COSMOS
Navigate the Compliance Universe

Compliance Today - July 2021
Increasing OIG and DOJ telehealth fraud enforcement likely on horizon

By Michael Podberesky, Esq.; Andrea Lee Linna, Esq.; and Amanda Ray, Esq.

Michael Podberesky (mpodberesky@mcguirewoods.com) is a Partner in the Washington, DC, office; **Andrea Lee Linna** (alinna@mcguirewoods.com) is a Partner in the Chicago office; and **Amanda Ray** (aray@mcguirewoods.com) is an Associate in the Chicago office of the McGuireWoods LLP law firm.

- linkedin.com/in/michael-podberesky-0193493/
- linkedin.com/in/andrealeelinna/
- linkedin.com/in/amanda-ray-10338b89/

Approximately one year after the Centers for Medicare & Medicaid Services (CMS) modified telemedicine requirements to expand telehealth access during the COVID-19 public health emergency (PHE), recent Department of Health & Human Services (HHS) Office of Inspector General (OIG) statements and Department of Justice (DOJ) enforcement actions indicate that government scrutiny of telemedicine compliance is on the rise. These actions likely represent the tip of the iceberg of an ensuing wave of telehealth-focused audits and enforcement actions.

OIG focus on telehealth fraud

OIG has telegraphed its intent to focus on telehealth-related fraud. Notably, the OIG added Medicare Part B telehealth services audits to its Compliance Work Plan for January–March of 2021.[1] Moreover, on February 26, OIG's Principal Deputy Inspector General Christi Grimm commented in an open letter that while "OIG recognizes the promise that telehealth and other digital health technologies have for improving care coordination and health outcomes," it is critical to ensure "that new policies and technologies with potential to improve care and enhance convenience achieve these goals and are not compromised by fraud, abuse, or misuse."[2] To that end, Grimm stated that "OIG is conducting significant oversight work assessing telehealth services during the public health emergency," which she anticipates will be published later this year, and "will continue to vigilantly pursue…'telefraud' schemes and monitor the evolution of scams that may relate to telehealth."

Earlier this year, DOJ announced actions pertaining to two massive telehealth-related fraud schemes. In a news release issued February 4, DOJ described a telehealth fraud scheme involving dozens of durable medical equipment (DME) supply companies that submitted more than $400 million in illegal DME claims to Medicare and the Department of Veterans Affairs.[3] The defendants involved in the scheme bribed physicians to approve a high volume of telehealth claims when the physicians had no telehealth interaction with the beneficiaries. DOJ announced charges against 86 individuals involved in a similar fraud scheme involving telemedicine in a September 2020 news release, which it described as the "largest health care fraud and opioid enforcement action in Department of Justice history."[4] The defendant's telemedicine executives paid physicians to order unnecessary DME, genetic and diagnostic testing, and pain medications, causing an alleged $4.5 billion in false claims submitted to federal healthcare programs and private insurers by 86 criminal defendants in 19 judicial

districts. While these cases involve allegations of expansive and egregious fraud schemes, they represent low-hanging fruit and subsequent enforcement actions—both those initiated by the government as well as qui tam suits brought by whistleblowers under the False Claims Act—will likely target less apparent violations such as billing for missed appointments or submitting claims for sessions that are not as long or as complex as billed for.

Telefraud vs. noncompliance with Medicare telemedicine requirements

These recent actions by the OIG and DOJ, particularly the way they are categorized, have come under scrutiny by industry stakeholders who claim that the agencies' focus on telehealth fraud is not telehealth at all. The Alliance for Connected Care, an industry association representing telemedicine providers, has voiced concerns about the OIG's failure to distinguish blatant "telefraud" schemes, which focus on DME, compounding pharmacy, opioids, diagnostic tests, and other areas, from instances of inappropriate telehealth billing resulting from Medicare's temporary expansion of reimbursement of telehealth during the PHE, which is more likely to be representative of valid concerns about telehealth fraud.[5] The Alliance for Connected Care also rejected the notion that recent enforcement actions targeted instances of telehealth fraud. It stated the indicted actors did not, in essence, furnish care via telemedicine. While there appears to be a distinction between telefraud and noncompliance with Medicare telemedicine requirements, the OIG has not yet clarified its view whether such a categorical distinction exists. Regardless, it will be up to prosecutors and investigators evaluating allegations of telehealth-related misconduct, and ultimately judges and juries, to determine whether telehealth billing errors were the results of confusion and good faith efforts (and therefore not actionable under the False Claims Act or criminal laws) or reckless indifference, deliberate ignorance, or willful misconduct.

