HINSHAW

Alerts

The OIG Issues Special Fraud Alert Identifying "Suspect" Telemedicine Contract Arrangements

August 3, 2022
Health Care Alert

Attorneys

Michael A. Dowell

On July 20, 2022, the United States Department of Justice (the DOJ) announced charges against multiple defendants alleging fraudulent schemes (including telemedicine arrangements) totaling more than $1.2 billion. That same day, the OIG issued a Special Fraud Alert describing suspect characteristics (Suspect Characteristics) of fraudulent telemedicine arrangements between telemedicine companies (Telemedicine Companies) with practitioners (Practitioners) and providers (Providers). The continuing focus on telemedicine health care fraud schemes signals heightened enforcement scrutiny of such arrangements.

OIG and DOJ Telemedicine Enforcement Actions

The Special Fraud Alert notes that the Office of Inspector General (OIG) has conducted dozens of investigations of fraud schemes involving companies that purported to provide telehealth, telemedicine, or telemarketing services (collectively, Telemedicine Companies) and exploited the growing acceptance and use of telehealth.

In September 2020, the DOJ announced charges against 86 criminal defendants who submitted $4.5 billion in allegedly false and fraudulent claims connected to telemedicine. The DOJ alleged that "telemedicine executives paid doctors and nurse practitioners to order unnecessary, genetic and other diagnostic testing, and pain medication, either without any patient interaction or with only a brief telephonic conversation with patients they had never met or seen." The kickbacks received by the ordering providers resulted in false claims submitted to federal health care programs.

In September 2021, the DOJ announced charges against 138 defendants for their alleged participation in various health care fraud schemes that resulted in approximately $1.4 billion in alleged losses, which included $1.1 billion in fraud committed using telemedicine. According to the DOJ:

Certain defendant telemedicine executives allegedly paid doctors and nurse practitioners to order unnecessary durable medical equipment, genetic and other diagnostic testing, and pain medications, either without any patient interaction or with only a brief telephonic conversation with patients they had never met or seen. Durable medical equipment companies, genetic testing laboratories, and pharmacies then purchased those orders in exchange for

illegal kickbacks and bribes and submitted over $1.1 billion in false and fraudulent claims to Medicare and other government insurers. In some instances, medical professionals billed Medicare for sham telehealth consultations that did not occur as represented. The proceeds of the scheme were spent on luxury items, including vehicles, yachts, and real estate.

On July 20, 2022, the DOJ announced charges against 36 individuals involved in alleged telemedicine fraudulent schemes that resulted in $1.2 billion in alleged false and fraudulent telemedicine claims. One common element of the fraudulent telemedicine schemes was Telemedicine Companies using kickbacks to aggressively recruit and reward Practitioners and arranging with Practitioners to order or prescribe medically unnecessary items and services for patients who were solicited and recruited by Telemedicine Companies. According to the OIG:

"While the facts and circumstances of each case differed, often they involved at least one practitioner ordering or prescribing items or services for purported patients they never examined or meaningfully assessed to determine the medical necessity of items or services ordered or prescribed. In addition, telemedicine companies commonly paid practitioners a fee that correlated with the volume of federally reimbursable items or services ordered or prescribed by the practitioners, which was intended to and did incentivize a practitioner to order medically unnecessary items or services. These types of volume-based fees not only implicate and potentially violate the federal anti-kickback statute, but they also may corrupt medical decision-making, drive inappropriate utilization, and result in patient harm.

The OIG Telemedicine Special Fraud Alert

The OIG publishes Special Fraud Alerts to notify the healthcare industry that the OIG has become aware of certain abusive practices which the OIG plans to pursue and prosecute or bring civil and administrative action—as appropriate—to address potential violations of fraud and abuse laws including the Anti-Kickback Statute, False Claims Act and Civil Monetary Penalties Law. Accordingly, the Telemedicine Special Fraud Alert published by the OIG on July 20, 2022 followed enforcement and significant prosecutions of and settlements with individuals and entities that have engaged in suspect telemedicine arrangements with Telemedicine Companies. The Telemedicine Special Fraud Alert additionally identifies the risks of engaging in suspect arrangements with Telemedicine Companies. The objective of the Special Fraud Alert is to help healthcare organizations identify and correct potential problems in their telemedicine contractual arrangements.

Based on OIG's and DOJ's analysis of prior enforcement actions, the OIG developed the following list of Suspect Characteristics related to Practitioner and Provider arrangements with Telemedicine Companies which—taken together or separately—could suggest an arrangement that presents a heightened risk of fraud and abuse. The presence or absence of any one of the listed factors is not determinative of whether a particular arrangement with a Telemedicine Company would be grounds for legal sanctions. However, they do provide a basis for higher scrutiny and increased risks for violations.

The OIG identified the following as Suspect Telemedicine Contract Arrangements:

1. Telemedicine Company Patient Recruitment. The patients for whom the Practitioner orders or prescribes items or services were identified or recruited by the telemedicine company, 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.
2. Physician-Patient Relationship Not Established. The Practitioner has limited, if any, interaction with the patients (e.g., patient questionnaire or audio-only contact), and does not have sufficient contact with or information from the patient to meaningfully assess the medical necessity of the items or services ordered or prescribed. Practitioners are not given an opportunity to review the patient's real medical records (e.g., from the patient's primary care provider).
3. Physician Compensation Based On Services Ordered or Prescribed. The Telemedicine Company compensates the Practitioner based on the volume of items or services ordered or prescribed, which may be characterized to the Practitioner as compensation based on the number of purported medical records that the Practitioner reviewed. According to the OIG, "these types of volume-based fees not only implicate and potentially violate the Federal anti-kickback statute, but they also may corrupt medical decision-making, drive inappropriate utilization, and result in

patient harm."

