2022

# Telemedicine Scams

Katrice B. Copeland

# Telemedicine Scams

*Katrice Bridges Copeland*[*]

*ABSTRACT: Telemedicine emerged as a lifeline during the COVID-19 pandemic. Although the technology existed long before the pandemic, its use was limited due to strict government regulations that limited reimbursement for telemedicine visits. In response to the pandemic, the Government waived many of its restrictions for the duration of the Public Health Emergency. These changes fueled the growth of telemedicine.*

*The problem, however, is that telemedicine makes it easier to conduct fraud on a large scale because without in-person visits, medical providers can reach many more beneficiaries in a short period of time. Thus, the size and scale of typical health care fraud schemes, such as sending medically unnecessary durable medical equipment, is magnified. This type of fraud has been on the rise since 2016, and, with the relaxed rules for telemedicine reimbursement during the pandemic, there is a serious concern that there will be a sharp increase in telemedicine fraud.*

*This Article examines the fraudulent practices in the telemedicine industry and the conditions that permit them to flourish. This Article critically assesses the changes to telemedicine coverage and their relationship to fraud. It examines the fraudulent practices through the lens of the fraud triangle to determine why telemedicine fraud occurs. After assessing the causes of telemedicine fraud, this Article argues that there is no need for additional criminal statutes to address telemedicine fraud. As the typical telemedicine scam involves the payment of kickbacks and billing for medically unnecessary treatment and services, the existing fraud laws such as the Anti-Kickback statute and the False Claims Act are sufficiently capacious to address the criminality involved in these cases. This Article also argues that in lieu of additional criminal statutes, the Government should focus on additional*

[*] Professor of Law, Penn State Law, University Park, PA. B.S., University of Illinois; J.D., University of Michigan Law School. For helpful comments on this project, I thank Lucy Hodder, Valarie Blake, Deborah Farringer, Kristin Madison, Laura Hoffman, Carl Coleman, John Jacobi, Adam Muchmore, Tara Ragone, and Michal Buchhandler-Raphael. I would also like to thank the participants of the 44th Annual Health Law Professors Conference and Seton Hall's Sixth Annual Health Law Works-in-Progress Retreat. I am grateful to Sierra Zellner, Penn State Law class of 2022, for research assistance.

*measures to prevent or detect telemedicine fraud because preventative measures are the best way to safeguard the integrity of federal health care programs.*



## INTRODUCTION

Telemedicine, which is remote patient care using electronic communication, emerged as a lifeline during the COVID-19 pandemic.[1]

1. *See Telehealth and Telemedicine*, AM. ACAD. OF FAM. PHYSICIANS (Dec. 2021), https://www.aafp.org/about/policies/all/telehealth-telemedicine.html [https://perma.cc/6659-HCLQ]; HEALTHCARE FRAUD PREVENTION P'SHIP, WHITE PAPER: FRAUD, WASTE, AND ABUSE IN THE CONTEXT OF COVID-19, at 14–16 (2022), https://www.cms.gov/files/document/hfpp-white-paper-healthcare-fraud-waste-and-abuse-context-covid-19.pdf [https://perma.cc/Y9RB-VZ8]. This Article will use the term "telemedicine" when discussing patient video or telephone visits but will not change quotations that use the term "telehealth" in lieu of telemedicine when describing these visits.

Although the technology existed long before the COVID-19 pandemic, its use was limited due to strict government regulations. In response to the COVID-19 pandemic, the U.S. Department of Health and Human Services ("HHS") made significant changes to its regulations regarding the use and reimbursement of telemedicine services for the duration of the declared Public Health Emergency.[2] These changes, along with the imposition of stay-at-home orders and the sharp rise in COVID-19 hospitalizations during 2020, fueled the growth of telemedicine.[3] In turn, telemedicine reduced the burden on the health care system and allowed patients to receive care safely in their own homes while under stay-at-home orders or practicing social distancing.[4]

The changes to telemedicine coverage have ushered in both a great expansion of health care access and immense new possibilities for fraud through the exploitation of the Public Health Emergency regulation changes. There have long been concerns about a dearth of health care providers in rural, economically disadvantaged, and underserved areas.[5] Telemedicine has often been touted as one way to increase access to health care in underserved communities.[6] Prior to the expansion of telemedicine during the pandemic, Medicare coverage for telemedicine services was only permitted if: (1) the beneficiary was located in a rural or health professional shortage area; (2) services were delivered in an interactive audio and video telecommunication system; and (3) the beneficiary was in a practitioner's office or a specified medical facility during the telemedicine visit.[7] The waiver of these requirements permitted people in underserved and urban areas to access care through telemedicine, allowed beneficiaries to have telemedicine visits in their own homes, and allowed audio only telemedicine visits (alleviating some concerns about disparate access to broadband and electronic devices). Thus, the number of telemedicine visits skyrocketed during the first year of the pandemic.

At the same time, however, telemedicine makes it easier to conduct fraud on a large scale. Medical providers are able to reach many beneficiaries in a

2. *See* HEALTHCARE FRAUD PREVENTION P'SHIP, *supra* note 1, at 12–17.

3. *See id.* Telemedicine visits for primary care "increased from 4.1% in Q1 2020 to 35.3% in Q2 2020." *Id.* at 18. In addition, "[i]nitial data from Medicaid and CHIP beneficiaries captured from March through June 2020 indicated that 2,632% more services were delivered via telehealth than during the same period in 2019." *Id.*

4. *See infra* Section I.B.2.

5. *See* MEGAN LAHR, CARRIE HENNING-SMITH, ADRITA RAHMAN & ASHLEY M. HERNANDEZ, UNIV. MINN. RURAL HEALTH RSCH. CTR., BARRIERS TO HEALTH CARE ACCESS FOR RURAL MEDICARE BENEFICIARIES: RECOMMENDATIONS FROM RURAL HEALTH CLINICS 1 (2021), https://3pea7g1qp8f3t9ooe3z3npx1-wpengine.netdna-ssl.com/wp-content/uploads/2021/09/UMN-RHC-Access-to-Care-PB_1.20_508.pdf [https://perma.cc/5UMW-FCFS].

6. Taylan Bozkurt, Jose F. Flórez-Arango & Matt Levi, *Telemedicine*, *in* CDC YELLOW BOOK ch. 2(15) (2020), https://wwwnc.cdc.gov/travel/yellowbook/2020/preparing-international-travelers/telemedicine [https://perma.cc/XZ74-KVMS]; *see infra* Section I.A.

