K&L GATES

QUI TAM QUARTERLY

HUNTING TELEHEALTH FRAUD UNDER COVID-19 WAIVERS AND EXPANSION

By: Stephen D. Bittinger, Kim H. Looney, and Nora E. Becerra

Over the COVID-19 pandemic, telehealth has evolved from an infrequent method of providing health care services that was often abused into a vital tool used by providers to connect with patients. This article examines fraudulent uses of telehealth, government agency uses of claims analysis and data analytics in telehealth fraud investigations, and government agency technological advancements in this regard. This article also provides recommendations on how to minimize risk of involvement in improper telehealth arrangements.

COVID-19 Telehealth Expansion Created Opportunities for Fraud

Prior to the advent of the COVID-19 pandemic and subsequent public health emergency (PHE), telehealth services were limited in both the amount of reimbursement and the location for which telehealth services could be reimbursed. During the pandemic, those requirements have been significantly relaxed, and some regulations have even been temporarily waived. For example, one of the first actions the Centers for Medicare and Medicaid Services (CMS) took pursuant to the emergency declaration by President Trump on 13 March 2020, under the Stafford Act and the National Emergencies Act, was to expand Medicare telehealth benefits to allow all beneficiaries to receive telehealth in any location, including their homes.[1] This relaxed regulatory environment, along with the financial stimulus provided by Congress through the CARES Act, has led to an explosion in the provision of telehealth services. The number of telehealth visits increased from about 10,000 per week to 300,000 per week in late March of 2020, according to CMS.[2]

While telehealth services will certainly never fully replace in-person care, they were proven during the PHE to be a reliable and convenient additional access point for patients. Therefore, certain changes made during the PHE to facilitate their use are likely here to stay. CMS is in the process of reviewing the temporary changes made to telehealth in order to determine which of these changes should be permanent and whether they require regulatory action.[3] Some factors under consideration include whether or not the mode of delivery is clinically safe and appropriate for patients, what the payment rates for telehealth services should be, and how to protect beneficiaries and taxpayer dollars from unscrupulous actors.[4]

With an increase in the usage of telehealth services, the Department of Justice (DOJ), the Office of Inspector General for the Department of Health and Human Services (HHS-OIG), and CMS have increased scrutiny of these services. These agencies are focused within the confines of their respective authority on how to combat fraud and abuse and maintain governmental reimbursement program integrity. Fraud and abuse can—and has—taken a variety

of different forms, including false claims from inaccurate billing and coding to complex kickback schemes. In recent years, government enforcement agencies have been able to significantly increase their capability to coordinate legal efforts to stop fraud and abuse across multiple agencies in multiple jurisdictions due to advances in claims analysis and data analytics. These technological advances allow the government to identify potentially improper conduct by isolating claims billing patterns across multiple parties.

After exploring compliance and coding issues related to telehealth through the lens of recent government investigations and enforcement actions, this article will offer a discussion of best practices for providers and suppliers attempting to compliantly navigate the sea change of telehealth implementation. These recommendations will assist with identifying potential traps and pitfalls in the provision of telehealth services in today's regulatory environment.

Understanding the Compliance, Coding, and Data Analytics Behind Telehealth Fraud Investigations

Long before the DOJ announces a major health care fraud operation, an analysis of claims data intended to detect anomalies and variances is used to identify potentially fraudulent patterns and targets. By examining how suspect telehealth services are identified by government investigators,[5] suppliers and providers may themselves be in a better position to identify improper telehealth arrangements.

Although there are significant technical differences in identifying the coding and compliance issues relating to telehealth for various types of providers and suppliers, a central issue is common: ensuring that documentation and claims data reflects an actual patient-physician relationship and the related course of treatment.

Telehealth and DMEPOS Suppliers

Examining pre-pandemic enforcement actions such as Operation Brace Yourself,[6] where the crux of the illegal conduct surrounded improper telehealth arrangements, the question becomes how the government will use data analysis to investigate for potential fraud in light of the dramatic increase in telehealth services, particularly in arenas where such services were previously rare. Prior to the PHE, patients that had no prior clinical relationship with a prescribing telemedicine physician was a highly unusual circumstance and more easily identifiable as an anomalous claims pattern.[7] Government agencies could use Medicare regulations prior to the PHE that required an ordering physician to have a face-to-face examination with a patient in order to prescribe durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) (i.e., the provider billed the appropriate Evaluation and Management (E/M) code) to find outliers.[8] Then, the supplier received the written order from the ordering physician, fulfilled the order, and billed for the supply.[9] Government data miners were able to examine the unusually high volume of braces being dispensed and quickly focused their attention on a specific group of potential targets, such as beneficiaries who did not have an E/M code billed by a physician within the prescribing time prior to the distribution of the supply. While the government also relied on whistleblowers and patient complaints, data analysis allowed the government to isolate potentially fraudulent claims across a wide number of suppliers.[10]

This raises the question as to how the government will pivot to investigate claims under regulatory waivers implemented during the pandemic that dramatically changed the requirements of DMEPOS suppliers and opened the door for telemedicine to serve as both a vital resource during uncertain times as well as a catalyst for potential for fraud.

