COSMOS
Navigate the Compliance Universe

Compliance Today - November 2022

Allison M. Cohen (acohen@bakerdonelson.com,linkedin.com/in/allisonmcohen/) is Shareholder at Baker, Donelson, Bearman, Caldwell & Berkowitz PC, Washington, DC.

Telehealth compliance in the evolving landscape marked by increased OIG scrutiny

By Allison M. Cohen

Telehealth utilization grew significantly over the past few years to maintain access to critical healthcare services during a global pandemic. Numerous federal and state waivers, legislative flexibilities, and executive orders facilitated this growth by lifting some of the more challenging regulatory barriers and thereby making telehealth arrangements easier to structure in a compliant manner. Extensions of the U.S. Department of Health and Human Services' (HHS) public health emergency (PHE), as well as temporary legislation expanding Medicare coverage of telehealth services, have prolonged uncertainty regarding the regulatory landscape for telehealth when all COVID-19-related waivers and flexibilities terminate. At the same time, it is clear that HHS Office of Inspector General (OIG) has telehealth on its radar. To clarify its positions on telehealth compliance, OIG has been issuing guidance and publications to clarify its positions on telehealth compliance. By reviewing and analyzing noteworthy publications and national prosecutions, we can better understand the future of regulatory enforcement concerning telehealth arrangements.

2022 National Health Care Fraud Enforcement Action

The more broadly publicized OIG and the Department of Justice (DOJ) prosecutions have largely focused on schemes involving alleged violations of the federal Anti-Kickback Statute (AKS) [1] and submissions of false claims for the fraudulent provision of telehealth services in violation of the False Claims Act (FCA). OIG's "2022 National Health Care Fraud Enforcement Action" was a coordinated effort by OIG, DOJ, and law enforcement partners to combat healthcare fraud related to telehealth services.[2] In this most recent takedown, 36 defendants in 13 U.S. federal districts were charged with participating in fraudulent schemes involving telehealth-related technology. Defendants included telemedicine executives who allegedly paid practitioners to order medically unnecessary items and services, including laboratory testing and durable medical equipment (DME). The charges against the defendants were for more than $1.2 billion in fraudulent telemedicine, cardiovascular and cancer genetic testing, and DME schemes.[3] Additionally, the Centers for Medicare & Medicaid Services Center for Program Integrity (CPI) concurrently announced that it took administrative actions against 52 providers involved in similar schemes.[4]

Among the 2022 National Health Care Fraud Enforcement Action allegations were that laboratory owners and operators paid illegal kickbacks and bribes in exchange for referrals by medical professionals working with fraudulent telemedicine and digital health companies.[5] Cardiovascular genetic testing schemes have emerged as arrangements that will be subject to increased scrutiny after this recent prosecution.[6] Medicare had not approved cardiovascular testing for use as general screening tests proven to effectively indicate increased risk of

developing future cardiac conditions.[7] Nonetheless, over $174 million in false and fraudulent claims were allegedly submitted to Medicare based on orders for cardiovascular and genetic testing—the results of which were not used in the treatment of patients.[8] Similar to past telefraud schemes, some defendants were alleged to have controlled an international telemedicine network that used deceptive marketing techniques to target Medicare beneficiaries and induce them to agree to cardiovascular genetic testing, other genetic testing, and DME.[9]

These schemes involving purported telemedicine companies, telemarketers, and practitioners that were paid kickbacks in exchange for illegal referrals closely resemble the arrangements prosecuted in past telefraud takedowns. For example, "Operation Rubber Stamp" in the Southern District of Georgia targeted a similar criminal network involving individuals and companies that collected data from patients lured into the scheme by an international telemarketing network and sold it to DME suppliers, pharmacies, or labs.[10] Operation Rubber Stamp was part of a series of DOJ–HHS actions alleging telefraud, which also included Operations Double Helix and Brace Yourself.[11] The operations all involved enforcement of the AKS against illegal referral arrangements between telemedicine providers and manufacturers of DME (e.g., orthotic braces) and laboratory testing companies (e.g., cancer genetic tests).[12]

In both the recent and previous enforcement actions, the allegations do not suggest that the defendants' actions were good-faith efforts to provide telehealth services in which practitioners misunderstood billing requirements. Instead, there was often a complete failure to engage in any interaction that would qualify as telehealth, establish the practitioner/patient relationship, or satisfy any of the standards for remote services that could lead to legitimate orders for medical items or services. The earlier takedowns raised awareness and led to further scrutiny of telehealth services and arrangements in which companies that purport to provide telehealth services profit from false or fraudulent claims for medically unnecessary services.

Special Fraud Alert: OIG alerts practitioners to exercise caution

On July 20, 2022, concurrent with news releases related to the 2022 National Health Care Fraud Enforcement Action, the OIG issued a "Special Fraud Alert" to alert "Practitioners to Exercise Caution When Entering Into Arrangements with Purported Telemedicine Companies."[13] This Special Fraud Alert highlights OIG's key takeaways from investigations of various schemes, similar to those referenced above, involving fraud by companies that claimed to provide telehealth and telemarketing services (Telemedicine Companies).

OIG notes that these schemes commonly use kickbacks to aggressively recruit and reward practitioners for perpetrating fraud by ordering and prescribing unnecessary items and services for individuals whom telemedicine companies recruit.[14]

In many arrangements, the practitioners have limited interaction (if any) with the purported patient and prescribe or order items and services without regard to medical necessity or clinical appropriateness. Moreover, in many cases, the practitioner at issue does not even review actual medical records for the patient. Then the telemedicine company sells the practitioners' orders or prescriptions to other individuals or entities that fraudulently bill for the unnecessary items and services.