Post-pandemic reimbursement of telehealth

The concern that telehealth services are uniquely susceptible to fraud has been increasingly cited in expanding post-pandemic telehealth reimbursement discussions. The Medicare Payment Advisory Commission (MedPAC), a congressionally appointed advisory committee that makes recommendations to Congress, issued a March 15 report to Congress about permanently expanding post-pandemic telehealth reimbursement.[6] MedPAC expressed apprehension that expanding reimbursement for telehealth services after the pandemic "raises program integrity concerns." MedPAC claimed that "telehealth technology might make it easier to carry out fraud on a large scale because clinicians employed by fraudulent telehealth companies can interact with many beneficiaries from many parts of the country in a short amount of time." Also, MedPAC expressed concern that "if telehealth is expanded and beneficiaries become more comfortable receiving care through telehealth, they might become more vulnerable to being exploited by companies that pretend to be legitimate telehealth providers."

To limit the risks for telehealth fraud, MedPAC recommended that Congress implement the following safeguards if Congress decides to expand Medicare post-pandemic telehealth reimbursement permanently.

- Apply "additional scrutiny to outlier clinicians who bill many more telehealth services per beneficiary than other clinicians."
- Require clinicians to provide an in-person, face-to-face visit with a beneficiary before ordering expensive DME or expensive clinical laboratory tests.
- Prohibit "'incident to' billing for telehealth services provided by any clinician who can bill Medicare directly."

Implementing telehealth compliance best practices

In light of the OIG priorities and DOJ enforcement activities, as well as the regulatory complexity and existing gray areas, healthcare providers can take steps such as the following to decrease the risk of facing OIG or DOJ scrutiny of telemedicine claims. Each healthcare entity should tailor their telehealth compliance efforts to fit their organization and activities.

1. **Add telehealth to compliance work plan.** Evaluate the need to add OIG-focused telemedicine compliance audits to your company's compliance work plan. Review and add relevant items from the OIG Work Plan periodically and consider conducting external audits to ensure telemedicine claims are accurate and compliant. We recommend reviewing the OIG Work Plan monthly, as the OIG updates its Work Plan frequently.

2. **Implement robust auditing and monitoring**. Perform regular telemedicine auditing and monitoring to ensure that all coding and documentation requirements are satisfied. Monitor claims for potential telehealth issues such as upcoding, billing for canceled appointments, and billing for services not eligible for telehealth reimbursement. Lastly, consider updating existing compliance programs to address newly developed or expanded telehealth programs.

3. **Audits should consider PHE telehealth flexibilities.** Audit compliance with the temporary telehealth flexibilities enacted during the PHE and ensure plans are in place to revert to pre-PHE or new telehealth requirements as necessary. This could include:

    a. Ensuring PHE telehealth programs comply with the Health Insurance Portability and Accountability Act (HIPAA) and other relevant data privacy and security laws. During the PHE, the Office for Civil Rights announced it would exercise enforcement discretion and not impose penalties for noncompliance with the HIPAA rules against covered healthcare providers in connection with the good faith provision of telehealth during the PHE.[7] It is unlikely this enforcement discretion will continue after the PHE, so healthcare providers must ensure their new telehealth programs comply with the HIPAA rules, such as ensuring telehealth platforms meet HIPAA security requirements and business associate agreements are in place with telehealth vendors.

    b. Ensuring telehealth providers are complying with state licensure requirements. During the PHE, most states moved to waive or streamline licensure requirements to allow providers from other states to deliver care to residents of the state. Many states have begun to roll back licensure waivers and now require providers to be licensed in the state where the patient is located. Providers should consistently monitor for state law changes.

    c. Ensuring providers are appropriately prescribing controlled substances over telehealth. During the PHE, the Drug Enforcement Administration (DEA) worked with HHS to allow DEA-registered practitioners to use telemedicine to issue prescriptions for controlled substances to patients outside of a hospital or clinical setting.[8] Providers should begin to prepare if these policies are not in place after the PHE.