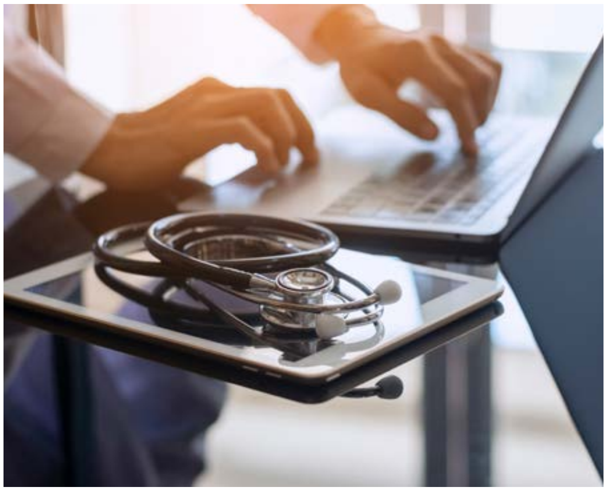
In March 2020, CMS published an Interim Final Rule[11] holding that, to the extent a national coverage determination or local coverage determination and guidance articles would require a face-to-face or in-person encounter for issuance of DMEPOS, such requirements would not apply during the PHE. This rule did not alter face-to-face requirements mandated by statute for program integrity purposes for equipment such as power mobility devices.[12] Regulatory flexibility allowed most supply types to be legally ordered through telehealth.[13] Under this current regulatory framework, the government will need to re-center its focus beyond whether an E/M was billed prior to prescribing to whether the claims data can establish a patient-physician relationship via telemedicine. For suppliers, the False Claims Act (FCA) risk becomes an analysis of whether or not the supplier is able to demonstrate the validity of the patient-physician relationship based on telemedicine documentation provided to support the medical necessity of the order for the supply.

Telehealth and Medical Reference Laboratories

In another pre-pandemic enforcement action, the government was able to identify patterns of improper claims in Operation Double Helix by the absence of an encounter with a physician or an encounter with an out-of-state telehealth provider.[14] In this action, the focus of the government was on prescribing genetic testing either without any patient interaction or with only a brief telephonic conversation with patients they had never met or seen. The lack of historical evidence of a physician-patient relationship was asserted by the government as a strong indicator of fraud. In addition, because the specific cancer-screening genetic test was only covered for patients with an active diagnosis of cancer to aid an oncologist in treatment, the government could also determine potentially fraudulent claims by the absence of clinically related claims in the patients' histories. Many laboratories that were unaware of the origin of the sham telemedicine claims processed and billed for these improper claims due to inadequate compliance and procedures to identify valid from invalid telehealth services. Under the expanding use of telehealth after the pandemic, the government would still be able to use a patient's individual treatment history to isolate potentially improper claims, but a far more robust analysis will be required to determine the propriety of the patient-physician relationship where patients are more likely to have isolated treatment episodes with a physician they may be seeing for the first time.

After the PHE, laboratories must effectively address how to identify and manage the expanding arena of telehealth concerns to avoid such enforcement actions. For example, there have been many compliance concerns surrounding specimen collection and travel allowances based on a telemedicine visit. CMS considers beneficiaries to be "confined to the home" or "homebound" if it is medically contraindicated for the patient to leave the home. During the PHE, a beneficiary could be considered "homebound" if: (1) a physician has determined that it is medically contraindicated for a beneficiary to leave the home because he or she has a confirmed or suspected diagnosis of COVID-19, or (2) where a physician has determined that it is medically contraindicated for a beneficiary to leave the home because the patient has a condition that may make the patient more susceptible to contracting COVID-19. However, post-PHE, Medicare will only allow payment for a specimen collection fee when it is medically necessary for a laboratory technician to draw a specimen from either a nursing home patient or homebound patient.[15] This raises the question as to the whether there will be a corresponding increase in telemedicine visits that include a homebound determination to allow patients and laboratories the continued ease of treatment that may draw government scrutiny.

