LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What To Watch In Telehealth Enforcement

By **Kate Driscoll and Logan Wren** (October 21, 2021, 6:23 PM EDT)

Kate Driscoll

Logan Wren

Telehealth surged in 2020 to swiftly meet the exigencies of the COVID-19 public health emergency and is poised to remain a permanent fixture in our health care system.[1]

Telehealth now accounts for nearly 17% of all office and outpatient visits — 38 times higher than pre-COVID-19 averages — and is projected to become a $250 billion industry.[2] This rapid expansion of telehealth to ensure access to quality care during the public health emergency has altered consumer perceptions and expectations, transformed the regulatory landscape, and reinvigorated investment in telehealth.[3]

The precipitous rise of telehealth services has also opened the door to new and adapted forms of fraud, which has led to increased scrutiny and coordinated legal efforts and enforcement actions by the U.S. Department of Justice, the U.S. Department of Health and Human Services' Office of Inspector General, and the Centers for Medicare and Medicaid Services.

This article identifies telehealth fraud enforcement trends and provides recommendations on how telehealth providers can mitigate their risk and keep pace with the ever-changing regulatory and enforcement environment.

Telehealth Enforcement Trends During COVID-19

Telehealth fraud enforcement actions during the public health emergency reveal that the DOJ will prosecute a wide spectrum of targets across various jurisdictions: from telehealth companies, laboratories and pharmacies to executives and individual practitioners.

The alleged fraud loss stemming from telehealth fraud schemes during the public health emergency has been staggering. Based on the DOJ's major enforcement actions during the public health emergency, three major telehealth enforcement trends have emerged.

Kickback Schemes

Kickback schemes involving telehealth companies have been ripe for enforcement during the public health emergency.

The typical kickback scheme unfolds as follows:

- A telehealth company solicits illegal kickbacks and bribes from durable medical equipment supplier, pharmacy or laboratory in exchange for ordering unnecessary durable medical equipment, testing and medications.

- The telehealth company pays physicians to write medically unnecessary orders for these items.

- A durable medical equipment supplier, laboratory or pharmacy fills the orders, and in some cases, never even fills the order, in exchange for kickbacks to the telehealth company and submits the claim to a government health insurer for reimbursement.

The DOJ's focus on kickbacks is evidenced in the recent September takedown of more than 40 defendants across 11 judicial districts, alleging $1.1 billion in false and fraudulent claims submitted to government health insurers stemming from telemedicine schemes.

The indictment alleges that telemedicine executives paid doctors and other health personnel to order unnecessary durable medical equipment, diagnostic testing and pain medications, with either no patient interaction or only a brief telephone call with a patient they had never seen before.[4]

It is alleged that durable medical equipment companies, laboratories and pharmacies then purchased those orders in exchange for kickbacks and bribes — ultimately submitting more than $1 billion in fraudulent claims to government insurers.[5]

This takedown was led by the Fraud Section's National Rapid Response Strike Force, which was created during the public health emergency, in part, to coordinate large-scale, complex telemedicine fraud prosecutions across various districts nationwide — a clear indicator that combating telehealth fraud is a top priority for the DOJ.

In another complex case, a telehealth company owned by Creaghan Harry created shell companies opened in the names of straw owners in the U.S. and foreign countries in an effort to evade law enforcement.[6] It is alleged that the kickbacks were funneled into the shell companies and then transferred into the telemedicine company's account to pay the physicians to write the unnecessary orders.[7]

Fraudulent Billing Tactics

Submission of claims for services or supplies that were never provided or for so-called phantom patients that never existed has been the target of recent enforcement actions during the public health emergency.

For example, in May 2021, the DOJ brought criminal charges against defendants who, in an effort to exploit CMS' relaxed Medicare reimbursement of telemedicine health services during the public health emergency, allegedly submitted false and fraudulent claims to Medicare for sham telemedicine encounters that never occurred.[8] This takedown was also led by the Fraud Section's National Rapid Response Strike Force.

