

OIG Issues Special Fraud Alert Regarding Telemedicine Arrangements

Health Care Law Brief Blog on July 21, 2022

On July 20, 2022, the Office of Inspector General for the Department of Health and Human Services (“OIG”) issued a [special fraud alert](#) (“Alert”) advising “practitioners to exercise caution when entering into arrangements with purported telemedicine companies.” The Alert is only one of four such “[special fraud alerts](#)” that the OIG has issued in the past decade and it illustrates the importance of OIG’s statements.

OIG Flags Seven Characteristics of Telehealth Fraud

In the Alert, OIG cautions that certain companies that purport to provide telehealth, telemedicine, or telemarketing services (collectively, “[Telemedicine Companies](#)”) have carried out fraudulent schemes by: (i) aggressively recruiting physicians and non-physician practitioners (collectively, “[Providers](#)”) and (ii) paying kickbacks to such Providers in exchange for the ordering of unnecessary items or services, including durable medical equipment, genetic testing, and other prescription items. According to OIG, the fraudulent schemes have varied in design and operation and involved a variety of individuals, Providers, and health care vendors, including call centers, staffing companies, and marketers.

The Alert identifies seven suspect characteristics in telehealth arrangements, which present a heightened risk of fraud and abuse under applicable Federal health care laws:

1. Recruitment of patients by a telemarketing company, sales agent, recruiter, call center, or health fair, and/or through internet, television, or social media that advertised free or low out-of-pocket cost items or services.
2. Encounters in which a Provider 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.

3. Compensation of Providers based on the volume of items or services ordered or prescribed, which may be characterized to the Provider as compensation based on the number of purported medical records that the Provider reviewed.
4. Furnishing items and services only to Federal health care program beneficiaries.
5. Carving out Federal health care program beneficiaries, notwithstanding the fact that the entity may bill Federal health care programs. The OIG notes that carve-out arrangements may still result in criminal, civil, or administrative liability for a Provider for any resulting fraudulent activity that involves Federal health care program beneficiaries.
6. Furnishing only one product or a single class of products (g., durable medical equipment, genetic testing, diabetic supplies, or various prescription creams), and the restriction by a Telemedicine Company of a Provider's treatment options to a predetermined course of treatment.
7. An expectation by the Telemedicine Company that the Provider does not follow up with patients, and the Telemedicine Company failing to furnish Providers with information required to follow up with patients (g., the telemedicine company does not require Providers to discuss genetic testing results with each purported patient).

Providers Face Risks Despite Assurances Made by Entities Involved in Suspect Schemes

The Alert also describes how Telemedicine Companies involved in fraudulent schemes have “often” told Providers that they do not need to contact their patients, or that they only need to speak to the patients by telephone. The OIG’s statement is significant as it implies that some fraudulence schemes use Providers’ unfamiliarity with technology, inexperience with telehealth, and lack of knowledge regarding telehealth legal requirements, to involve potentially unwitting participants in the schemes. The allegation should be particularly concerning to health care providers involved in telehealth arrangements where the providers rely upon the advice of a third party, who is not their attorney or employer, to assist them in complying with the laws, regulations, and payor requirements governing telehealth encounters.

Given that telehealth recently gained widespread acceptance, as a result of the COVID-19 pandemic, many health care providers and companies lack a comprehensive understanding of the complex federal and state regulatory regime implicated by the use of telehealth. For example, whether a telehealth encounter can be conducted via telehealth, or whether an encounter can occur via asynchronous technology such as online forms, is a fact-specific analysis that depends upon the laws of the state, the type of patient encounter, and, where seeking reimbursement, the applicable payer requirements.

The Alert Reflects the Government's Continued Interest in Identifying and Rooting Out Telehealth-Related Fraud

The Alert describes that the OIG “has conducted dozens of investigation of fraud schemes that purported to provide telehealth, telemedicine, or telemarketing services.” The Alert follows a series of Department of Justice (“[DOJ](#)”) prosecutions related to telehealth. For example, in the span of one month alone—May 2021—DOJ announced two indictments alleging a similar fact pattern: the payment of kickbacks in return for the issuance, via telehealth, of genetic testing orders. Moreover, on the same day that the Alert was issued, DOJ [announced](#) a wide-ranging prosecution against 36 individuals, across 11 federal judicial districts, involved in various telehealth-related schemes.

Resources for Telehealth Companies and Providers

As we’ve previously [addressed](#), persons and entities engaged in telehealth arrangements must recognize that such platforms implicate the laws of every jurisdiction in which patients are located, including any federal laws that may apply. Therefore, a telehealth platform operating in all fifty states will, for example, need to comport with the laws governing telehealth encounters, including provider licensure and scope of practice, in all fifty states. Moreover, in order to substantiate the validity of any telehealth encounter, practitioners engaged in the rendering of care via telehealth means must ensure that those encounters comport with the requirements of state law, payor billing requirements (which may be more stringent than state law), and the standard of care.

To provide educational information to the public, the OIG has also updated its [telehealth webpage](#) with a variety of resources, including prior announcements and prosecutions.

[View Original](#)

- **Matthew J. Westbrook**
Senior Counsel
- **Jonian Rafti**
Associate