While lapses in compliance to these regulatory changes may not rise to the level of fraudulent intent, implementing adjustments now will help to mitigate risk moving forward, given the increased use of technology and data mining by the government. Laboratories will need to develop a strong understanding of compliant documentation of appropriate telemedicine services used to support orders to guard against the risk of FCA liability for submitting claims for tests where a legitimate patient-physician relationship does not exist.



Innovative Technology and Its Impact on Compliance Measures

Federal government resources have been in place for almost a decade to set the foundation for utilizing data analytics in large-scale, coordinated enforcements. The Medicare Fraud Strike Force, established under the HHS-OIG, and the DOJ's Health Care Fraud Strike Force were created in 2007 to harness data analytics through federal, state, and local resources. They have worked to prevent and combat health care fraud, waste, and abuse.[16] The strike forces focus on detecting billing anomalies, such as those described above, to identify emerging fraudulent schemes. The results have been widespread and dramatic, not only from the number of people criminally charged, but also from the number of providers, suppliers, and laboratories that have suffered civil and administrative consequences due to a failure to effectively identify improper arrangements and remove themselves.

Using prior enforcement actions as a road map to look ahead, there is a clear trend among government agencies, such as CMS, HHS-OIG, and DOJ, to implement technology and techniques for collecting and analyzing data. In his remarks at the Federal Bar Association's Qui Tam Conference, Acting Assistant Attorney General Brian M. Boynton described how the Civil Division of DOJ will continue to use data analytics as a vital tool to uncover fraud in Medicare data, stating:

> Our sophisticated data analytics allow us to identify patterns across different types of health care providers—giving us a way to identify trends and extreme outliers. We can see where the highest risk physicians are located in each state and federal district, and how much they are costing the Medicare program. The data can even allow us to demonstrate and quantify sophisticated relationships, such as a

> physician offering controlled substance prescriptions to a patient who is likely to divert them. Identifying these types of relationships can help us combat prescription drug abuse as well as many other types of health care fraud. Indeed, the Civil Division has been actively using its data analysis for this very purpose.[17]

The DOJ recently announced the establishment of the COVID-19 Fraud Enforcement Task Force, which is focused on harnessing government resources, including data analytics, to identify fraud in the midst of regulatory flexibilities implemented to combat the PHE. The task force is comprised of: (1) the Criminal and Civil Divisions of the DOJ, (2) the Executive Office for U.S. Attorneys, and (3) the Federal Bureau of Investigation.[18] Based on this announcement, we can expect that government agencies will continue to employ similar tactics used in prior investigations, and improper use of telehealth services will be high on their priority list. These investigations are imminent, and the DOJ has emphasized that it plans to use every tool at its disposal—including criminal, civil, and administrative measures—to identify fraud through shared "information and insights" across government agencies.[19] Some of the interagency partners identified are the Department of Labor, the Department of the Treasury, the Department of Homeland Security, the Small Business Administration, the Special Inspector General for Pandemic Relief, and the Pandemic Response Accountability Committee.[20]

Artificial intelligence (AI) will likely serve as the next major stepping stone in the advancement of data analytics technology. In January 2021, HHS released its strategy for implementing AI across its programs.[21] AI is described in the HHS strategy document as the process through which computer systems are developed to automate routine tasks normally requiring human intelligence, such as drawing data-based insights.[22] HHS identifies AI as "a critical enabler" of its missions in the future.[23]

CMS began exploring different methods for implementing AI into its arsenal for detecting fraud and monitoring health outcomes prior to the release of the HHS AI strategy. In 2019, CMS launched an AI Health Outcomes Challenge. The multistage challenge was purposed in determining ways in which AI could serve as a solution for predicting patient health outcomes for Medicare beneficiaries for potential use by the CMS Innovation Center.[24] The AI competition was the CMS Innovation Center's first prize competition, and the first initiative to focus on AI-driven solutions.[25] CMS highlighted that one major insight from the competition was discovering potential ways in which the CMS Innovation Center could utilize public-private partnerships in the future to generate innovative technological solutions for the Medicare program.[26]

Considering the HHS AI strategy and the focused efforts and resources CMS and other agencies have allocated to understand and implement technology into current programs, as well as HHS-OIG's and DOJ's commitment to honing data analytics and new technologies, AI and machine-learning technology is anticipated to be implemented in the near future as another way to harness data analytics in fraud and abuse compliance.

Best Practices to Minimize Risk

Telehealth providers and those who rely on the validity of a telemedicine visit to bill for a service or supply should be proactive and put compliance plans into place to mitigate the risk of violations and resulting enforcement sanctions. Administering services across state lines should be of particular concern, as state law could also add an additional layer of complexity. Licensure requirements, corporate practice of medicine, fee splitting, requirements for prescribing drugs and ordering DMEPOS, and supervision requirements for allied health professionals should be evaluated. When contracting to provide services across providers and entity types, additional consideration, including referral and anti-kickback issues, should be considered.