Other billing issues likely to be scrutinized by the DOJ and subject to upcoming enforcement actions

against telehealth providers include improper coding, such as upcoding for higher reimbursement requests,[9] exaggerating the time spent delivering telemedicine services, or misrepresenting the type of virtual service provided (e.g., Medicare telehealth visits, virtual check-ins for established patients, and e-visits via online patient portal).[10] [11]

Ordering Medically Unnecessary Services

Billing for unnecessary services is another trend of DOJ telehealth fraud enforcement actions during the public health emergency, including medically unnecessary diagnostic tests, medications, orthotic braces and other durable medical equipment.[12]

In some cases, COVID-19 testing claims were bundled with Medicare claims for additional, more expensive laboratory tests, such as medically unnecessary cancer genetic screenings, respiratory pathogen panel testing and allergy tests.[13]

In other cases, the telemedicine doctors did not meet with, or only had cursory conversations with, the patients before prescribing these costly tests or durable medical equipment, which were ultimately reimbursed by federal health insurers.[14]

For example, in September 2020, the DOJ, with assistance from HHS-OIG, charged more than 86 defendants in 19 judicial districts, including telemedicine executives, durable medical equipment companies, genetic testing laboratories, pharmacies and individual doctors.

The indictment alleged a $4.5 billion fraud scheme that lured hundreds of thousands of unsuspecting victims into receiving medical services, testing and devices they did not actually need.[15] This takedown was also led by the Fraud Section's National Rapid Response Strike Force.

In addition to the criminal action, CMS took separate administrative action and — in a record-breaking regulatory enforcement action in telemedicine fraud — revoked the Medicare billing privileges of hundreds of medical professionals for their involvement.[16]

The DOJ has also used the False Claims Act as an enforcement tool to combat telehealth fraud, specifically the ordering of medically unnecessary DME and diagnostic testing.

For example, in January, Kelly Wolfe, the operator of a durable medical equipment billing and consulting company agreed to pay the government more than $20 million to resolve FCA violations as part of a criminal and civil resolution for a scheme involving various durable medical equipment supply companies that submitted thousands of false durable medical equipment claims to Medicare for medically unnecessary durable medical equipment supplies, including orthotic braces, which were generated through unlawful kickbacks to telemedicine companies and doctors.[17]

In August, the DOJ charged Richard Laksonen, Hugh Deery II, Colleen Browne and Mosab Deen, medical practitioners who signed off on fraudulent orders for medically unnecessary braces and cancer genetic testing promoted by telemarketers, ultimately resulting in both civil and criminal outcomes, including civil FCA settlements (ranging from $28,000 to $300,000) and criminal guilty pleas to making false statements relating to health care.[18]

Mitigating Telehealth Fraud Risk

Given the rapid expansion of telehealth, which is expected to remain permanently embedded in our health care system, telehealth providers must take advantage of all available safeguards to mitigate the risk of fraud. There are several ways telehealth providers can proactively mitigate their risk of running afoul of fraud in a time of increasing government civil and criminal enforcement:

Instituting a Robust Compliance Program

At a minimum, telehealth providers need a robust compliance plan that is routinely audited to keep pace with the dynamic regulatory landscape.

In June 2020, the DOJ published guidance on the evaluation of corporate compliance programs, which should serve as a guide to providers when building or evaluating a compliance program.[19]

Resources from other relevant government agencies, including CMS[20] and HHS,[21] should be reviewed, and compliance programs should be updated accordingly. Special attention should be paid to services that cross state lines as states have varied rules regarding limitations and requirements to prescribe drugs and durable medical equipment via telemedicine; licensure requirements; fee-splitting limitations; and restrictions on the corporate practice of medicine.[22]

A deep dive into marketing strategies and materials as well as telehealth relationships with third parties should be conducted to mitigate potential kickback issues. The compliance program should detail how telehealth services comply with the Health Insurance Portability and Accountability Act and other data privacy and security laws.

Telehealth providers should review all billing and coding practices to confirm parity with current regulatory guidance. Ensuring that your organization has clean internal channels to report compliance concerns, as well as a trained investigative team to review potential violations, is critical to detecting risk early on and should be a central component of the compliance program.[23]

Data and Qualitative Analytics

The DOJ relies on data analytics to identify irregularities and potential fraud.[24] Integrating data and qualitative research will allow telehealth providers to quickly detect and prevent fraud by monitoring outliers and tracking long-term billing trends of medical practitioners.[25]

If an outlier is detected, such as a physician who bills considerably more telehealth services than others, additional scrutiny should be applied.

This additional review can include analysis of the outlier-physician's medical records to ensure the existence of a sufficient doctor-patient relationship, that expensive durable medical equipment or laboratory testing ordered appears medically necessary, and that the services rendered are consistent with those billed to the federal health insurer.[26]

Frequent Compliance Training

Telehealth's regulatory landscape has undergone tremendous change during the public health emergency and remains in flux. All clinicians and staff should receive routine mandatory compliance training, including training on how to properly code and bill for telemedicine services that are submitted to government health insurers for reimbursement. Telehealth providers should track the completion of

these trainings to ensure compliance.

