Arnold & Porter

July 25, 2022

Relaxed Regulations Leads to a Surge in Telehealth Use . . . and a Surge of Enforcement

Advisory

By Allison W. Shuren, Jacqueline L. Degann, Michael C. Wood, Loreli (Lori) Wright

DOJ and Multiple Divisions of HHS Focus on Telehealth Fraud

Before the COVID-19 pandemic, telehealth made up less than one percent of Medicare visits and outdated billing policies made the use of telehealth modalities infeasible for most providers. A recent study by US Department of Health and Human Services' Office of Health Policy, however, shows that telehealth has exploded in recent years, with the number of Medicare fee-for-service (FFS) beneficiary telehealth visits increasing 63-fold in 2020, from approximately 840,000 in 2019 to nearly 52.7 million (five percent of Medicare FFS clinician visits) in 2020. Most beneficiaries (92%) received telehealth visits from their homes during the Public Health Emergency (PHE) which was not permissible under Medicare prior to the pandemic.[1]

With this unprecedented surge of telehealth usage—and the corresponding increase in government spending on telehealth services—multiple divisions of US Department of Health and Human Services (HHS) and the US Department of Justice (DOJ) have turned their attention to telehealth. Agencies are increasing enforcement actions against telehealth fraud, emphasizing suspect characteristics of problematic telehealth arrangements, and updating billing policies to allow greater flexibility to continue the use of some of the telehealth modalities that we've grown accustomed to during the Public Health Emergency.

Specifically, on Wednesday, July 20, HHS Office of Inspector General (OIG) released a special fraud alert (the Alert), highlighting the growth and prevalence of fraudulent and suspect arrangements within telemedicine and telehealth.[2] On the same day, DOJ announced that it charged telemedicine company executives, owners and executives of clinical laboratories, durable medical equipment companies, marketing organizations, and medical professionals for $1.2 billion in health fraud, stemming in part from the agency's increased focus on fraudulent telemedicine schemes, while the Centers for Medicare & Medicaid Services (CMS) and the Center for Program Integrity (CPI) announced it took adverse administrative actions against providers involved in similar telehealth schemes. Furthermore, CMS is scheduled later this month to publish proposed changes to the Medicare Physician Fee Schedule for CY2023 with long-awaited updates to telehealth policies.

OIG Special Fraud Alert

The Alert describes fraud schemes, specifically in the form of kickbacks, involving companies that purport to provide telehealth, telemedicine, or telemarketing services (collectively, "Telemedicine Companies"), exploiting the growing acceptance and use of telehealth. This commonly includes Telemedicine Companies paying practitioners in exchange for ordering or prescribing items or services: (1) for purported patients with whom the practitioners have limited or no interaction; and (2) without regard to medical necessity, leading to fraudulent billing and personally implicating practitioners and other health care workers for violating multiple federal laws including the federal anti-kickback statute[3], the Civil Monetary Penalties Law provision for kickbacks[4], the criminal health care fraud statute[5], and the False Claims Act.[6]

Although telehealth regulations were relaxed during the pandemic to allow increased access to providers, there has been a corresponding inverse correlation of fraud and abuse risk. The Alert sheds light into recent enforcement by OIG, as well as DOJ, on fraud cases involving kickbacks from Telemedicine Companies to practitioners, including fees to practitioners that correlate with the volume of federally reimbursable items or services, incentivizing a practitioner to order medically unnecessary items or services. The cases often involved at least one practitioner who never meaningfully (or ever) examined a patient to determine the medical necessity of ordered services, items, or prescriptions. Some cases cited fraud due to a lack of sufficient documentation or justification for orders resulting from telemedicine encounters, impacting the decision-making and care provided by other downstream providers or entities such as health systems,

pharmacies, durable medical equipment suppliers, laboratories and others. This further illustrates how telemedicine schemes found to be fraudulent by the agencies touch nearly every facet of the healthcare ecosystem—even those unconnected to the provision of telemedicine, or those several steps removed from such care.