Resources are available directly from government agencies to assist providers and suppliers with compliance and include, but are not limited, to the following:

- CMS maintains resources for providers, which are available on its "Coronavirus (COVID-19) Partner Resources" website.[27] Resources specific to telehealth include: COVID-19 Frequently Asked Questions (FAQs) on Medicare Fee-for-Service (FFS) Billing[28] and Telehealth.hhs.gov.[29]
- HHS provides several resources for delivering telehealth safely during COVID-19 and billing appropriately for said services.[30]
- CMS maintains telemedicine resources, including a Medicaid & CHIP Telehealth Toolkit (which includes information on patient populations eligible for telehealth, coverage and reimbursement policies, and technology requirements[31]) and a HRSA Medicare Telehealth Payment Eligibility Analyzer,[32] among others.

Providers, suppliers, and laboratories should review available resources on a regular basis and update internal compliance programs to ensure they have a firm understanding of how to identify legitimate telemedicine services that billed, or used to support claims billed, to reduce risk of FCA liability.

Conclusion

It is clear that telehealth has made dramatic advances during the PHE, many of which will remain after the waivers. While telehealth adds tremendous value to health care services, it also carries high potential for abuse. Using prior investigations and enforcement actions as a guide, it is clear that telehealth services are—and will continue to be—a main focus as the government implements new data analysis techniques to identify and assess fraud and abuse in the administration of services in the industry.

K&L Gates' Health Care group routinely assists providers and suppliers on matters concerning government audits and fraud and abuse. Our team is well equipped to provide strategic advice as providers and suppliers navigate regulatory complexities applicable to their services under the evolving regulatory framework.

Endnotes

[1] Seema Verma, *Early Impact of CMS Expansion of Medicare Telehealth During COVID-19*, HEALTH AFFS. (July 15, 2020), https://www.healthaffairs.org/do/10.1377/hblog20200715.454789/full/.

[2] Editorial Board, *The Doctor Will Zoom You Now*, WALL ST. J. (Apr. 27, 2020), https://www.wsj.com/articles/the-doctor-will-zoom-you-now-11587935588.

[3] Verma, *supra* note 1.

[4] *Id.*

[5] News Release, Dep't of Just. Off. of Pub. Affs., Federal Indictments & Law Enforcement Actions in One of the Largest Health Care Fraud Schemes Involving Telemedicine and Durable Medical Equipment Marketing Executives Results in Charges Against 24 Individuals Responsible for Over $1.2 Billion in Loss (Apr. 9, 2019), https://www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes; News Release, Dep't of Just. Off. of Pub. Affs., Federal Law Enforcement Action Involving Fraudulent Genetic Testing Results in Charges Against 35 Individuals Responsible for Over $2.1 Billion in Losses in One of the Largest Health Care Fraud Schemes Ever Charged (Sept. 27, 2019), https://www.justice.gov/opa/pr/federal-law-enforcement-action-involving-fraudulent-genetic-testing-results-charges-against; News Release, Dep't of Just. Off. of Pub. Affs., DOJ Announces Coordinate Law Enforcement to Combat health Care Fraud Related to COVID-19 (May 26, 2021), https://www.justice.gov/opa/pr/doj-announces-coordinated-law-enforcement-action-combat-health-care-fraud-related-covid-19.

[6] Dep't of Just. Off. of Pub. Affs., *supra* note 5.

[7] *Id.*

[8] Ctrs. for Medicare & Medicaid Servs., Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) Order Requirements, https://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Medical-Review/Faceto-FaceEncounterRequirementforCertainDurableMedicalEquipment (last visited June 26, 2021).

[9] *Id.*

[10] Dep't of Just. Off. of Pub. Affs., *supra* note 5.

[11] CMS-1744-IFC (Mar. 13, 2020), https://www.cms.gov/files/document/covid-final-ifc.pdf.

[12] *Id.*

[13] Medicaid.gov, Telemedicine, https://www.medicaid.gov/medicaid/benefits/telemedicine/index.html (last visited June 26, 2021).

[14] News Release, Dep't of Just. Off. of Pub. Affs., Federal Law Enforcement Action Involving Fraudulent Genetic Testing Results in Charges Against 35 Individuals Responsible for Over $2.1 Billion in Losses in One of the Largest Health Care Fraud Schemes Ever Charged (Sept. 27, 2019), https://www.justice.gov/opa/pr/federal-law-enforcement-action-involving-fraudulent-genetic-testing-results-charges-against.