Require In-Person Visits for Expensive Testing and Durable Medical Equipment

In a telehealth setting, it is easier to engage in fraud on a large scale because a physician can speak to many patients in various locations in a much shorter period of time than in-person visits.[27]

This has been particularly problematic with respect to the purchase of expensive, medically unnecessary durable medical equipment and laboratory testing. The recent enforcement actions allege billions of fraud loss in this category.

Requiring physicians to provide in-person visits with a patient before ordering expensive durable medical equipment or laboratory testing is a safeguard that can decrease the likelihood of fraud.[28]

While requiring an in-person visit may be less convenient for the patient and the physician, on balance, it will allow the doctor to conduct a more thorough needs assessment and diminish the incidence of fraud.[29] At a minimum, telehealth providers should monitor telehealth billing for durable medical equipment and expensive diagnostic testing to detect any irregularities.

Conclusion

Telehealth surged in response to the public health emergency and is slated to remain a permanent fixture in health care.

The enforcement actions during the public health emergency serve as a bellwether of increased government scrutiny in the area of telehealth fraud for years to come. Telehealth providers, suppliers and related entities must stay abreast of changing regulations and remain focused on developments in government enforcement to inform their risk mitigation efforts.

The strategies above are necessary first steps to reduce the incidence of fraud in the wake of increasing enforcement actions, but companies must remain vigilant and nimble to keep pace with telehealth's dynamic and evolving landscape.

Kate Driscoll is of counsel and Logan Wren is an associate at Morrison & Foerster LLP.

[1] Oleg Bestsennyy et al., "Telehealth: A Quarter-Trillion-Dollar Post-COVID-19 Reality?" McKinsey & Company (July 9, 2021), https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality.

[2] Id.

[3] See id.

[4] Press Release, "National Health Care Fraud Enforcement Action Results in Charges Involving Over

$1.4 Billion in Alleged Losses," DOJ (Sept. 17, 2021), https://www.justice.gov/opa/pr/national-health-care-fraud-enforcement-action-results-charges-involving-over-14-billion.

[5] Id.

[6] Press Release, "Telemedicine Company Owner Charged in Superseding Indictment for $784 Million Health Care Fraud, Illegal Kickback and Tax Evasion Scheme," DOJ (Aug. 10, 2021), https://www.justice.gov/opa/pr/telemedicine-company-owner-charged-superseding-indictment-784-million-health-care-fraud.

[7] Bill Wichert, "Telehealth Exec Hit with New Charges in $784M Fraud Case," Law360 (Aug. 11, 2021), https://www.law360.com/articles/1411650/telehealth-exec-hit-with-new-charges-in-784m-fraud-case.

[8] Press Release, "DOJ Announces Coordinated Law Enforcement Action to Combat Health Care Fraud Related to COVID-19," DOJ (May 26, 2021), https://www.justice.gov/opa/pr/doj-announces-coordinated-law-enforcement-action-combat-health-care-fraud-related-covid-19.

[9] See Paul Giancola and Claudia Stedman, "Telehealth Fraud Triggered by COVID-19 Pandemic," JD Supra (Feb.16, 2021), https://www.jdsupra.com/legalnews/telehealth-fraud-triggered-by-covid-19-8657616/.

[10] The types of virtual services have different requirements and billing codes. See "Medicare Telemedicine Health Care Provider Fact Sheet," CMS (Mar. 17, 2020), https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet.

[11] See Centers for Medicare & Medicaid Services, "Medicare Fraud & Abuse: Prevent, Detect, Report" (January2021), https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Fraud-Abuse-MLN4649244.pdf (describing strategies to prevent different forms of Medicare fraud, including common billing issues).

[12] "2020 National Health Care Fraud and Opioid Takedown: Case Descriptions," DOJ, https://www.justice.gov/criminal-fraud/hcf-2020-takedown/case-descriptions.

[13] Press Release, "DOJ Announces Coordinated Law Enforcement Action to Combat Health Care Fraud Related to COVID-19," DOJ (May 26, 2021), https://www.justice.gov/opa/pr/doj-announces-coordinated-law-enforcement-action-combat-health-care-fraud-related-covid-19.

