements with respect to telehealth, especially relating to professional licensure. Although handled differently by individual states, there have been significant modifications and, in some cases, waivers of traditional state-based licensure requirements for telehealth providers to facilitate the use of telehealth services. Though these changes may become more permanent, for now they are temporary, and should not be the basis for long-term planning related to utilization of telehealth.

• *Maintaining a relevant and responsive compliance infrastructure.* Maintaining relevant and robust compliance policies and processes always is essential for health-care organizations, especially as providers increase their submission of claims for telehealth services to government and private payers. Providers should track documentation requirements for submission of claims, and audit claims regularly to ensure lawful billing.

• *Being mindful of Medicare's anti-solicitation rules.* Generally, Medicare prohibits unsolicited telephone calls to beneficiaries. Telehealth providers may only call those who have opted-in to receive such communications. While there has been some loosening of certain restrictions—e.g., agents may send unsolicited emails to potential beneficiaries if there is an opt-out option—the relaxing of these requirements does not apply to telephone calls. Therefore, obtaining *and* documenting patient consent is critical.

• *Document, document, document.* Telehealth providers should keep meticulous records in patient files to withstand audit scrutiny. Consider investing in technology that enables the recording of virtual sessions with patients, as this is often a telehealth company's best line of defense in rebutting patient complaints and other allegations, and likely will become the new baseline expectation. Keeping contemporaneous records of when and why cost-sharing was waived (e.g., COVID-19 emergency declaration waiver), also will substantially assist in the inevitable disputes with government and private payors.

Melissa L. Jampol *is a Member of the Firm in the Health Care & Life Sciences and Litigation & Business Disputes practices, in the New York and Newark offices of Epstein Becker Green.* **Amy Lerman** *is a Member of the Firm in the Health Care &Life Sciences practice, in the firm's Washington, D.C., office.* **Elena M. Quattrone** *is an Associate in the Health Care & Life Sciences practice, in the New York office.*