4. **Review telehealth claims across all payers.** Look beyond Medicare and analyze compliance with Medicaid and private insurance telehealth requirements.

5. **Assess arrangements affecting fair market value.** Review practices of providing free or below-fair-market-value telehealth equipment to physicians and patients.

6. **Identify and mitigate high-risk practices**. Review telehealth practices for high-risk practices, such as cold-calling patients to bill for telehealth services or requiring no or brief interactions between a telehealth

provider and a patient before billing for services, which could be construed as insufficient to create a patient–provider relationship.

7. **Monitor DME and lab billing.** Review all telehealth billing for DME and costly lab services, a focus of many of the recent telehealth enforcement actions.
8. **Track regulatory changes**. Track the latest regulatory guidance from federal and state sources (e.g., HHS, CMS, OIG, and state regulatory bodies) for changes in telemedicine regulatory or compliance requirements.
9. **Continue telehealth compliance education and training**. Provide and track the completion of telemedicine compliance training and education furnished to clinical and nonclinical staff.
10. **Monitor litigation risks**. Monitor telehealth programs for risk of qui tam suits, such as recent employee or former employee complaints about telehealth practices.
11. **Report overpayments**. If potential telemedicine compliance billing errors are found, confer with legal counsel to assess the scope of an appropriate inquiry and determine whether an overpayment adjustment or other type of self-report should be made.

Takeaways

- The Office of Inspector General auditing efforts are likely to pick up speed as the course of telehealth use continues to remain active among the provider community.
- The Department of Justice enforcement actions will likely continue against telehealth fraud where the Office of Inspector General has not differentiated telehealth billing errors.
- If Congress permanently expands telehealth reimbursement after the pandemic, healthcare providers should expect continued audit scrutiny.
- Regularly assess auditing and monitoring efforts over telehealth programs and implement best practices.
- Monitor telehealth fraud and enforcement actions and forthcoming regulations to adapt telehealth programs to the regulatory enforcement landscape.

1 "Work Plan Archives," HHS OIG, accessed May 14, 2021, https://bit.ly/3bwN54h.
2 Christi A. Grimm, "Principal Deputy Inspector General Grimm on Telehealth," HHS OIG, February 26, 2021, https://bit.ly/3hKpHV1.
3 DOJ, "Florida Businesswoman Pleads Guilty to Criminal Health Care and Tax Fraud Charges and Agrees to $20.3 Million Civil False Claims Act Settlement," news release, February 4, 2021, https://bit.ly/3hEvI5c.
4 DOJ, U.S. Attorney's Office for the Eastern District of Texas, "Largest Health Care Fraud and Opioid Enforcement Action in Department of Justice History Results in Charges Against 345 Defendants Responsible for More than $6 Billion in Alleged Fraud Losses," news release, September 30, 2020, https://bit.ly/3eUW9Cg.
5 Krista Drobac, "Alliance for Connected Care Letter to Principal Deputy Inspector General Christi Grimm," February 9, 2021, https://bit.ly/3yi0wio.
6 MedPAC, "Chapter 14: Telehealth in Medicare after the coronavirus public health emergency," *Report to the Congress: Medicare Payment Policy*, March 2021, https://bit.ly/3tOYDWZ.
7 "Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency," Office of Civil Rights, HHS, last reviewed January 20, 2021, http://bit.ly/3danGfP.

8 "Prescribing controlled substances via telehealth," Policy changes during COVID-19, Health Resources & Services Administration, last updated January 28, 2021, https://bit.ly/3u7JCQb.