7. *See infra* Section I.B.1.

short period of time, and they do not need an in-person visit to order expensive and unnecessary laboratory tests, prescriptions, or durable medical equipment ("DME").[8] HHS and the Department of Justice ("DOJ") have been combatting a rise in large-scale telemedicine fraud since 2016.[9]

In September 2020, the DOJ announced the largest health care fraud takedown in history, "Operation Rubber Stamp," which had a total of 345 defendants and resulted in more than $6 billion in alleged fraud losses.[10] More than two-thirds of the losses, $4.5 billion, were related to telemedicine.[11] Although the schemes vary, the masterminds behind the schemes are typically telemedicine executives who hire marketing firms to target Medicare patients and collect their information.[12] The telemedicine executives then provide the information to doctors and nurse practitioners and pay them to order unnecessary DME (such as orthotics or braces), genetic and other diagnostic testing, and pain medications.[13] The doctors and nurse practitioners then contact the patients with whom they have no prior relationship and have brief telemedicine visits or no visit at all before writing the orders.[14] The DME companies, genetic testing laboratories, and pharmacies then purchase those orders in exchange for illegal kickbacks and bribes and submit false and fraudulent claims for reimbursement to Medicare and other government insurers.[15]

The DOJ's historic 2020 takedown exposed fraud that occurred prior to the COVID-19 pandemic and the resultant surge in the demand for

---

8. MEDICARE PAYMENT ADVISORY COMM'N, REPORT TO CONGRESS: MEDICARE PAYMENT POLICY 471 (2021) [hereinafter 2021 REPORT TO CONGRESS], https://www.medpac.gov/wp-content/uploads/import_data/scrape_files/docs/defaultsource/reports/mar21_medpac_report_to_the_congress_sec.pdf [https://perma.cc/JQJ3-Y9F7]. The Balanced Budget Act of 1997 (Public Law No. 105–33) established the Medicare Payment Advisory Commission as an independent congressional agency charged with advising Congress on issues affecting the Medicare program. The Medicare Payment Advisory Commission provides two reports to Congress each year. *Id.* at foreword.

9. OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., 2020 NATIONAL HEALTH CARE FRAUD TAKEDOWN (2020), https://oig.hhs.gov/documents/root/230/2020HealthCare Takedown_FactSheet_9dtIhW4.pdf [https://perma.cc/2TBK-F6LJ].

10. *Id.*; Press Release, U.S. Dep't of Just., Operation Rubber Stamp: Major Health Care Fraud Investigation Results in Significant New Charges (Oct. 7, 2020), https://www.justice.gov/usao-sdga/pr/operation-rubber-stamp-major-health-care-fraud-investigation-results-significant-new [https://perma.cc/273Z-8CA9]; *see* U.S. DEP'T OF HEALTH & HUM. SERVS. & U.S. DEP'T OF JUST., HEALTH CARE FRAUD AND ABUSE CONTROL PROGRAM ANNUAL REPORT FOR FISCAL YEAR 2020, at 34 (2020) [hereinafter HEALTH CARE FRAUD REPORT], https://oig.hhs.gov/publications/docs/hcfac/FY2020-hcfac.pdf [https://perma.cc/7AHP-5JDS].

11. HEALTH CARE FRAUD REPORT, *supra* note 10, at 9–10.

12. OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., NATIONAL TELEFRAUD TAKEDOWN: THE ALLEGED SCHEME AND KEY PLAYERS (2020), https://oig.hhs.gov/documents/root/232/telemed-scheme-print_CkIjtht.pdf [https://perma.cc/2825-V2T8].

13. *See id.*

14. *See id.*

15. *See id.*

telemedicine. The concern is that increased utilization of telemedicine services will further expose federal health care programs to fraudulent schemes. As HHS Deputy Inspector General Gary Cantrell explained, "[t]elemedicine can foster efficient, high-quality care when practiced appropriately and lawfully.[] Unfortunately, bad actors attempt to abuse telemedicine services and leverage aggressive marketing techniques to mislead beneficiaries about their health care needs and bill the Government for illegitimate services."[16] Indeed, there has been at least one major case involving telemedicine fraud since the beginning of the pandemic.[17] The HHS Office of Inspector General ("OIG") is so concerned with the risk of telemedicine fraud that it has taken the extraordinary step of issuing a "Special Fraud Alert" warning practitioners about suspicious agreements with telemedicine companies.[18]

The primary victims of telemedicine scams are Medicare and other federal health care programs that "ha[ve] footed the bill for billions worth of" unnecessary genetic tests, DME, and prescriptions.[19] The telemedicine scams further tax government health care programs that are already struggling financially. Patients are also substantially harmed through these scams. In some cases, the harm is financial, in that "patients [have] had to pay for declined services."[20] In other situations, patients either never received the DME, test results, or medications, or they turned out to be useless "to the patients and their actual primary care doctors."[21] Further, "the misdirection, fake diagnoses, and unneeded tests misled patients and delayed their chance to seek appropriate treatment for medical complaints."[22] With respect to genetic testing in particular, the Government may deny a future claim for a

16. Press Release, U.S. Dep't of Just., National Health Care Fraud and Opioid Takedown Results in Charges Against 345 Defendants Responsible for More than $6 Billion in Alleged Fraud Losses (Sept. 30, 2020), https://www.justice.gov/opa/pr/national-health-care-fraud-and-opioid-takedown-results-charges-against-345-defendants [https://perma.cc/36L4-FTRY].

17. *See infra* Section III.A.

18. OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., SPECIAL FRAUD ALERT: OIG ALERTS PRACTITIONERS TO EXERCISE CAUTION WHEN ENTERING INTO ARRANGEMENTS WITH PURPORTED TELEMEDICINE COMPANIES 1 (2022) [hereinafter SPECIAL FRAUD ALERT], https://oig.hhs.gov/documents/root/1045/sfa-telefraud.pdf [https://perma.cc/M3PR-Q9WN].

19. Annalisa Merelli, *Telehealth Fraud Has Cheated the US of Billions in the Pandemic*, QUARTZ (July 20, 2022), https://qz.com/2014700/telehealth-frauds-cost-the-us-more-than-6-billion [https://perma.cc/Z5TN-DNKX].

20. *Id.*

21. OFF. OF INSPECTOR GEN., *supra* note 9. Unnecessary genetic tests in particular will have very little value for the patient. "The results from these tests only provide information about risks for developing a particular disease, and individuals can take only minimal action on the information, particularly when the results are presented to patients without proper interpretation or guidance by their treating physician or a healthcare provider." HEALTHCARE FRAUD PREVENTION P'SHIP, WHITE PAPER: GENETIC TESTING FRAUD, WASTE, & ABUSE 13–14 (2020), https://www.cms.gov/files/document/hfpp-genetic-testing-fwa-white-paper.pdf [https://perma.cc/FFR6-SZ4C].

22. OFF. OF INSPECTOR GEN., *supra* note 9 (emphasis omitted).

necessary genetic test due to reimbursement for the previous unnecessary test.[23] In addition to the patients directly affected by the fraud, taxpayers end up facing "rising . . . health care premiums and out-of-pocket costs."[24]

This is the first Article to address fraud in the telemedicine industry. Once the Public Health Emergency is over, it will be impossible to put telemedicine back into a box and shut the lid. Telemedicine is here to stay. It is not clear which, if any, of the previous restrictions on access to telemedicine the Government will reimpose. The Government's interest in investigating and prosecuting telemedicine fraud will likely increase, as will the need to impose new measures to prevent telemedicine fraud. In formulating new rules aimed at telemedicine fraud, the key question is how to balance access to care with fraud prevention.