[14] See id.

[15] "2020 National Health Care Fraud Takedown," HHS-OIG, https://oig.hhs.gov/newsroom/media-materials/2020takedown/; "2020 National Health Care Fraud Takedown Factsheet," HHS-OIG, https://oig.hhs.gov/documents/root/230/2020HealthCareTakedown_FactSheet_9dtIhW4.pdf.

[16] Press Release, "National Health Care Fraud and Opioid Takedown Results in Charges Against 345 Defendants Responsible for More Than $6 Billion in Alleged Fraud Loss," DOJ (Sept. 30, 2020), https://www.justice.gov/opa/pr/national-health-care-fraud-and-opioid-takedown-results-charges-against-345-defendants.

[17] Settlement Agreement of January 2021, United States and the State of Florida ex rel. Albright v. Regency, Inc. et al., No. 8:19-cv-686-T-30AEP (M.D. Fla. filed Mar. 20, 2019), https://www.justice.gov/opa/press-release/file/1364736/download; see also Press Release, "Florida Businesswoman Pleads Guilty to Criminal Health Care and Tax Fraud Charges and Agrees to $20.3 Million Civil False Claims Act Settlement," DOJ (Feb. 4, 2021), https://www.justice.gov/opa/pr/florida-businesswoman-pleads-guilty-criminal-health-care-and-tax-fraud-charges-and-agrees-203.

[18] Press Release, "U.S. Attorney Announces Criminal and Civil Enforcement Actions Against Medical Practitioners for Roles in Telemedicine Fraud Schemes," DOJ (Aug. 24, 2021), https://www.justice.gov/usao-wdmi/pr/2021_0824_Happy_Clickers.

[19] U.S. Department of Justice, Evaluation of Corporate Compliance Programs (June 2020), https://www.justice.gov/criminal-fraud/page/file/937501/download.

[20] "Coronavirus (COVID-19) Partner Resources," CMS, https://www.cms.gov/outreach-education/partner-resources/coronavirus-covid-19-partner-resources.

[21] "Telehealth: Health Care from the Safety of Our Homes," HHS, https://www.telehealth.hhs.gov/.

[22] See American Health Law Association, "Enforcement 2020: Telehealth Providers Move to the Top of OIG's Watch List," at 3 (Dec. 16, 2020), https://www.buchalter.com/wp-content/uploads/2020/12/AHLA_Bulletin_HIT_Robbins_Brendel_12-16-20.pdf; Stephen D. Bittinger et al., "Qui Tam Quarterly: Hunting Telehealth Fraud Under COVID-19 Waivers and Expansion," National Law Review (Aug.27, 2021), https://www.natlawreview.com/article/qui-tam-quarterly-hunting-telehealth-fraud-under-covid-19-waivers-and-expansion.

[23] For the risks of whistleblowing in the telemedicine context, see Tycko & Zavareei Whistleblower Practice Group, "The United States Department of Justice Scores Another Victory Exposing Telemedicine Fraud in an Ongoing Mission to Protect the Integrity of Healthcare Programs and Save Taxpayers Billions," National Law Review (Apr.27, 2021), https://www.natlawreview.com/article/united-states-department-justice-scores-another-victory-exposing-telemedicine-fraud; Phillips & Cohen, "Telemedicine Fraud: How Whistleblowers Can Report It and Get Rewarded," https://www.phillipsandcohen.com/whistleblower-resources/telemedicine-fraud-how-whistleblowers-can-report-it-and-get-rewarded/.

[24] See American Health Law Association, "Enforcement 2020: Telehealth Providers Move to the Top of OIG's Watch List," at 3 (Dec. 16, 2020), https://www.buchalter.com/wp-content/uploads/2020/12/AHLA_Bulletin_HIT_Robbins_Brendel_12-16-20.pdf.

[25] Gary Call, "Provider Strategies for Mitigating Telehealth Fraud & Abuse in 2021," HIT Consultant (Jan.14,2021), https://hitconsultant.net/2021/01/14/strategies-mitigating-telehealth-fraud-abuse-2021/#.YVt-SprMJyw.

[26] See Medicare Payment Advisory Commission, "Report to the Congress, Medicare Payment Policy," at xxvii (Mar. 2021), http://www.medpac.gov/docs/default-source/default-document-library/mar21_medpac_report_to_the_congress_secv2.pdf?sfvrsn=0.

[27] See id.

[28] See id.

[29] See id.