

## OIG Warns Telehealth Industry: “With Great Power Comes Great Responsibility”

Article By:

Matthew M. Shatzkes

Eva Schifini

John M. Tilton

---

On February 4, 2021, the Department of Justice (“DOJ”), Office of Public Affairs, issued a Press Release (the “[DOJ Press Release](#)”) announcing that Kelly Wolfe, President of Regency, Inc., a medical billing company located in Florida, pleaded guilty to conspiracy to commit healthcare fraud through a “pernicious telefraud scheme”<sup>[1]</sup> involving fraudulent Medicare and CHAMPVA (Civilian Health and Medical Program of the Department of Veterans Affairs) claims for medically unnecessary durable medical equipment (“DME”) supplies. As a result of Wolfe’s criminal plea, Wolfe could face up to 13 years in federal prison.

In addition to her criminal plea, Wolfe and Regency agreed to a [civil settlement](#) of up to \$20,332,516 to resolve allegations that Wolfe and her co-conspirators violated the federal False Claims Act and the federal Anti-Kickback Statute by bribing physicians to write prescriptions for DME supplies based upon non-existent telemedicine visits and procedures involving Medicare and CHAMPVA beneficiaries. With these phony prescriptions in hand, the sham DME companies collectively submitted well over \$400 million in illegal Medicare and CHAMPVA claims before the companies were shut down as part of the “Operation Brace Yourself” – a joint initiative of the DOJ, the Federal Bureau of Investigation and other federal agencies designed to root out and shut down fraudulent practices in the telemedicine and DME industries.

In the DOJ’s statement about the case, the Department of Health and Human Services’ Office of the Inspector General (“OIG”) referred to these collective allegations as a “pernicious telefraud scheme.” Telehealth industry leaders, such as the [American Telemedicine Association](#) and the [Alliance for Connected Care](#) have rebuked this categorization and requested that the DOJ and OIG avoid conflating telefraud and “traditional fraud masquerading as telehealth.”

Although the events of the “pernicious telefraud scheme” predate the current COVID-19 public health emergency, concerns about fraud have trailed the rapid expansion of telehealth during the pandemic as well as conversations about the future of telehealth in a post-pandemic world. For example, at a September 2020 meeting of the Medicare Payment Advisory Commission

---

(“MedPAC”), MedPAC members discussed how – and whether – to permanently expand telehealth as part of the Medicare program.[2] In her comments on the subject, Sue Thompson, Chief Executive Officer at UnityPoint Health and MedPAC member, remarked that there are “three core risks in the chapter around telehealth,” with the third risk being the risk of “large-scale fraud.”[3]

In response to concerns about fraud within the telehealth industry, telehealth companies and professional associations such as the American Telemedicine Association have focused on the critical need to, “differentiate between telehealth providers and fraudulent outfits as the latter can threaten public confidence in new technologies and care models that benefit growing numbers of patients and providers.”[4] This sentiment was most recently echoed in a [February 9, 2021 letter](#) from Krista Drobac, Executive Director of the Alliance for Connected Care (the “ACC”), to Christi Grimm, Principal Deputy Inspector General, U.S. Department of Health and Human Services Office of Inspector General (the “OIG”). According to Ms. Drobac, terms such as “telefraud” and other rhetorical flourishes as used by the DOJ and the OIG are misleading and disrespectful. Moreover, their use may eventually undermine the ongoing use of telehealth platforms to provide increased access to care for seniors who may be homebound or have limited access to providers.

On February 26, 2021, shortly on the heels of DOJ Press Release and seemingly in an effort to strike a balance between the need to continue fraud enforcement efforts in the telehealth industry while responding to industry concerns that the benefits of telehealth were possibly getting overshadowed by OIG and DOJ enforcement actions, Ms. Grimm released an [open letter](#) (the “Open Letter”) to both (i) affirm the OIG’s belief in the utility and value of virtual care, telehealth, and other digital health technologies, as a means to address the myriad challenges of the COVID-19 public health emergency; and (ii) announce that the “OIG is conducting significant oversight work assessing telehealth services during the public health emergency” in order to inform policy makers and other stakeholders. While hinting that some of the federal regulatory flexibilities granted to telehealth providers during the public health emergency may be here to stay, Ms. Grimm re-affirmed the OIG’s commitment to curbing fraud, waste, and abuse in the telehealth industry – a commitment recently evidenced by the OIG’s Work Plan updates relating to telehealth services provided by [Home Health Agencies](#) and [Medicare Part B](#) providers generally. Finally, assuaging industry concerns, Ms. Grimm used the Open Letter to distinguish between two types of fraudulent telehealth schemes: (1) telefraud, i.e., fraud involving sham remote visits, and (2) traditional fraud involving telehealth, i.e., fraudulent billing for other items or services (e.g., DME or genetic tests) made in connection with telehealth visits.

In light of the continuing oversight and enforcement activity by the DOJ, the OIG and other government agencies, healthcare providers who utilize telehealth platforms in the provision of care to Medicare and other federal healthcare program beneficiaries are well advised to take a fresh look at their telehealth operations. By focusing internal compliance efforts on telehealth activities – including the conduct of internal audits focused on the mitigation of traditional fraud, waste, and abuse risks – providers may be better positioned to successfully answer telehealth compliance questions raised in the context of external audits.

## FOOTNOTES

[1] Special Agent in Charge, Omar Pérez Aybar, U.S. Department of Health and Human Services Office of Inspector General, as quoted in the DOJ Press Release.

[2] [“MedPAC members weigh future of telehealth coverage,”](#) by Kat Jercich, Healthcare IT News (September 9, 2020)

[3] *Id.*

[4] Ann Mond Johnson, Chief Executive Officer, the American Telemedicine Association, “[ATA Comments on National Health Care Fraud and Opioid Takedown and International Telemarketing Scammers](#)” (October 2, 2020)

Copyright © 2024, Sheppard Mullin Richter & Hampton LLP.

---

National Law Review, Volumess XI, Number 69

Source URL: <https://natlawreview.com/article/oig-warns-telehealth-industry-great-power-comes-great-responsibility>