This Article examines telemedicine schemes that take advantage of the vulnerabilities in federal health care programs such as Medicare and Medicaid. Part I provides background on telemedicine and the Government's pre- and post-pandemic coverage of telemedicine services. It also examines the relationship between telemedicine coverage restrictions and fraud. Part II provides an overview of the statutes used to prosecute telemedicine schemes. It also discusses the Government's fraud detection methods. Part III assesses the state of fraud in the telemedicine industry. It begins by scrutinizing the schemes that telemedicine executives utilize to defraud patients and insurers. It then examines telemedicine fraud through the lens of the fraud triangle to assess why telemedicine fraud occurs.

Part IV argues that there is no need for additional criminal statutes to address telemedicine fraud. As the typical telemedicine scam involves the payment of kickbacks and billing for medically unnecessary treatment and services, the existing fraud laws such as the Anti-Kickback statute and the False Claims Act are sufficiently capacious to address the criminality involved in these

---

23. HEALTHCARE FRAUD PREVENTION P'SHIP, *supra* note 21, at 13. The Healthcare Fraud Prevention Partnership explained that if a patient was caught up in one of these schemes and had genetic tests it could lead to serious problems in the future:

> If that individual were to have hereditary cancer testing ordered by a treating provider in the future, the claim might be denied as most hereditary genetic testing is only allowed once-in-a-lifetime. At a critical time where the test is needed in earnest, the record may show such an analysis was already performed and is no longer an available benefit for that individual.

*Id.*

24. Press Release, U.S. Dep't of Just., 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 Losses (Apr. 9, 2019), https://www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes [https://perma.cc/4MXE-L82X]; *see also* Anthony Kyriakakis, *The Missing Victims of Health Care Fraud*, 2015 UTAH L. REV. 605, 619 ("[M]ost of the direct economic harms third-party payers and insurers suffer are eventually passed along to taxpayers, employers, and beneficiaries in the form of higher tax burdens, more expensive premiums, and less comprehensive coverage.").

cases. It also argues that in lieu of additional criminal statutes, the Government should focus on additional measures to prevent or detect telemedicine fraud because preventative measures are the best way to assure program integrity. Further, Part IV examines three potential fraud prevention and detection measures. First, it assesses the viability of a rule requiring a pre-existing doctor-patient relationship that was established in person prior to reimbursement for durable medical equipment and expensive genetic tests. Second, it examines the impact that a rule limiting reimbursement for telemedicine visits based on the provider's payment model would have on fraud prevention. Third, it explores the potential for changes to Medicare enrollment and claim reimbursement to identify and prevent fraud before it occurs. Lastly, Part IV also assesses each proposal through the lens of the fraud triangle and the underlying need to balance the conflicting goals of telemedicine (access to care) with fraud enforcement (cost containment). This Article concludes that changes to Medicare enrollment and claims reimbursement will be the most effective way to prevent fraud and preserve access to care.

## I. BACKGROUND

### A. *TELEHEALTH AND TELEMEDICINE*

Although "[t]here is no single definition for telehealth," telehealth is generally understood to be "a collection of means [or methods] to enhance [health] care and education delivery" using telecommunications technologies.[25] Telemedicine refers specifically to "the practice of medicine using [communication] technology to deliver care" remotely.[26] Thus, the focus is on the provision of clinical services (examination, diagnosis, and treatment) from a distance. The term telehealth has often been used interchangeably with telemedicine, but telehealth is broader than telemedicine because it encompasses "a broader scope of remote . . . services."[27] For example, a live video visit between a doctor and patient is telemedicine whereas a patient's use of an online patient portal to view her medical records is telehealth.

25. *What is Telehealth?*, CTR. FOR CONNECTED HEALTH POL'Y, https://www.cchpca.org/what-is-telehealth [https://perma.cc/SLT4-EB7W].

26. *Telehealth and Telemedicine*, *supra* note 1.

27. *Id.* ("[T]elehealth can refer to remote non-clinical services such as provider training, continuing medical education or public health education, administrative meetings, and electronic information sharing to facilitate and support assessment, diagnosis, consultation, treatment, education, and care management."); *see also* PHILIPPE BARDY, THE HUMAN CHALLENGE OF TELEMEDICINE 4 (2019) (explaining that telehealth applications include "all sites and portals, in whole or in part related to health, that can be found on the internet. These sites, well known to patients and practitioners, offer numerous services: advice, recommendations, articles, forums, newsletters and, for some of them, online medical records").

Telemedicine companies, that are at the center of the fraud schemes discussed in this Article, provide telemedicine services by hiring health care providers and furnishing the remote communications technology for those providers. The telemedicine companies pay health care providers to conduct consultations with patients. Telemedicine companies then bill private or public insurance companies or offer a membership program to their customers to generate revenue.

There are several different approaches used in the provision of telemedicine services. In real-time or synchronous visits, the information and data are transferred live.[28] Typically, this type of visit occurs through the use of video conferencing between the patient and health care provider, but it may also include activities such as the live viewing of ultrasounds as they take place or the streaming of medical procedures from the operating room.[29] In "store-and-forward" or asynchronous approaches, prerecorded medical information, such as patient intake forms or X-rays, is transmitted to a health care provider "to diagnose or treat [an] issue."[30] It is commonly "used for patient intake or follow-up care."[31] Telemonitoring, or remote patient monitoring, is the use of personal health technologies to record, process, and transmit information from the patient to the doctor.[32] Remote monitoring could include at-home devices, such as heart rate or blood pressure monitors and can be used for chronic disease management.[33]

Telemedicine is uniquely situated to address some of the most pressing problems in health care. In particular, it can help address problems such as inequalities in "accessibility, cost, [and] the shortage of trained physicians."[34] One of the biggest benefits of telemedicine is the cost and time savings. Patients need not travel to the doctor, which reduces both travel costs and waiting time.[35] In addition, it makes it easier to visit with specialists who may not be located in the patient's community.[36] Telemedicine is particularly useful

28. U.S. DEP'T OF HEALTH & HUM. SERVS., TELEHEALTH FOR DIRECT-TO-CONSUMER CARE (2021), https://telehealth.hhs.gov/providers/direct-to-consumer/synchronous-direct-to-consumer-telehealth [https://perma.cc/Z7KM-5ZLR].

29. *See id.*

30. U.S. DEP'T OF HEALTH & HUM. SERVS., ASYNCHRONOUS DIRECT-TO-CONSUMER TELEHEALTH (2021), https://telehealth.hhs.gov/providers/direct-to-consumer/asynchronous-direct-to-consumer-telehealth [https://perma.cc/FNV5-MWDC].