[15] Ctrs. for Medicare & Medicaid Servs., Internet-Only Manual, Pub. 100-04, Chapter 16, Section 60.1.2, https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/clm104c16.pdf.

[16] *See* Dep't of Health & Hum Servs., Off. of Inspector Gen, Medicare Fraud Strike Force, https://oig.hhs.gov/fraud/strike-force/ (last visited June 19, 2021); see also Dep't of Just., Strike Force Operations, https://www.justice.gov/criminal-fraud/strike-force-operations (last visited June 19, 2021).

[17] News Release, Dep't of Just. Off. of Pub. Affs., Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Federal Bar Association Qui Tam Conference (Feb. 17, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-federal-bar.

[18] News Release, Dep't of Just. Off. of Pub. Affs., Attorney General Announces Task Force to Combat COVID-19 Fraud (May 17, 2021), https://www.justice.gov/opa/pr/attorney-general-announces-task-force-combat-covid-19-fraud.

[19] *Id.*

[20] *Id.*

[21] U.S. Dep't of Health & Hum. Servs., Artificial Intelligence (AI) Strategy (Jan. 2021), https://www.hhs.gov/sites/default/files/final-hhs-ai-strategy.pdf.

[22] *Id.* at 2.

[23] *Id.*

[24] Press Release, Ctrs. for Medicare & Medicaid Servs., CMS Selects Winner and Runner-Up in Artificial Intelligence Health Outcomes Challenge (Apr. 30, 2021), https://www.cms.gov/newsroom/press-releases/cms-selects-winner-and-runner-artificial-intelligence-health-outcomes-challenge.

[25] Press Release, Ctrs. for Medicare & Medicaid Servs., Lessons Learned from the CMS Artificial Intelligence Health Outcomes Challenge (May 13, 2021), https://www.cms.gov/blog/lessons-learned-cms-artificial-intelligence-health-outcomes-challenge.

[26] *Id.*

[27] Ctrs. for Medicare & Medicaid Servs., Coronavirus (COVID-19) Partner Resources, https://www.cms.gov/outreach-education/partner-resources/coronavirus-covid-19-partner-resources (last visited June 26, 2021).

[28] Ctrs. for Medicare & Medicaid Servs., COVID-19 Frequently Asked Questions (FAQs) on Medicare Fee-for-Service (FFS) Billing (last updated Jan. 7, 2021) https://www.cms.gov/files/document/medicare-telehealth-frequently-asked-questions-faqs-31720.pdf.

[29] U.S. Dep't of Health & Hum. Servs., Telehealth: Health care from the safety of our homes, https://www.telehealth.hhs.gov/ (last visited June 26, 2021).

[30] U.S. Dep't of Health & Hum. Servs., Telehealth: Delivering Care Safely During COVID-19, https://www.hhs.gov/coronavirus/telehealth/index.html (last visited June 26, 2021); Getting Started With Telemedicine, https://telehealth.hhs.gov/providers/getting-started/ (last visited June 26, 2021); Telehealth Policy Changes During Covid-19, https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/ (last visited June 26, 2021); Billing For Telehealth During Covid-19, https://telehealth.hhs.gov/providers/billing-and-reimbursement/ (last visited June 26, 2021).

[31] Ctrs. for Medicare & Medicaid Servs., CMS Medicaid & CHIP Telehealth Toolkit, https://www.medicaid.gov/medicaid/benefits/downloads/medicaid-chip-telehealth-toolkit.pdf.

[32] Health Res. & Servs. Admin., HRSA Medicare Telehealth Payment Eligibility Analyzer, https://data.hrsa.gov/.

Authors

Stephen D. Bittinger
Partner

Charleston
+1.843.579.5694
Washington D.C.
+1.202.778.9000
stephen.bittinger@klgates.com

Kim H. Looney
Partner

Nashville
+1.615.780.6727
kim.looney@klgates.com

Nora E. Becerra
Associate

Chicago
+1.312.807.4222
nora.becerra@klgates.com

Members of our team are regular contributors to Triage: Timely Conversations for Health Care Professionals, a podcast created by K&L Gates to inform our clients and friends of the firm about the latest developments in health law.

Subscribe to Triage through **Apple Podcasts**, **Google Podcasts**, and **Spotify** to have our episodes delivered directly to you as they become available.

Learn more about our Health Care Fraud and Abuse practice at klgates.com/Health-Care-Fraud-and-Abuse-US-Practices.

K&L GATES

K&L Gates is a fully integrated global law firm with lawyers located across five continents. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants, and entrepreneurs in every major industry group, as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit klgates.com.

This publication is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.