To help make Practitioners aware of suspect arrangements within Telemedicine Companies, the Alert delineates suspect characteristics which, taken together or separately, could suggest an arrangement that presents a heightened risk of fraud and abuse:

- The practitioner orders or prescribes items or services to purported patients identified or recruited by the Telemedicine Company.[7]
- The practitioner does not have sufficient contact or information from the purported patient to meaningfully assess the medical necessity of the items or services ordered or prescribed.[8]
- The Telemedicine Company compensates the practitioner based on the volume of items or services ordered or prescribed.[9]
- The Telemedicine Company only furnishes items and services to federal health care program beneficiaries and does not accept insurance from any other payor.
- The Telemedicine Company claims to only furnish items and services to individuals who are not federal health care program beneficiaries but still bill federal health care programs.
- The Telemedicine Company only furnishes one product or a single class of products[10] potentially restricting a practitioner's treating options to a predetermined course of treatment.
- The Telemedicine Company does not expect practitioners (or another practitioner) to follow up with purported patients nor does it provide practitioners with the information required to follow up with purported patients.[11]

Although the Alert outlines multiple areas in which practitioners' involvement with Telemedicine Companies could violate federal laws and result in criminal, civil, or administrative liability, it is not intended to discourage legitimate telehealth arrangements.[12] OIG encourages practitioners to use heightened scrutiny, exercise caution, and consider the above list of suspect criteria prior to entering into arrangements with Telemedicine Companies.

DOJ Enforcement Actions

As of July 21, 2022, DOJ has highlighted 18 recently unsealed criminal actions alleging conspiracies to defraud federal healthcare programs within telehealth and telemedicine. Upwards of 36 defendants are suspected of kickbacks and bribes in exchange for the referral of Medicare beneficiaries for medically unnecessary genetic testing, durable medical equipment, and other supplies facilitated by telehealth.[13] The DOJ appears poised to reveal additional charges and schemes as other cases and investigations move forward.

These newly unsealed cases are similar to previous telehealth enforcement actions. In February a nurse practitioner (NP) in Georgia was convicted of health care fraud for her involvement in a complex telemedicine scheme.[14] It was found that the NP signed unnecessary orders for patients she never examined or spoke with, which were then sold to companies that generated reimbursement from Medicare. Similarly, in 2021, a series of criminal and civil enforcement actions under the False Claims Act in Michigan arose when telehealth marketers urged Providers to prescribe medically unnecessary or unwanted services on Medicare beneficiaries.[15] "Despite many red flags that these items and services were illegitimate," some practitioners were unaware of the scheme. DOJ highlighted that, had the providers taken "the time to listen to these recorded phone calls," they would have known that the calls were run by telemarketers and not medical professionals.

While signs of fraud may be more obvious in a traditional, in-person, provider's office, those aspects that make telehealth convenient and accessible may be the same factors allowing fraud to flourish undetected due to less obvious controls. Increased due diligence by Providers, in particular on how referrals and patient encounters are generated, may be required to ensure compliance with state and federal laws and reduce their risk of personal liability in enforcement actions. Although many of DOJ's nationwide enforcement actions remain under seal, recent trends suggest providers, health systems, pharmacies, durable medical equipment suppliers, laboratories and other health care providers should remain vigilant and enhance compliance controls related to telemedicine. Moreover, even where certain federal laws may not apply, providers and others should still take care to conduct appropriate due diligence as actions under broader state "all-payor" AKS statutes may follow.

Telehealth Changes in 2023 Physician Fee Schedule

In its forthcoming proposed rules, CMS recaps the process for adding new services to the list of telehealth services. Under the standard process, CMS adds services to the telehealth list if they are determined to fall within one of three categories of services:

- Category 1: Services similar to professional consultations, office visits, and office psychiatry services that are currently on the Medicare

telehealth list; or

- Category 2: Services that are not similar to those on the current telehealth services list but for which there is evidence demonstrating that the use of a telecommunications system to furnish the service produces demonstrated clinical benefit to the patient.
- Category 3: Services that were added to the Medicare telehealth services list during the PHE for which there is likely to be clinical benefit when furnished via telehealth, but there is not yet sufficient evidence available to consider the services for permanent addition under the Category 1 or Category 2 criteria.

Category 3 services ultimately need to meet the criteria under Category 1 or 2 in order to be permanently added to the Medicare telehealth services list.