4. Commercial Insurance Carve-Out. The telemedicine company only furnishes items and services to federal healthcare program beneficiaries and does not accept insurance from any other payer.
5. Governmental Payors Carve-Out, but Governmental Payors Billed. The telemedicine company claims to only furnish items and services to individuals who are not federal healthcare program beneficiaries but may, in fact, bill federal healthcare programs.
6. Telemedicine Company Only Furnishes One Product or One Class of Products. The telemedicine company only furnishes one product or a single class of products (e.g., durable medical equipment, genetic testing, diabetic supplies, or various prescription drugs), potentially restricting a practitioner's treating options to a predetermined course of treatment. Furthermore, the Telemedicine Company may direct Practitioners to order or prescribe a preselected item or service, regardless of medical necessity or clinical appropriateness
7. No Follow-up Care by Telemedicine Company. The telemedicine company does not expect practitioners (or another practitioner) to follow up with patients, nor does it provide practitioners with the information required to follow up with patients (e.g., the telemedicine company does not require practitioners to discuss laboratory test results with each patient).

According to the OIG, each of the Suspect Characteristics pose federal fraud and abuse concerns because of the potential for considerable harm to Federal health care programs and their beneficiaries, which may include: (1) an inappropriate increase in costs to Federal health care programs for medically unnecessary items and services and, in some instances, items and services a beneficiary never receives; (2) potential to harm beneficiaries by, for example, providing medically unnecessary care, items that could harm a patient, or improperly delaying needed care; and (3) corruption of medical decision-making.

Action Steps for Telemedicine Companies, Practitioners, and Providers

Practitioners and Providers who enter into arrangements with Telemedicine Companies in which one or more of the Suspect Characteristics are present should exercise caution, as failure to comply with applicable fraud and abuse laws may result in criminal, civil, or administrative liability depending on the facts and circumstances. Telemedicine Companies, Practitioners, and Providers engaged in telemedicine arrangements should adopt and implement Telemedicine compliance programs in order to ensure compliance with applicable laws. Telemedicine companies should compare their business practices against the Suspect Characteristics and, if necessary, make appropriate changes in updates/ modifications to their compliance programs.

Telemedicine Compliance Program

A telemedicine compliance program can demonstrate how a Telemedicine Company, Practitioner, or Provider meets or exceeds applicable legal requirements. Thus it is important that they adopt and implement an effective telemedicine compliance program, conduct a compliance program risk assessment to identify risk areas, and customize the telemedicine compliance program policies and procedures to address risk areas. Additional essential areas that should be encompassed by a telemedicine compliance program are set forth below:

- *State Telemedicine Laws*. A Telemedicine Company operating in all fifty states must comply with all State telemedicine laws governing valid physician-patient relationships and accepted telehealth modalities;
- *Provider Licensure.* Confirm compliance with applicable licensure requirements for Practitioners and Providers (including physician supervision, prescriptive authority, scope of practice, and standard of care);
- State laws generally require a physician to conduct an appropriate patient examination and assessment prior to issuing a prescription, if medically necessary. Documentation of the patient assessment/examination and implementation of appropriate controls to ensure that prescribed services or products are medically necessary is essential;
- *Provider Compensation Arrangements*. Evaluate all contractual or financial arrangements with physicians or referral sources and ensure that compensation does not vary by the volume or value of services provided; and also ensure that the compensation methodology does not result in prohibited fee splitting or violate corporate practice of medicine

prohibitions;

- *Payor Billing Arrangements.* Billing for services must be in compliance with state and federal laws as well as third-party payor requirements;
- *Referral Arrangements*. Assess all referral and payment relationships to make sure there are not any kickback, self-referral, or inducement issues. Telemedicine Companies, Practitioners, and Providers should establish and implement a written legal review and approval process for all telemedicine contractual arrangements;
- *Policies and Procedures.* Telemedicine policies and procedures should be designed to prevent and detect violations of applicable law—including permissible telemedicine modalities and telemedicine service documentation requirements. Policies and procedures should be documented in writing, and training should be provided to impacted employees.
- *Privacy and Security*. Telemedicine privacy and security protocols should include the use of HIPAA compliant messaging, voice and data transfer, and information storage. Telemedicine Practitioners and Providers should ensure that business associate agreements with Telemedicine Companies are in place and that patient authorization, consent, and notice is obtained and documented as required.

Conclusion

The OIG noted that the "Special Fraud Alert is not intended to discourage legitimate telehealth arrangements" but to use caution. The OIG's Special Fraud Alert—coupled with recent trends in telemedicine fraud and abuse enforcement actions—sends a clear forewarning that Telemedicine Company contractual arrangements will receive heightened scrutiny going forward. To avoid potential investigations and enforcement actions, Telemedicine Companies, Practitioners, and Providers should heed the OIG's guidance and carefully analyze the fraud and abuse risk associated with participating in any telemedicine arrangement. Risk assessments and auditing and monitoring of telemedicine arrangements are imperative. Entities and individuals engaged in telemedicine activities should consider retaining competent health law counsel with the knowledge and experience to help confirm that telemedicine arrangements are compliant and that identified risks have been mitigated and/or addressed.