31. *Id.*

32. *See Telehealth: Defining 21st Century Care*, AM. TELEMEDICINE ASS'N, https://www.americantelemed.org/resource/why-telemedicine [https://perma.cc/NVG5-GQBK].

33. *Id.*

34. Mohit Joshi, *Telehealth Has Huge Potential, but Challenges Remain*, FORBES (Feb. 12, 2020, 8:20 AM), https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2020/02/12/telehealth-has-huge-potential-but-challenges-remain/?sh=2a4714b6191a [https://perma.cc/MXG8-BQ3W].

35. Bozkurt et al., *supra* note 6, ch. 2(15).

36. *Id.*

in rural areas[37] and underserved communities.[38] A major stumbling block for telemedicine access in rural and underserved areas, however, is the lack of reliable and affordable broadband connectivity.[39] Without reliable broadband connectivity, the electronic transmission of data that is necessary for live video visits is not possible. And even when broadband is available in rural or underserved communities, "its cost can be three times" the cost "in urban areas."[40]

Another impediment to the widespread use of telemedicine is state physician licensing laws. Forty-eight "states and the District of Columbia require that physicians" treating patients through the use of telemedicine must "be licensed in the state [where] the patient" resides.[41] Thus, a specialist licensed to practice in Maryland could not have a telemedicine visit with a patient in rural West Virginia unless the specialist is also licensed in West Virginia. One way to address this issue is through multistate compacts that allow providers in participating states to have an expedited procedure for multi-state licensing. As of March 2018, twenty-two states have enacted a physician multistate compact called the Interstate Medical Licensure Compact.[42] The multistate compacts serve the dual purposes of increasing access to care and assisting the use of telemedicine.[43]

The other major barrier to widespread use of telemedicine is the uncertainty concerning cost and reimbursement. Historically, the Government's policies and regulations concerning telemedicine have been difficult to navigate. As will be discussed in greater detail in the next Part, Medicare

37. "Telemedicine has benefits in both rural and urban areas, but it is not always a viable option. In remote rural areas, there may not be the bandwidth and connectivity capable of supporting the communication technologies." *Id.*

38. *See Telehealth vs. Telemedicine*, AMD GLOB. TELEMEDICINE (Feb. 3, 2020), https://www.amdtelemedicine.com/blog/article/telehealth-vs-telemedicine-how-telehealth-different-telemedicine [https://perma.cc/C6TQ-CWBX].

39. Gary Shapiro, *Broadband Access: Health Care's Newest Challenge*, STAT (Nov. 12, 2021), https://www.statnews.com/2021/11/12/broadband-access-newest-challenge-health-care [https://perma.cc/F6YL-KH3U].

40. MEDICAID & CHIP PAYMENT & ACCESS COMM'N, REPORT TO CONGRESS ON MEDICAID AND CHIP: MARCH 2018, at 46 (2018) [hereinafter MARCH 2018 MACPAC REPORT], https://www.macpac.gov/wp-content/uploads/2018/03/Report-to-Congress-on-Medicaid-and-CHIP-March-2018.pdf [https://perma.cc/HBK7-Y9ME] ("Although the Federal Communications Commission and the U.S. Department of Agriculture have programs to facilitate expansion of broadband to rural areas, the required application, cost sharing, and process for obtaining funds may prevent health care providers from accessing them. In addition, there are likely to be costs associated with the acquisition, installation, maintenance, repair, and replacement of front-end technology needed to establish telehealth as a way of delivering services. However, not all states provide payment for these costs, which may be prohibitive and thus affect providers' ability or willingness to adopt telehealth." (citation omitted)).

41. *Id.*

42. *Id.*

43. *Id.*

provided very limited support for telemedicine.[44] Medicare's reimbursement for telemedicine visits was based on very strict geographic limitations, and Medicare would not reimburse telemedicine visits that took place in a patient's home.[45] In addition, the reimbursement rate for telemedicine visits was typically lower than an in-person visit.[46] The Public Health Emergency brought on by COVID-19 acted as a catalyst in the adoption of telemedicine and required regulatory flexibilities concerning reimbursement.

### *B. MEDICARE AND MEDICAID COVERAGE FOR TELEMEDICINE SERVICES*

Medicare is a national, federally funded insurance program that provides free or below-cost health care benefits for individuals who are age sixty-five or older or those with long-term disabilities.[47] Medicare includes payments for telemedicine visits under Medicare Part B which covers outpatient care.[48] In 2019, Medicare provided benefits to nearly sixty-one million beneficiaries at a cost of around $782 billion.[49] Medicaid is a joint federal-state program that supports states' coverage of medical care and other support services for certain categories of low-income individuals.[50] The Federal Government pays a share, known as the Federal Medical Assistance

44. *See infra* Section I.B.1.

45. *See infra* Section I.B.1.

46. *See infra* Section I.B.1.

47. *See* 42 U.S.C. §§ 1395–1395hhh (2018) (providing the standard for Medicare); CTRS. FOR MEDICARE & MEDICAID SERVS., MEDICARE PROGRAM - GENERAL INFORMATION (2021) [hereinafter CMS MEDICARE GENERAL INFORMATION], http://www.cms.gov/MedicareGenInfo [https://perma.cc/C4VR-CSLH] (noting that Medicare provides coverage to those aged sixty-five and older, individuals with certain disabilities, and individuals with end-stage renal disease). Medicare has four parts: Part A (inpatient hospital care), Part B (outpatient care), Part C (Parts A and B delivered through a managed care plan), and Part D (prescription drug coverage). *See* 42 U.S.C. §§ 1395–1395hhh. Private insurance companies sell Part C plans. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., WHAT IS MEDICARE PART C? (2021), https://www.hhs.gov/answers/medicare-and-medicaid/what-is-medicare-part-c/index.html [https://perma.cc/QXD9-46PV]. Part C includes the same coverage as original Medicare but may also include additional benefits. *Id.*

48. 42 U.S.C. § 1395m(m) (describing special payment rules for particular items and services under Part B). Medicare Part B covers medical services provided by physicians, medical clinics, laboratories, and other qualified health care providers, such as office visits, laboratory testing, and minor surgical procedures. CMS MEDICARE GENERAL INFORMATION, *supra* note 47. Medicare also covers telemedicine visits through Part C, but the focus of this article is on coverage under Medicare Part B. *See* 42 U.S.C. § 1395m(m).

49. ALISON MITCHELL ET AL., CONG. RSCH. SERV., R43357, MEDICAID: AN OVERVIEW 1 (2021), https://sgp.fas.org/crs/misc/R43357.pdf [https://perma.cc/3AKU-PZ44].

50. CTRS. FOR MEDICARE & MEDICAID SERVS., DUALLY ELIGIBLE INDIVIDUALS - CATEGORIES (2022), https://www.cms.gov/Medicare-Medicaid-Coordination/Medicare-and-Medicaid-Coordination/Medicare-Medicaid-Coordination-Office/Downloads/MedicareMedicaidEnrolleeCategories.pdf [https://perma.cc/9UEX-PCDD]. "Medicaid was designed to provide coverage to groups with a wide range of health care needs that historically were excluded from the private health insurance market (e.g., individuals with disabilities who require [long-term services and supports] or indigent populations in geographic locations where access to providers is limited)." MITCHELL ET AL., *supra* note 49, at 3.