CMS plans to retain all those services added to the Medicare telehealth services list on a Category 3 basis until the end of CY 2023 in order to permit development of more evidence that could support permanent addition to the list. The specific CPT codes added to Category 3 in the proposed rule include certain codes for ophthalmological services; speech, language, and audiology services; ventilation assistance management; neurological services; behavioral health services; physical, occupational, and speech therapy; critical care services; and patient self-management training. Additionally, CMS seeks to include prolonged services codes (GXXX1, GXXX2, and GXXX3) on the telehealth list on a Category 1 basis due to these services' similarity to psychiatric diagnostic procedures and office/outpatient visits currently on the list on a Category 1 basis.

Several other services which had been previously added to the Medicare telehealth services list on an interim basis in order to respond to the PHE for COVID-19 were not extended on a Category 3 basis in the CY 2023 proposed Final Rule. Accordingly, those services will no longer be covered when provided via telehealth, effective on the 152nd day after the expiration of the PHE.

CMS also plans to establish new policies for the use of modifiers and place of service (POS) codes for telehealth services. Telehealth services furnished before the end of the 151-day period will continue to be processed for payment as Medicare telehealth claims when accompanied with the modifier "95." During the 151-day period, physicians and practitioners can continue to report the POS code that would have been reported had the service been furnished in-person. After the end of the 151-day period, claims will no longer require modifier "95" but the appropriate POS indicator must be included - either POS "02" (re-defined as Telehealth Provided Other than in Patient's Home)[16] or POS "10" (redefined as Telehealth Provided in Patient's Home).[17]

Lastly, under current rules, after Dec. 31 of the year in which the PHE ends, the pre-PHE rules for direct supervision will apply and there will no longer be in place a temporary exception to allow immediate availability for direct supervision through virtual presence. In its proposed rule, CMS asks for information on whether the flexibility to meet the immediate availability requirement for direct supervision through the use of real-time, audio/video technology should potentially be made permanent.

Practitioners providing telehealth services or participating in telehealth arrangements should ensure they have adequate compliance systems in place to detect fraud as they navigate changing telehealth regulations.

[1] *Id.*

[2] Office of Inspector General (OIG), *Special Fraud Alert: OIG Alerts Practitioners To Exercise Caution When Entering Into Arrangements With Purported Telemedicine Companies*, (July 20, 2022).

[3] Section 1128B(b) of the Social Security Act (the Act).

[4] Section l 128A(a)(7) of the Act.

[5] 18 U.S.C. § 1347.

[6] 31 U.S.C. §§ 3729-33.

[7] Through use of telemarketing company, sales agent, recruiter, call center, health fair, and/or through internet, television, or social media advertising for free or low out-of-pocket cost items or services.

[8] The Alert makes reference specifically to audio only technology or when only patient demographics are included in the purported patient's medical records.

[9] This may be characterized to the Practitioner as compensation based on the number of purported medical records that the Practitioner reviewed.

[10] For example, durable medical equipment, genetic testing, diabetic supplies, or various prescription creams.

[11] For example, the Telemedicine Company does not require Practitioners to discuss genetic testing results with each purported patient.

[12] See "Principal Deputy Inspector General Grimm on Telehealth" (Feb. 26, 2021).

[13] U.S. Department of Justice, Telemedicine Enforcement Action, *Telemedicine Court Documents* (updated July 21, 2022).

[14] U.S. Attorney's Office Southern District of Georgia, *Georgia nurse practitioner convicted of health care fraud in complex telemedicine fraud scheme*, (Feb. 2, 2022). Additionally, a 2021 enforcement action involving more than $4.5 billion connected to telemedicine fraud identified schemes by providers that also implicated staffing and telemedicine companies who received money to sign orders that were prepared by telemarketers who had no medical training or certification. *See* U.S. Attorney's Office District of Montana, *Two Montana nurse practitioners admit telemedicine scheme to defraud Medicare of more than $18 million*, (April 21, 2022).

[15] U.S. Attorney's Office Western District of Michigan, *U.S. Attorney Announces Criminal And Civil Enforcement Actions Against Medical Practitioners For Roles In Telemedicine Fraud Schemes*, (Aug. 24, 2021).

[16] Descriptor: The location where health services and health related services are provided or received, through telecommunication technology. Patient is not located in their home when receiving health services or health related services through telecommunication technology.

[17] Descriptor: The location where health services and health related services are provided or received through telecommunication technology. Patient is located in their home (which is a location other than a hospital or other facility where the patient receives care in a private residence) when receiving health services or health related services through telecommunication technology.