

## DOJ & OIG RAMP UP ENFORCEMENT AND OVERSIGHT TO COMBAT TELEMEDICINE FRAUD

On September 2, 2022, the Office of the Inspector General (“OIG”) published a [study](#) assessing potential Medicare program integrity risks related to the proliferation of telehealth services during the first year of the COVID-19 pandemic. OIG identified 1,714 providers with billing practices deemed “high risk” to the Medicare program. These providers billed approximately 500,000 beneficiaries and received \$127.7 million in Medicare fee-for-service payments. Although these high-risk providers represent a small proportion of total telehealth services, OIG noted a need for “strong, targeted oversight of telehealth services.” To that end, OIG is recommending that CMS: (1) strengthen monitoring and targeted oversight of telehealth services; (2) provide additional education to providers on appropriate billing for telehealth services; (3) improve the transparency of “incident to” services when clinical staff primarily delivered the telehealth service; (4) identify telehealth companies that bill Medicare; and (5) follow up on the providers identified in the report.

This study comes on the heels of a recent [Press Release](#) issued July 20, 2022 (“Press Release”), in which the Department of Justice (“DOJ”) announced criminal charges against 36 defendants in 13 federal districts across the United States largely alleging fraud in the telemedicine space. On that same day, OIG issued a [Special Fraud Alert](#) (“Alert”) alerting health care practitioners to the risk associated with certain telehealth arrangements.

The charges were the result of a nationwide coordinated investigative effort that focused on alleged schemes involving laboratory owners and operators paying illegal kickbacks to providers working with telemedicine/digital medical technology companies in exchange for patient referrals. Specifically, among the allegations contained in [court documents](#), the government alleged that telemedicine companies arranged for medical professionals to order expensive genetic tests and durable medical equipment regardless of patient need and sometimes without any patient interaction or with only a brief telephonic conversation.

According to the DOJ, losses from the alleged fraudulent conduct exceeded \$1.2 billion, with over \$1 billion of that amount involving telemedicine schemes.

### GOVERNMENT CONTINUES NATIONAL CRACKDOWN ON TELEMEDICINE-RELATED FRAUD

The Press Release also comes after a string of prior DOJ telemedicine enforcement actions involving more than \$8 billion in fraud in just three years. Inspector General Christi A. Grimm of the U.S. Department of Health and Human Services stated that the latest enforcement action reinforces the department’s commitment to “...disrupt[ing] fraud schemes that use the guise of telehealth to expand the reach of kickback schemes designed to cheat federally funded health care programs.”

### PROVIDERS BEWARE: OIG FLAGS SEVEN CHARACTERISTICS OF FRAUDULENT TELEHEALTH ARRANGEMENTS

In the wake of the DOJ announcement, OIG issued the Alert in which it identified [seven suspect characteristics](#) of fraudulent telehealth arrangements. (These include 2019’s [Operation Brace Yourself](#), 2019’s [Operation Double Helix](#), 2020’s [Operation Rubber Stamp](#), and the telemedicine component of the 2021 [National Health Care Fraud Enforcement Action](#).) The “suspect characteristics,” which present a heightened risk of criminal, civil and administrative liability under applicable federal health care laws, include the following:

1. The telemedicine company identifies and recruits patients by advertising free or low out-of-pocket cost items or services.
2. The practitioner has insufficient patient contact or information to meaningfully assess the medical necessity of what is ordered or prescribed.
3. The telemedicine company compensates the practitioner based on the volume of items or services ordered or prescribed.
4. The telemedicine company provides items and services only to federal health care program beneficiaries.
5. The telemedicine company claims to provide items and services to non-federal beneficiaries but still bills federal health care programs.
6. The telemedicine company only provides one product or a single class of products (e.g., durable medical equipment, genetic testing,

diabetic supplies or various prescription creams), thereby restricting a practitioner's treatment options to a predetermined course of treatment.

7. The telemedicine company expects practitioners not to follow up with patients or fails to provide practitioners with the necessary information to follow up with patients (e.g., the telemedicine company does not require practitioners to discuss genetic testing results with each purported patient).

## **PRACTICAL TAKEAWAYS**

The above reports and announcements underscore the reality of OIG's continued focus on, and aggressive enforcement efforts in, the telemedicine space. While many of the characteristics identified in the Alert have the hallmarks of outright fraud and involve egregious conduct, providers and telehealth companies should consider the identified "suspect characteristics" when structuring patient care arrangements.

To that end, particularly with respect to arrangements involving remote prescribing by physicians without a pre-existing patient relationship, participants should consider the following questions when assessing the potential risk of a telemedicine arrangement:

- Does the arrangement involve exclusively, or primarily, on federal health care program business?
- How is the telemedicine company generating or soliciting its beneficiary referrals?
- *What safeguards exist to ensure their practitioners have sufficient patient contact and information to assess the medical necessity of goods and services ordered?*
- Do the practitioners employ interactive video assessments, or do they resort to quick telephone calls and/or offline reviews of intake sheets?
- Are practitioners compensated per evaluation or only for those for which they order durable medical equipment supplies?
- Are the practitioners limited in prescribing or ordering only one of the manufacturer's products (or class of products)?
- Has qualified health care counsel analyzed the telemedicine company's current or proposed arrangements?

Given the high stakes and the complex regulatory environment involved, and in light of OIG's "targeted oversight" of telehealth services, providers are strongly encouraged to seek counsel for appropriate telehealth legal analyses and business arrangement strategies.

If you would like assistance reviewing your current or proposed telehealth operations or arrangements, or if you have any other questions related to health care compliance, please contact:

- [Chris Eades](mailto:ceades@hallrender.com) at (317) 977-1460 or [ceades@hallrender.com](mailto:ceades@hallrender.com).
- [Keith Dugger](mailto:kdugger@hallrender.com) at (214) 615-2051 or [kdugger@hallrender.com](mailto:kdugger@hallrender.com);
- [Erin Drummy](mailto:edrummy@hallrender.com) at (317) 977-1414 or [edrummy@hallrender.com](mailto:edrummy@hallrender.com);
- [Joe Wolfe](mailto:jwolfe@hallrender.com) at (414) 721-0482 or [jwolfe@hallrender.com](mailto:jwolfe@hallrender.com); or
- Your primary Hall Render contact.

Special thanks to Avi Kerendian, Summer Associate, for assisting with this article.

*Hall Render blog posts and articles are intended for informational purposes only. For ethical reasons, Hall Render attorneys cannot give legal advice outside of an attorney-client relationship.*