Percentage,[51] of each state's Medicaid costs.[52] Medicaid's coverage of telemedicine visits varies from state to state. In 2019, Medicaid had approximately seventy-five million enrollees at a cost of $627 billion.[53]

1. Pre-Pandemic Coverage of Telemedicine Services

Medicare Part B's coverage of telemedicine visits began in 2001. The Balanced Budget Act of 1997 authorized Medicare coverage of certain telemedicine services through the physician fee schedule ("PFS").[54] Since the Balanced Budget Act of 1997, Congress gradually expanded telemedicine coverage by increasing the list of approved providers, modifying the payment structure, and expanding the definition of rural areas. The Center for Medicare and Medicaid Services ("CMS"), which administers Medicare and Medicaid, has "increased the number of permissible telehealth services through regulation by increasing the number of billing codes."[55] Medicare Part B reimburses for

---

51. The Federal Medical Assistance Percentage rate

> is determined annually and varies by state according to each state's per capita income relative to the U.S. per capita income. The formula provides higher [Federal Medical Assistance Percentage] rates, or federal reimbursement rates, to states with lower per capita incomes, and it provides lower [Federal Medical Assistance Percentage] rates to states with higher per capita incomes.

MITCHELL ET AL., *supra* note 49, at 16. The statutory minimum Federal Medical Assistance Percentage rate is fifty percent and the maximum is eighty-three percent. *Id.* In 2019, following the expansion of Medicaid under the Affordable Care Act, the average federal share of Medicaid was estimated at sixth-five percent. *Id.* at 18–19.

52. *See* JULIA PARADISE, THE KAISER COMM'N ON MEDICAID & THE UNINSURED, MEDICAID MOVING FORWARD 2 (2015), http://www.kff.org/medicaid/7235.cfm [https://perma.cc/M7PS-NDQ8].

53. MITCHELL ET AL., *supra* note 49, at 1. Approximately twenty percent of the U.S. population was covered by Medicaid in 2019. *Id.*

54. MEDICARE PAYMENT ADVISORY COMM'N, REPORT TO THE CONGRESS: MEDICARE AND THE HEALTH CARE DELIVERY SYSTEM 230, 235 (2016) [hereinafter 2016 REPORT TO CONGRESS], https://www.medpac.gov/wp-content/uploads/import_data/scrape_files/docs/default-source/reports/june-2016-report-to-the-congress-medicare-and-the-health-care-delivery-system.pdf [https://perma.cc/KC69-AU2P].

> (CMS) determines the payment rate for each service based on the clinician work required to provide the service, expenses related to maintaining a practice, and professional liability insurance (PLI) costs. Payments are adjusted to account for variations in the input prices in different markets. Medicare's payment rates also may be adjusted based on provider characteristics, additional geographic designations, and other factors. Medicare pays the provider the final calculated amount, less any beneficiary cost sharing.

MEDICARE PAYMENT ADVISORY COMM'N, PHYSICIAN AND OTHER HEALTH PROFESSIONAL PAYMENT SYSTEM 1 (2021), https://www.medpac.gov/wp-content/uploads/2021/11/medpac_payment_basics_21_physician_final_sec.pdf [https://perma.cc/P25T-AWUM].

55. MEDICARE PAYMENT ADVISORY COMM'N, REPORT TO CONGRESS: MEDICARE PAYMENT POLICY 480 (2018) [hereinafter 2018 REPORT TO CONGRESS], https://www.medpac.gov/wp-content/uploads/import_data/scrape_files/docs/default-source/reports/mar18_medpac_entirereport_sec_rev_0518.pdf [https://perma.cc/K6Z2-997C].

telemedicine services such as office visits, consultations, psychotherapy, and certain other medical or health services provided by its approved list of distant site practitioners, which includes physicians, nurse practitioners, and physician assistants.[56]

Although Medicare's coverage of telemedicine has expanded, the number of Medicare patients who were eligible for reimbursement for telemedicine visits remained very limited. Medicare will only reimburse telemedicine services for a geographically restricted set of patients. Patients must be located in a rural Health Professional Shortage Area or a county outside the Metropolitan Statistical Area, as determined by the Health Resources and Services Administration and the Census Bureau respectively.[57] Health Professional Shortage Areas designate areas where there are health care provider shortages in primary care, mental health, or dental health.[58] A Metropolitan Statistical Area is essentially a city surrounded by communities that are economically and socially integrated with the city.[59] Thus, telemedicine coverage is not available for the millions of Medicare patients who live in urban areas. The geographic restrictions on telemedicine coverage may help to reduce fraud because the restrictions limit the Medicare beneficiaries who can be targeted as part of telemedicine scams.

Even if a beneficiary can meet the geographical restrictions, the patient must travel to an originating site,[60] such as a physician's office or hospital, to use telemedicine services.[61] Patients at originating sites "must use an interactive audio and video telecommunications system that permits real-time

56. Distant site practitioners who can furnish and receive payment for covered telehealth services include: physicians, nurse practitioners, physician assistants, nurse-midwives, clinical nurse specialists, certified registered nurse anesthetists, clinical psychologists and clinical social workers, and registered dietitians or nutrition professionals. MEDICARE LEARNING NETWORK, CTRS. FOR MEDICARE & MEDICAID SERVS., TELEHEALTH SERVICES 4 (2020), https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/TelehealthSrvcsfctsht.pdf [https://perma.cc/5CUF-VTU2].

57. 42 U.S.C. § 1395m(m)(4)(c); MEDICARE LEARNING NETWORK, *supra* note 56, at 3.

58. HEALTH RES. & SERVS. ADMIN., WHAT IS SHORTAGE DESIGNATION? (2021), https://bhw.hrsa.gov/shortage-designation/hpsas [https://perma.cc/R8LP-CHYJ].

59. U.S. CENSUS BUREAU, METROPOLITAN AND MICROPOLITAN: ABOUT (2021), https://www.census.gov/programs-surveys/metro-micro/about.html [https://perma.cc/FEB4-DQWY].

60. "An originating site is the location where a Medicare [beneficiary] gets physician or practitioner medical services through a telecommunications system." MEDICARE LEARNING NETWORK, *supra* note 56, at 3.

