Client Alert: Regulators Turn Their Eyes to “Tele-Fraud”

A Priority Telehealth Update: Regulators Turn Their Eyes to “Tele-Fraud”

On July 20, 2022, the Office of the Inspector General (“OIG”) for the Department of Health and Human Services announced a Special Fraud Alert on the subject of “tele-fraud” (telehealth-related fraud). The trend towards greater focus on prevention and enforcement activity against telehealth fraud has been almost inevitable. The Covid-19 pandemic acted as a galvanic force for widespread adoption and third party payer coverage for telehealth services. As is universally the case when the government and payers expand coverage, healthcare “profiteers” looking to exploit the new opportunity moved into telehealth. The result is that an initial new “door opening” shifts into a phase of rooting out fraud and abuse.

With the public health emergency related to Covid-19 winding down, the government infrastructure that has already been shifting to examine Covid-19-related fraud and abuse more generally is also being redirected in a long-term manner toward telehealth. In part, this can be seen as part of the “normalization” of telehealth across multiple government agencies. From the Centers for Medicare and Medicaid Services (CMS) to the U.S. Department of Justice (DOJ), there appears to be recognition that, in the post-pandemic era, telemedicine will be a permanent feature of government-funded U.S. healthcare.

The recent Special Fraud Alert follows months of investigations, trial convictions, and reports related to telemedicine providers utilizing inducements and kickback to incentivize providers into ordering various medical tests and billing services that are deemed neither medically necessary nor clinically appropriate. The Alert details multiple types of “suspicious” activities that could signal fraudulent behavior. The Office of the Inspector General (OIG) recommends that patients, practitioners, and businesses involved in telemedicine proceed cautiously when encountering any of the following arrangements.

- Situations where practitioner-patient contact is so limited as to question whether an authentic clinical assessment was made.
- Lack of follow-up with patients, as well as no reliable means for patient or other medical professionals to follow-up with tele-provider.
- Significant difficulties accessing medical information relating back to telehealth patient-provider encounter.
- Aggressive outreach and advertisements offering free or low out-of-pocket-cost services to patients.
- Telehealth companies that reimburse practitioners based on volume metrics, such as the number of services ordered or medications prescribed.
- Telemedicine providers who work exclusively with patients enrolled in federally-funded health programs, while rejecting insurees covered by privately-funded plans.
- Organizations that direct their recruitment toward patients with private insurance while billing government-funded insurers.
- Companies that specialize in a single service or medical product (e.g. durable medical equipment, genetic testing, diabetes supplies, or topical prescription creams), particularly, when there appear to be an exceptionally limited, or uniformly homogenous, treatment options.

Ironically, many of the features about which the Special Alert complains resemble the direct-to-consumer, cash pay telehealth world of “focused condition” telehealth: providers who market limited, specialized treatment, often at low, out-of-pocket cost, that allows for standard of care to be satisfied through a digital encounter with limited diagnostic information. Nothing in the Special Alert should be read as an attack on direct-to-consumer telemedicine. When consumers are bearing the cost directly of this form of telemedicine, which has grown in popularity significantly in recent years, many of the features described by the government are unproblematic. American consumers have voted with their utilization of focused-condition telehealth platforms that they want efficient, convenient service offerings where standard of care allows for health professionals to provide it via telemedicine.

The difference in the area of federally-funded (and insurance-reimbursed) health programs, many features of

streamlining are leading regulators to suspect motivations of profiteering rather than efficiency. It is likely to be a slower process to see broad-based coverage of focused-condition healthcare by third party payers, including government programs. Fraud issues from verifying the identity of the provider to establishing medical necessity will require further evolutions in both telehealth technology and health policy.

For the time being, the recent string of DOJ criminal investigations and civil enforcement sanctions under the federal False Claims Act and the Anti-Kickback Statute are likely to continue and expand in telehealth. (We will detail more highlights of recent enforcement activity in a future update.) For providers relying on telemedicine in the context of government programs, including Medicare and Medicaid, and other third-party payer coverage, it is advisable to review the considerations raised in the Special Alert and to consider the risks associated with "tele-fraud."

Authored By:

Harry Nelson, Managing Partner, Nelson Hardiman
Daniel Eliav, Attorney, Nelson Hardiman
Yehuda Hausman, Law Clerk, Nelson Hardiman

Nelson Hardiman LLP, Healthcare Law for Tomorrow

Nelson Hardiman regularly advises clients on new healthcare law and compliance. We offer legal services to businesses at every point in the commercial stream of medicine, healthcare, and the life sciences. For more information, please contact us.

Interested in learning more?

Nelson Hardiman is hosting a series of webinars delving deeper into the regulatory questions at the intersection of telemedicine and abortion. For additional information, please visit our event website. To learn more about our telehealth practice, contact us today.