OIG is Circling the Telehealth Industry

Insights 10.28.22

As published in Law360 on July 28, 2022 and updated on October 18, 2022.

On July 20, the U.S. Department of Health and Human Services Office of Inspector General (OIG) issued a special fraud alert[1] advising health care providers to exercise caution when entering into arrangements with purported telemedicine companies.

Below, we explore the potential changes in OIG enforcement priorities that the new fraud alert indicates may be afoot and contextualize the significance of a special fraud alert in the health care fraud enforcement landscape.

PROFESSIONAL

DAVID S. SCHUMACHER
Partner
Boston

What is a special fraud alert?

The OIG periodically issues reports regarding potentially fraudulent and abusive health care practices it has recently identified and intends to investigate and prosecute. The purpose of a special fraud alert is to notify the health care community about the OIG's concerns to encourage providers to review their own practices to improve compliance.

Special fraud alerts are rare and significant.

The OIG issues special fraud alerts intermittently, without warning. While the OIG issued 11 special fraud alerts between 1994 and 2000, the new fraud alert is only the fourth special fraud alert issued in the last decade.

By comparison, the OIG published a dozen advisory opinions in the first half of 2022 alone. The government views special fraud alerts as important events, putting providers on notice of potentially abusive practices.

Indeed, some aggressive U.S. Department of Justice prosecutors take the position that a provider cannot raise a good faith defense if a practice under investigation was previously highlighted in a special fraud alert — a position that would be subject to a robust challenge, as a practice identified in a special fraud alert does not constitute a per se violation.

Sometimes, a special fraud alert serves as a vanguard for new enforcement activity — such as the 2014 alert concerning laboratory payments to referring providers. In contrast, some special fraud alerts highlight practices that have already received significant attention from the DOJ — such as the 2020 alert concerning pharmaceutical company speaker programs. Invariably, a special fraud alert is a harbinger of increased enforcement activity.

Importantly, the OIG expressly states in the new fraud alert that the presence of the identified suspect characteristics does not necessarily mean that a telemedicine arrangement is problematic.[2] That said, OIG labeling certain behaviors as suspect means that companies deploying these tactics may materially increase their chances of receiving unwanted attention from enforcement agencies.

Telemedicine has exploded in recent years, and is an important tool in providing access to care.

Telehealth utilization by Medicare beneficiaries has historically been quite low, for reasons including restrictive coverage and reimbursement requirements for Medicare telehealth services forth in Section 1834(m) of the Social Security Act[3] and concerns from certain lawmakers about expanded telehealth leading to increased costs and upticks in fraud.

During the COVID-19 public health emergency, each of the burdensome restrictions on Medicare telehealth services was either waived entirely or lessened in some manner, leading to an increase in telehealth utilization of no less than 6,300% among Medicare beneficiaries in 2020, according to a 2021 report published by HHS.[4]

OIG has at various times acknowledged the important role that telehealth and other digital health innovation can play as a means to provide better access to care, as part of health care system delivery reform efforts to lower costs and improve quality.[5] As another example, OIG issued a report in September that concludes the temporary expansions under Medicare "improved access to telehealth for Medicare beneficiaries, particularly for those who are medically underserved" – specifically, urban and Hispanic beneficiaries. OIG recommended that CMS take steps to transition from current pandemic-related flexibilities to "well-considered long-term policies" and use telehealth to advance health care equity.

At the same time, the proliferation of telemedicine has attracted attention from the DOJ and OIG.

Telehealth has been included on the OIG work plan since at least 2017, and enforcement actions began to pop up before the public health emergency, many of which focused on allegations of fraudulent arrangements involving products like durable medical equipment and prescription pain creams.[6]

The government's enforcement efforts intensified in September 2020, when the DOJ and OIG announced a national telefraud takedown, targeting illegal kickbacks paid by durable medical equipment companies, laboratories and pharmacies tied to medically unnecessary orthotic braces, diagnostic testing and prescription drugs payable by federal health care programs.

Those schemes essentially reinvented traditional fraud tactics through new modalities, and had little to do with the sort of virtual care so many Americans have received during the public health emergency in the form of synchronous audio-video and audio-only interactions.

Separately, OIG issued a report in September 2022 evaluating telehealth services during the first year of the pandemic, and implied particular scrutiny of telehealth companies.[7] OIG reviewed claims billed by 742,000 providers. Of those providers, OIG identified 1714 whose billing posed a high risk — approximately 0.2% of all providers). OIG further identified 41 of these providers as appearing to be associated with telehealth companies, though OIG had no systematic way to confirm — approximately 0.2% of the 0.2% presenting a high risk. Still, OIG expressly called out such companies in the report, noting that 1 of the outlier providers that appeared to be associated with a telehealth company was billing for seeing an average of 75 beneficiaries a day. One of its recommendations to CMS moving forward was to identify telehealth companies that bill Medicare.

The new OIG special fraud alert identified suspect characteristics.

In the new fraud alert, the OIG continues to target durable medical equipment companies, laboratories and pharmacies — industries implicated in the September 2020 takedown — while adding diabetes suppliers to the OIG's watchlist.