61. *Id.* Eligible originating sites include: hospitals, critical access hospitals, physician and practitioner offices, rural health clinics, federally qualified health centers, hospital-based renal dialysis centers, skilled nursing facilities, community mental health centers, renal dialysis facilities, homes of beneficiaries with End-Stage Renal Disease receiving home dialysis, and mobile stroke units. *See* 42 U.S.C. § 1395m(m)(4)(C)(ii).

communication" between the distant site practitioner[62] and the patient.[63] Therefore, patients are unable to access telemedicine services in their homes.[64] Medicare pays the originating site a facility fee, which was twenty-five dollars in 2017, under the PFS for telehealth service, and Medicare pays the distant site provider the "same rate for services delivered via tele[medicine] as they would [receive] for the in-person service, as required by [the] statute."[65] The originating site requirement makes it less likely that providers will bill Medicare for sham telemedicine visits. On February 9, 2018, Congress passed, and the President signed into law, the Bipartisan Budget Act of 2018, which expanded the coverage of telemedicine services under the PFS to include the treatment of strokes in urban areas.[66] It also permitted accountable care organizations[67] to bill for telemedicine "services originating from the patient's residence" in urban areas.[68]

In addition to restrictions on which Medicare beneficiaries can receive telemedicine services and where they can be received, Medicare also restricts the types of providers who can be reimbursed for telemedicine visits. Only physicians, and certain other practitioners, such as physician assistants and nurse practitioners, are eligible to receive Medicare payment for telemedicine visits.[69] Thus, many health care professionals, such as clinical psychologists and occupational therapists, are ineligible to furnish and bill for Medicare telemedicine services.

---

62. MEDICARE LEARNING NETWORK, *supra* note 56, at 4. Distant site practitioners who can furnish and receive payment for covered telehealth services include: physicians, nurse practitioners, physician assistants, nurse-midwives, clinical nurse specialists, certified registered nurse anesthetists, clinical psychologists and clinical social workers, and registered dietitians or nutrition professional. *Id.*; 42 U.S.C. § 1395m(m)(4)(C).

63. MEDICARE LEARNING NETWORK, *supra* note 56, at 4.

64. *See* 42 U.S.C. § 1395m(m)(4)(C).

65. U.S. GOV'T ACCOUNTABILITY OFF., GAO-17-365, HEALTH CARE: TELEHEALTH & REMOTE PATIENT MONITORING USE IN MEDICARE AND SELECTED FEDERAL PROGRAMS 8 (2017), https://www.gao.gov/assets/gao-17-365.pdf [https://perma.cc/74U4-9UHH].

66. 42 U.S.C. § 1395m(m)(6)(A) (explaining that the originating site requirements of 42 U.S.C. § 1395m(m)(4)(C) do "not apply with respect to telehealth services furnished on or after January 1, 2019, for purposes of diagnosis, evaluation, or treatment of symptoms of an acute stroke, as determined by the Secretary").

67. Accountable Care Organizations "are groups of doctors, hospitals, and other health care providers, who come together voluntarily to give coordinated high-quality care to their Medicare patients." CTRS. FOR MEDICARE & MEDICAID SERVS., ACCOUNTABLE CARE ORGANIZATIONS (ACOS) (2021), https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO [https://perma.cc/HVD9-SXTZ].

68. 2018 REPORT TO CONGRESS, *supra* note 55, at 479.

69. 42 U.S.C. § 1395m(m)(4)(E); *id.* § 1395u(b)(18)(C). The practitioners covered include: physician assistant, nurse practitioner, clinical nurse specialist, certified registered nurse anesthetist, certified nurse-midwife, clinical social worker, clinical psychologist, and registered dietician or nutrition professional. *Id.* § 1395m(m)(4)(E); *id.* § 1395u(b)(18)(C).

Medicaid coverage of telemedicine services varies by state and has become much more expansive in recent years.[70] "Each state has a Medicaid state plan" that CMS must approve that "describes . . . the services and populations that are covered under the state's Medicaid program."[71] States differ on whether they should cover telemedicine, what types of telemedicine they should cover, how telemedicine is provided or covered, which types of telemedicine providers are covered or reimbursed, and "how much to reimburse for telemedicine services."[72] Much like payment for telemedicine services under Medicare, Medicaid pays for telemedicine services "on an item-by-item basis" with facility-based telemedicine services included as part of "the fixed payment for a unit of care."[73]

### 2. COVID-19 and Resulting Coverage Changes

In the early months of 2020, the Federal Government began to express concern over the global outbreak of COVID-19.[74] By late January, the Secretary of HHS declared COVID-19 to be a Public Health Emergency.[75] On January 30, 2020, the World Health Organization declared the coronavirus outbreak to be a "Public Health Emergency of International Concern."[76] By

70. CTR. FOR CONNECTED HEALTH POL'Y, STATE TELEHEALTH MEDICAID FEE-FOR-SERVICE POLICY: A HISTORICAL ANALYSIS OF TELEHEALTH: 2013–2019, at 5 (2020), https://www.cchpca.org/sites/default/files/2020-01/Historical%20State%20Telehealth%20Medicaid%20Fee%20For%20Service%20Policy%20Report%20FINAL.pdf [https://perma.cc/B675-6YSY].

71. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 65, at 10 n.23.

72. *Id.* at 9–10.

73. 2018 REPORT TO CONGRESS, *supra* note 55, at 478.

74. An outbreak of COVID-19 was detected in Wuhan, China in December of 2019. CTRS. FOR DISEASE CONTROL & PREVENTION, BASICS OF COVID-19 (2021), https://www.cdc.gov/coronavirus/2019-ncov/your-health/about-covid-19/basics-covid-19.html [https://perma.cc/57Y8-67LX]. The cause of this outbreak is a new virus, known as the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). *See id.* Coronaviruses are a family of viruses that can cause mild-to-moderate upper-respiratory tract illnesses. *Id.* When an infected person coughs, sneezes, or even talks, the new coronavirus may be transmitted through expelled droplets. *Id.* These droplets can enter a person's system through the mouth, eyes, or nose. *Id.* It is also possible for the droplets to be inhaled into the lungs. *Id.*

75. Press Release, U.S. Dep't of Health & Hum. Servs., Off. of the Assistant Sec'y for Preparedness & Response, Determination that a Public Health Emergency Exists (Jan. 31, 2020), https://www.phe.gov/emergency/news/healthactions/phe/Pages/2019-nCoV.aspx [https://perma.cc/M4FC-9CA6]. The Secretary of HHS has renewed the public health emergency approximately every ninety days through January 11, 2023. *See* Press Release, U.S. Dep't of Health & Hum. Servs., Admin. for Strategic Preparedness & Response, Renewal of Determination that a Public Health Emergency Exists (Oct. 13, 2022), https://aspr.hhs.gov/legal/PHE/Pages/covid19-13Oct2022.aspx [https://perma.cc/Y8DW-6RHW] (noting previous renewals on April 21, 2020, July 23, 2020, October 2, 2020, January 7, 2021, April 15, 2021, July 19, 2021, October 15, 2021, January 14, 2022, April 12, and July 15, 2022).