In several recent enforcement actions, practitioners, telemedicine companies, and other participants have been held liable for violations of the AKS, FCA, and other federal laws.[15] The OIG issued the Special Fraud Alert to highlight common elements of these schemes that could be red flags when entering arrangements with "telemedicine companies." These "suspect characteristics" include:

- Telemedicine Company recruits purported patients through their telemarketing, sales, call center, and social media advertising of free or low out-of-pocket cost items or services.
- Practitioner contact with purported patients is insufficient "to meaningfully assess the medical necessity of the items or services ordered or prescribed."
- Practitioner compensation by the telemedicine company is "based on volume of items or services" ordered or prescribed, which is sometimes characterized as number of purported medical records reviewed.
- "Telemedicine Company only furnishes items and services to Federal health care program beneficiaries and does not accept insurance from any other payor."
- Telemedicine Company fraudulently "claims to only furnish items and services to individuals who are not Federal health care program beneficiaries but may in fact bill Federal health care programs."
- "Telemedicine Company only furnishes one product or a single class of products (e.g., durable medical equipment, genetic testing, diabetic supplies, or various prescription creams), potentially restricting a Practitioner's treating options to a predetermined course of treatment."
- Telemedicine Company does not expect practitioners to follow up with purported patients nor does it provide Practitioners with the information required to follow up with purported patients (e.g., not requiring practitioners to discuss genetic testing results with each purported patient).[16]

The OIG noted that the "Special Fraud Alert is not intended to discourage the use of legitimate telehealth arrangements," but rather these "suspect characteristics" are intended to help practitioners identify questionable telemedicine companies that should be approached with "heightened scrutiny." The list is not exhaustive, nor is the presence or absence of any of the factors determinative of whether an arrangement with a telemedicine company could be subject to legal sanctions.[17]

An important point from both recent enforcement actions and the Special Fraud Alert is that the OIG is monitoring for arrangements that fail to provide telehealth services and result in orders or claims for medically unnecessary items and services. Healthcare practitioners and entities should carefully evaluate telehealth companies before entering arrangements; they should be particularly cautious of any company or arrangement that exemplifies any suspect characteristics identified by OIG.

Takeaways

- Similar to prior telefraud takedowns, a 2022 National Health Care Fraud Enforcement Action prosecuted illegal kickback schemes involving purported telemedicine companies.
- Office of Inspector General (OIG) recently issued a "Special Fraud Alert" to caution practitioners of certain "suspect characteristics" of arrangements with so-called telemedicine companies identified through recent enforcement actions.
- Telehealth practitioners in these suspect arrangements often have too little interaction with patients to assess the need for medically necessary services.
- Other suspect characteristics include—but are not limited to—compensation based on volume of services provided and only furnishing a single class of products (e.g., genetic testing).
- Healthcare practitioners and entities should be particularly cautious of any company or arrangement that

exemplifies any suspect characteristics identified by OIG.

1 42 U.S.C. § 1320a-7b(b); 42 C.F.R. §§ 1001.952 et seq.
2 U.S. Department of Health & Human Services Office of Inspector General, "2022 National Health Care Fraud Enforcement Action," last updated July 29, 2022, https://oig.hhs.gov/newsroom/media-materials/2022-national-health-care-fraud-enforcement-action/.
3 U.S. Department of Justice, "Justice Department Charges Dozens for $1.2 Billion in Health Care Fraud: Nationwide Coordinated Law Enforcement Action to Combat Telemedicine, Clinical Laboratory, and Durable Medical Equipment Fraud," news release, July 20, 2022, https://www.justice.gov/opa/pr/justice-department-charges-dozens-12-billion-health-care-fraud.
4 U.S. Department of Justice, "Justice Department Charges Dozens."
5 U.S. Department of Justice, "Justice Department Charges Dozens."
6 U.S. Department of Justice, "Justice Department Charges Dozens."
7 U.S. Department of Justice, "Justice Department Charges Dozens."
8 U.S. Department of Justice, "Justice Department Charges Dozens."
9 U.S. Department of Justice, "Justice Department Charges Dozens."
10 U.S. Department of Justice, U.S. Attorney's Office for the Southern District of Georgia, "Operation Rubber Stamp: Major health care fraud investigation results in significant new charges." October 7, 2020, https://www.justice.gov/usao-sdga/pr/operation-rubber-stamp-major-health-care-fraud-investigation-results-significant-new.
11 U.S. Attorney's Office, U.S. Attorney's Office for the Southern District of Georgia, "Operation Rubber Stamp."
12 Vrushab Gowda, "Telemedicine is No Cure for Fraud and Abuse," *Bill of Health* (blog), Petrie-Flom Center at Harvard Law School, October 26, 2020, https://blog.petrieflom.law.harvard.edu/2020/10/26/telemedicine-telehealth-fraud-abuse/.
13 U.S. Department of Health & Human Services, Office of Inspector General, "Special Fraud Alert: OIG Alerts Practitioners to Exercise Caution When Entering Into Arrangements with Purported Telemedicine Companies," July 20, 2022, https://oig.hhs.gov/compliance/alerts/sfa-telefraud.pdf.
14 U.S. Department of Health & Human Services, Office of Inspector General, "Special Fraud Alert: OIG Alerts Practitioners."
15 U.S. Department of Health & Human Services, Office of Inspector General, "Special Fraud Alert: OIG Alerts Practitioners."
16 U.S. Department of Health & Human Services, Office of Inspector General, "Special Fraud Alert: OIG Alerts Practitioners."
17 U.S. Department of Health & Human Services, Office of Inspector General, "Special Fraud Alert: OIG Alerts Practitioners."