The OIG focuses on a number of factors in the new fraud alert that could be indicia of fraudulent activity and result in an enforcement action. Of note, the OIG specifically mentions virtual care companies and other provider groups utilizing telehealth technology, indicating a pivot within OIG to focus on digital health companies involved in the provision of virtual

care. The factors include:

- The purported 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, or through internet, television or social media advertising for free or low out-of-pocket cost items or services.
- 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.
- 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.
- 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 may in fact bill federal health care programs.
- 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.
- The telemedicine company does not expect clinicians to follow up with purported patients nor does it provide clinicians 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).

New emphasis has been placed on marketing and clinical decision making.

In addition, the new fraud alert expressly labels proactive marketing — including via social media — to advertise free or low-cost items or services covered by federal health care programs and exclusively marketing to beneficiaries of federal health care programs as suspect behavior.[8]

The Federal Trade Commission has also levied scrutiny on digital health companies in recent months focused on deceptive marketing and advertising practices, suggesting these issues could be at the forefront of discipline in telehealth moving forward.

The new fraud alert also labels models in which practitioners have limited choice in the treatment they can prescribe or the ways that they can communicate with patients as suspect, as well as models which neither require nor enable practitioners to provide follow-up care to their patients. It is clear based on the 2022 fraud alert that these practices materially increase the risk of government scrutiny and investigation.

Carving out federal health care programs is not a cure-all.

Many digital health companies operate on a cash-pay basis or do not bill federal health care programs. Some providers believe that omitting federal payors insulates them from federal fraud and abuse laws.

While many federal health care laws, including the federal anti-kickback statute, only apply to providers that bill federal health care programs, other federal laws, such as the Travel Act, potentially apply to practices impacting commercial payors.

In addition, state attorneys general, insurance commissioners and other agencies with broader jurisdiction — not to mention potential investors, health system affiliates, and commercial payors with whom growing digital health companies are eager to establish relationships — are all likely to review the new fraud alert with great interest as they assess the practices of telemedicine companies .

Finally, most states have their own versions of the federal laws addressing kickbacks and self-referrals, some of which are all-payor, meaning they even apply to direct-to-consumer cash-pay models.

The time for proactive compliance reviews is now.

The new fraud alert should be a flashing red light to the digital health community. The time to review and assess operations that touch on the topics addressed in the new fraud alert, including those that may have arisen during the public health emergency alongside the exponential growth of telehealth, is now.

A self-assessment could include review of current marketing practices, clinical autonomy and robustness of clinical decision making, compensation arrangements with referral sources, and remuneration to potential and current patients.

Based on experience with past special fraud alerts, numerous telehealth companies are likely to face subpoenas, civil investigative demands, and other inquiries from the OIG and the DOJ, and any practices that were identified in the new fraud alert will be regarded with suspicion.

While past telemedicine enforcement focused on companies which might be viewed as bad actors and the prescribing practices of specific practitioners, the next wave may cast a wider net. Such an approach could ultimately entangle companies making good faith compliance efforts, but which may not have contemplated or addressed the risk areas identified in the new fraud alert.

If you have any questions, please contact David Schumacher, Amy Joseph, or Jeremy Sherer in Boston, or any other member of our Hooper, Lundy & Bookman team.

[1] https://oig.hhs.gov/documents/root/1045/sfa-telefraud.pdf.

[2] By comparison, OIG states in the 2013 SFA addressing physician-owned distributors (PODs) that "OIG views PODs as inherently suspect under the anti-kickback statute."

[3] We discuss the status of those statutory restrictions here.

[4] HHS Office of the Assistant Secretary for Planning and Evaluation ("ASPE"), Medicare Beneficiaries' Use of Telehealth in 2020: Trends by Beneficiary Characteristics and Location (Dec. 3, 2021).

[5] See, e.g., 85 Fed. Reg. 77712 (Dec. 2, 2020) ("digital health companies hold great promise for improving coordination and management of care and achieving the goals of the Regulatory Sprint [to Coordinated Care]").

[6] See, e.g., U.S. Dept. of Justice Press Release, Four Men and Seven Companies Indicted for Billion-Dollar Telemedicine Fraud Conspiracy, Telemedicine Company and CEO Plead Guilty in Two Fraud Schemes (Oct. 15, 2018); U.S. Dept. of Justice Press Release, Federal Indictments & Law Enforcement Actions in One of the Largest Health Care Fraud Schemes Involving Telemedicine and Durable Medical Equipment Marketing Executives Results in Charges Against 24 Individuals Responsible for Over $1.2 Billion in Losses (Apr. 9, 2019).

[7] Medicare Telehealth Services During the First Year of the Pandemic: Program Integrity Risks OEI-02-20-00720 09-02-2022 (hhs.gov) (Sept. 2, 2022).

[8] At least some of the uptick in providers openly marketing their waiver of copays during the PHE relates to HHS-OIG's March 2020 declaration that copays could be waived for Medicare beneficiaries during the PHE. See HHS-OIG Fact Sheet, March 2020.

RELATED CAPABILITIES

Digital Health and Other Health Technologies