76. *COVID-19 Public Health Emergency of International Concern (PHEIC) Global Research and Innovation Forum*, WORLD HEALTH ORG. (Feb. 12, 2020), https://www.who.int/publications/m/item/covid-19-public-health-emergency-of-international-concern-(pheic)-global-research-and-innovation-forum [https://perma.cc/P47C-XGEJ].

late February and early March 2020, the global outbreak of COVID-19 had entered a new phase, with community spread occurring in many countries and several U.S. states.[77] Concerns grew over the potential for the disease to spread widely, leading to increased hospitalizations and deaths. On March 11, 2020, the World Health Organization declared COVID-19 a pandemic.[78] On March 13, 2020, President Trump declared the coronavirus pandemic to be a national emergency.[79]

After the declaration of COVID-19 as a Public Health Emergency, CMS explained that:

> [T]here is an urgency to expand the use of technology to help people who need routine care, and keep vulnerable beneficiaries and beneficiaries with mild symptoms in their homes while maintaining access to the care they need. Limiting community spread of the virus, as well as limiting the exposure to other patients and staff members will slow viral spread.[80]

Accordingly, CMS expanded access to telemedicine services on an emergency basis under the Social Security Act's 1135 waiver authority[81] and the Coronavirus Preparedness and Response Supplemental Appropriations Act.[82] The expansion applies to three types of virtual services: Medicare telemedicine visits (live, synchronous visits); virtual check-ins (brief communications through synchronous discussion over a telephone or exchange of information through video or image, i.e., store-and-forward); and E-Visits ("non-face-to-face patient-initiated communications" through online patient portals).[83]

The 1135 waivers, which went into effect on March 6, 2020, and remain in effect until the end of the Public Health Emergency,[84] addressed the

77. *See* CTRS. FOR DISEASE CONTROL & PREVENTION, COVID-19 TIMELINE (2022), https://bit.ly/3Lv2d2n [https://perma.cc/4GBB-PZFX].

78. *Id.*

79. *Id.*

80. CTRS. FOR MEDICARE & MEDICAID SERVS., MEDICARE TELEMEDICINE HEALTH CARE PROVIDER FACT SHEET (2020), https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet [https://perma.cc/LE5M-BX8Y]. The geographic limitation is set forth in 42 U.S.C. § 1395m(m).

81. Under section 1135 of the Social Security Act, the Secretary of Health and Human Services is authorized to temporarily waive or modify certain Medicare, Medicaid, and Children's Health Insurance Program ("CHIP") requirements to ensure that sufficient health care items and services are available to meet the needs of individuals enrolled in Social Security Act programs. *See* 42 U.S.C. § 1320b–5(b).

82. Coronavirus Preparedness and Response Supplemental Appropriations Act, Pub. L. No. 116-123, § 102, 134 Stat. 146, 156 (2020).

83. CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 80.

84. The waivers were initially intended to last for the duration of the Public Health Emergency, but Congress passed legislation in March 2022 that extended many of the telemedicine related waivers for 151 days after the end of the Public Health Emergency. Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, tit. III, subtit. A, §§ 301–306, 136 Stat. 49, 804–808 (2022) (providing flexibility extensions for geographic requirements and

biggest impediments to the adoption of telemedicine. First, CMS waived the geographic restrictions that limited reimbursement for Medicare telemedicine visits to patients living in rural areas.[85] Thus, Medicare patients all over the country have access to telemedicine visits for the duration of the Public Health Emergency.[86] In addition, CMS waived the requirement that patients participate in telemedicine visits from an originating site.[87] During the Public Health Emergency, patients may participate in telemedicine visits from their home rather than or in addition to originating sites.[88] CMS also waived the requirement of both audio and video technologies for telemedicine visits, making telephone (audio only) visits permissible.[89] This change allows the use of telemedicine visits for underserved populations where broadband is unavailable or beneficiaries do not have smart phones, tablets, or computers to have a video connection with their health care providers.

While the waiver of the geographic restrictions is laudable because of increased access to telemedicine visits, it also makes Medicare and Medicaid more vulnerable to fraud. A potential telemedicine scam is no longer limited to rural areas. Fraudsters can now target Medicare beneficiaries in urban areas. This dramatically increases the number of beneficiaries that fraudsters can target. It should be noted that in some of the telemedicine scams that took place prior to the pandemic, the fraudsters worked around the geographical restriction by not billing for the telemedicine visit itself.[90] Instead, they only billed for the durable medical equipment, genetic tests, or drugs.[91] With the waiver, the telemedicine companies can get reimbursed for

originating sites, practitioners eligible to furnish telemedicine services, and audio-only telemedicine services). Conversely, the HHS Office of Civil Rights has indicated that its exercise of enforcement discretion to not impose penalties on health care providers that fail to comply with the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996), ("HIPAA") rules will end as soon as the Secretary of HHS declares that the Public Health Emergency no longer exists or upon the expiration date of the declared Public Health Emergency. U.S. DEP'T OF HEALTH & HUM. SERVS., GUIDANCE ON HOW THE HIPAA RULES PERMIT COVERED HEALTH CARE PROVIDERS AND HEALTH PLANS TO USE REMOTE COMMUNICATION TECHNOLOGIES FOR AUDIO-ONLY TELEHEALTH (2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html [https://perma.cc/H9MN-64K5]. Thus, this Article will continue to refer to the waivers and flexibilities expiring at the end of the Public Health Emergency with the understanding that some of the waivers will last for an additional 151 days.

85. CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 80.

86. *Id.*

87. *Id.* With respect to telemedicine services for substance use disorder and mental health, the Consolidated Appropriations Act, Pub. L. No. 116-260, div. CC, tit. I, subtit. B, § 123, 134 Stat. 1182, 2956–2957 (2020) made the waiver permanent. *See* 42 U.S.C. § 1395m(m)(7).

88. CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 80.

89. CTRS. FOR MEDICARE & MEDICAID SERVS., COVID-19 EMERGENCY DECLARATION BLANKET WAIVERS FOR HEALTH CARE PROVIDERS 1 (2021), https://www.cms.gov/files/document/summary-covid-19-emergency-declaration-waivers.pdf [https://perma.cc/482K-Y8GK].

90. *See infra* Section III.A.

91. *See infra* Section III.A.

the telemedicine visit and the suppliers, pharmacies, or laboratories are also able to bill Medicare.

Second, CMS waived the restrictions on which types of medical providers could furnish telemedicine services.[92] Any provider who is eligible to bill Medicare may now furnish telemedicine services for the duration of the Public Health Emergency.[93] Much like the waiver of the geographic restrictions, this was necessary to expand access to telemedicine but also allows scamsters to target more providers to participate in fraud schemes. Third, Medicare will reimburse telemedicine visits at the same rate as regular, in-person visits.[94] The change in reimbursement is critical to incentivize providers to utilize telemedicine visits in lieu of in-person visits. At the same time, this also incentivizes disreputable telemedicine companies to increase the number of reimbursements for sham telemedicine visits because the sham visits are now worth more money. As mentioned previously, in some of the telemedicine scams the providers did not bill for the telemedicine visits.[95] Telemedicine was simply the mode for prescribing and ordering unnecessary durable medical equipment, genetic tests, and drugs. In those situations, parity is not a driver of the fraud.

