Published on *The National Law Review* https://natlawreview.com

OIG Special Fraud Alert on Arrangements with Telemedicine Companies

Article By:

Nathaniel M. Lacktman

Pamela L. Johnston

Matthew D. Krueger

Jana L. Kolarik

On July 20, 2022, HHS-OIG published a new Special Fraud Alert on arrangements with telemedicine companies, setting forth seven characteristics OIG believes could suggest a given arrangement poses a heighted risk of fraud and abuse. The Alert follows dozens of civil and criminal investigations into fraud schemes involving companies that claimed to provide telehealth, telemedicine, or telemarketing services, but allegedly engaged in kickbacks and substandard medical practices to generate medically unnecessary orders and prescriptions. Those purported telemedicine companies, OIG stated in the Alert, "exploited the growing acceptance and use of telehealth" and present "the potential for considerable harm to Federal health care programs and their beneficiaries."

Alert Not Intended to Discourage Legitimate Telemedicine Arrangements

OIG was careful to state that not all telemedicine companies are suspect, and this Alert is not intended to discourage legitimate telemedicine arrangements. Indeed, in 2021, OIG previously noted , "[f]or most, telehealth expansion is viewed positively, offering opportunities to increase access to services, decrease burdens for both patients and providers, and enable better care, including enhanced mental health care." OIG is aware that many practitioners have appropriately used telehealth services during the current Public Health Emergency (PHE) to provide medically necessary care to their patients.

To help practitioners distinguish between suspect and bona fide telemedicine companies, the Alert contains a list of "suspect characteristics" which, taken together or separately, could suggest a telemedicine arrangement presents a heightened risk of fraud and abuse. Like prior Special Fraud Alerts, this new one is useful and practical because it establishes clear guiderails, summarized in a short, publicly-available document. Simultaneous with the release of this Alert, OIG updated its Telehealth Resource Page, which contains a warehouse of its compliance and enforcement resources.

Telemedicine Arrangement “Suspect Characteristics”

OIG developed a list of suspect characteristics related to telemedicine arrangements which, taken together or separately, could suggest the arrangement presents a heightened risk of fraud and abuse. The list is illustrative, not exhaustive, and the presence or absence of any one (or more) of these factors is not determinative of whether a particular arrangement with a telemedicine company would be grounds for legal sanctions.

1. The purported patients for whom the practitioner (clinician) 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. The practitioner does not have sufficient contact with or information from the purported patient to meaningfully assess the medical necessity of the items or services ordered or prescribed.

3. 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.

4. The telemedicine company only furnishes items and services to Federal health care program beneficiaries and does not accept insurance from any other payer.

    - For example, OIG noted instances in which a telemedicine company requires the practitioner to use audio-only technology to facilitate engagement with purported patients, regardless of their preference, and does not provide the practitioner with other telehealth modalities. Additionally, a telemedicine company may provide a practitioner with purported “medical records” that reflect only cursory patient demographic information or a medical history that appears to be a template but does not provide sufficient clinical information to inform the practitioner’s medical decision-making.

5. The telemedicine company 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.

    - An attempt to carve out Federal health care program beneficiaries from arrangements with telemedicine companies may still result in criminal, civil, or administrative liability for a practitioner’s role in any resulting fraudulent activity that involves Federal health care program beneficiaries.

6. 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 creams), potentially restricting a practitioner’s treating options to a predetermined course of treatment.

7. 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 (e.g., the telemedicine company does not require practitioners to discuss genetic testing results with each purported patient).

According to the OIG, schemes that contain these suspect characteristics can raise fraud concerns because of the potential for considerable harm to Federal health care programs and their beneficiaries. This 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.

What Will the Government Do Next?

The telehealth sector has blossomed and responded to the pandemic and assisted millions of patients in a time of need. Yet as the pandemic's intensity diminishes, many telemedicine companies that were previously cash-only retail medicine are now billing health insurance and the Federal health care programs (including Medicare, Medicaid, and TriCare) in order to diversify their sources of revenue and addressable market. This is a good thing for patient access to care and continued growth of digital health services. At the same time, this diversification in patient-payer mix, the expiration of PHE waivers, and the abatement of the pandemic will encourage DOJ and HHS-OIG to increase investigations of telemedicine companies and target arrangements and practices the government agencies believe are illegal.

This enforcement scrutiny will most likely arrive in the form of: 1) search warrants; 2) DEA subpoenas; 3) Grand Jury subpoenas; 4) civil investigative demands (CIDs) from DOJ in connection with False Claims Act investigations; and 5) HHS-OIG inquiries in connection with Civil Monetary Penalty and other investigations and audits. Moreover, False Claims Act data mining is thriving and companies cannot expect to fly under the radar, particularly when billing Federal healthcare programs. And the DOJ has renewed its pledge to hold individual executives personally liable for wrongdoing.

The Alert emphasizes the risk of illegal kickbacks posed by suspect arrangements between telemedicine companies and practitioners. If one purpose of the payment arrangement is to induce referrals of Medicare patients, that arrangement – particularly if notorious and not protected by a statutory/regulatory Safe Harbor – can place all participants at real risk of civil and criminal enforcement. Even subtle suspect arrangements can cause an employee or other knowledgeable person to file a *qui tam* / False Claims Act action under seal in court. If that occurs, DOJ is required to investigate the allegations in order to decide whether or not to intervene and take over the prosecution. Even non-criminal civil actions are a serious enforcement tool DOJ regularly relies upon to stop health care companies from entering into such arrangements.

What Does this Mean for DME/HME Companies, Genetics Labs, and Pharmacies?

As noted by OIG, a claim that seeks reimbursement for items or services resulting from a violation of the Federal anti-kickback statute constitutes a false or fraudulent claim for purposes of the False Claims Act. OIG specifically flagged its concern with kickbacks paid in exchange for prescriptions of durable medical equipment, genetic tests, wound care items, diabetic supplies, and prescription creams/medications. Entities billing such items based on orders sent by telemedicine companies should be diligent in vetting their practices and marketing arrangements to reduce compliance risk.

What Does this Mean for Telemedicine and Digital Health Companies?

In short: conduct a privileged compliance review of your current operations and arrangements, identify risk areas, and promptly fix them. After nearly three years operating under PHE waivers, some executives may assume the waivers will continue indefinitely (they won't). Do not wait until the very last minute before planning out what operations your company must change when the waivers end. Instead, responsible entrepreneurs and investors in the digital health industry should anticipate this wave of DOJ and OIG investigations, and alter their practices now to conform to a post-waiver world.

Another prudent approach, particularly for those companies moving into third party reimbursement, is to implement a healthcare fraud and abuse compliance program. An effective compliance program can not only serve as a mitigating factor if a company becomes the target of an investigation, it can (ideally) keep the company's operations in check so it doesn't become a target in the first place. Compliance programs can also make use of the data already available in the company to get ahead of the government's data mining. Compliance programs are customized and scaled to the specific company, and need not be a significantly expensive undertaking.

There is a difference between bona fide digital health services and suspect arrangements that do not involve the legitimate use of telemedicine technology to deliver medical care. OIG refers to the latter as "telefraud" schemes, and has noted it is important to distinguish those schemes from "telehealth fraud." In contrast to telefraud schemes, OIG has studied how telehealth can be an important tool to improve patient access to behavioral health services. OIG even issued a policy statement and a fact sheet explaining that "physicians and practitioners do not risk enforcement action if they waive any cost-sharing for telehealth visits during the Public Health Emergency."

We will continue to monitor and track for updates.

National Law Review, Volume XII, Number 201