Fourth, practitioners can provide telemedicine services to patients with whom they have no prior doctor-patient relationship.[96] This waiver probably

---

92. U.S. DEP'T OF HEALTH & HUM. SERVS., MEDICARE PAYMENT POLICIES DURING COVID-19 (2022), https://telehealth.hhs.gov/providers/billing-and-reimbursement/medicare-payment-policies-during-covid-19/ [https://perma.cc/3R3Q-BKZB].

93. *Id.*

94. CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 80. Prior to the PHE, "most telehealth services were paid at the lower PFS rate used to pay clinicians providing care in facilities (the facility-based rate), rather than the higher rate used to pay office-based clinicians (the nonfacility rate), because the practice expenses associated with furnishing telehealth services were presumed to be lower." 2021 REPORT TO CONGRESS, *supra* note 8, at xxvii.

95. *See supra* text accompanying notes 90–91.

96. On March 6, 2020, the Coronavirus Preparedness and Response Supplemental Appropriations Act, Pub. L. No. 116-123, 134 Stat. 146, 156 (2020), expanded access to telemedicine and defined "Qualified Provider" of telemedicine services as follows:

> (3) QUALIFIED PROVIDER.—The term 'qualified provider' means, with respect a telehealth service (as defined in paragraph (4)(F) of section 1834(m)) furnished to an individual, a physician or practitioner (as defined in paragraph (4)(D) or (4)(E), respectively, of such section) who—
>
> (A) furnished to such individual an item or service for which payment was made under title XVIII during the 3-year period ending on the date such telehealth service was furnished; or
>
> (B) is in the same practice (as determined by tax identification number) of a physician or practitioner (as so defined) who furnished such an item or service to such individual during such period.

Coronavirus Preparedness and Response Supplemental Appropriations Act, Pub. L. No. 116-123, § 102(a)(3), 134 Stat. 146, 156 (2020). Under this provision, Medicare would only cover telemedicine services if the treating physician or someone in her medical practice had a face-to-face appointment with that patient in the preceding three years. Essentially, this provision

poses the greatest fraud risk. If providers do not need to have a prior relationship with the patient, it is easier to solicit a wide range of Medicare beneficiaries and hold short telemedicine visits where the provider prescribes or orders durable medical equipment, drugs, and genetic tests without regard to medical necessity.

Fifth, OIG permitted health care providers to reduce or waive cost-sharing (coinsurance and deductibles) for telemedicine visits paid by federal health care programs without the threat of administrative sanctions.[97] Typically, a reduction or waiver of cost-sharing obligations would be considered an inducement for a referral in violation of the federal Anti-Kickback Statute ("AKS").[98] It could also be a violation of the civil monetary penalty and exclusion laws related to kickbacks[99] and the civil monetary penalty law prohibition on inducements to beneficiaries.[100] OIG noted, however, that they were not mandating that providers reduce or waive cost-sharing obligation for telemedicine services during the COVID-19 emergency.[101] Instead, OIG stated that it will not impose administrative sanctions when arrangements meet two conditions: "[(1)] A physician or other practitioner reduces or waives cost-sharing obligations (i.e., coinsurance and deductibles) that a beneficiary may owe for telehealth services furnished consistent with the then-applicable coverage and payment rules," and "[(2)] The telehealth services are furnished during the time period subject to the COVID-19 Declaration."[102] Further, OIG explained that nothing in the policy statement affects a provider's "responsibility to bill only for services performed and to comply with legal authorities related to proper billing, claims submission, cost reporting, or related conduct."[103] The policy changes apply to all covered "modalities,

---

prohibited reimbursement if there was not a preexisting doctor-patient relationship. Section 3703 of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) modified this earlier federal legislation by eliminating the definition of "Qualified Provider," which means that physicians can provide telemedicine services to new patients. Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136, div. A, tit. III, subtit. D, § 3703, 134 Stat. 281, 416 (2020).

97. CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 80; OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., OIG POLICY STATEMENT REGARDING PHYSICIANS AND OTHER PRACTITIONERS THAT REDUCE OR WAIVE AMOUNTS OWED BY FEDERAL HEALTH CARE PROGRAM BENEFICIARIES FOR TELEHEALTH SERVICES DURING THE 2019 NOVEL CORONAVIRUS (COVID-19) OUTBREAK 1 (2020) [hereinafter OIG POLICY STMT.], https://oig.hhs.gov/fraud/docs/alertsandbulletins/2020/policy-telehealth-2020.pdf [https://perma.cc/ZMG6-UNXR].

98. OIG POLICY STMT., *supra* note 97, at 1 (citing Social Security Act § 1128B(b), 42 U.S.C. § 1320a–7b(b)); *see infra* Section II.A.

99. *Id.* (citing Social Security Act §§ 1128(b)(7), 1128A(a)(7), 42 U.S.C. §§ 1320a–7(a)(7) to –7a(b)(7)).

100. *Id.*

101. *Id.* at 2.

102. *Id.* at 1.

103. *Id.* at 2.

including telehealth visits, virtual check-in services, e-visits, monthly remote care management, and monthly remote patient monitoring."[104]

Sixth, CMS waived some of the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[105] which limited the use of telemedicine services. HIPAA is a federal law that protects the privacy and security of patient information.[106] HHS issued regulations to implement the requirements of HIPAA. The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") addresses the use and disclosure of protected health information.[107] Protected health information includes "[*i*]*ndividually identifiable health information*,"[108] which is "held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral."[109] Therefore, when third parties electronically transmit protected health information to health care providers, the third party must comply with HIPAA's Privacy Rule.[110]

HIPAA's requirements apply to covered entities and their "business associates."[111] "A business associate is defined as any person who, on behalf of a covered entity, 'creates, receives, maintains, or transmits protected health

---

104. OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., FAQS—OIG POLICY STATEMENT REGARDING PHYSICIANS AND OTHER PRACTITIONERS THAT REDUCE OR WAIVE AMOUNTS OWED BY FEDERAL HEALTH CARE PROGRAM BENEFICIARIES FOR TELEHEALTH SERVICES DURING THE 2019 NOVEL CORONAVIRUS (COVID-19) OUTBREAK (2020), https://oig.hhs.gov/fraud/docs/alertsandbulletins/2020/telehealth-waiver-faq-2020.pdf [https://perma.cc/RHM8-XV2F].

105. *See generally* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in various sections of 42 U.S.C.).

106. *See generally id.* (setting forth HIPAA requirements). Indeed,

> HIPAA imposes obligations on health care providers and other "covered entities," including health plans and health clearinghouses, regarding their transmission of "protected health information". . . .
>
> Under HIPAA, health care providers must treat [protected health information] consistent with requirements set forth in several HHS regulations known as the "Privacy Rule," the "Security Rule," and the "Breach Notification Rule."

CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10490, HIPAA, TELEHEALTH, AND COVID-19, at 1 (2020).

107. U.S. DEP'T OF HEALTH & HUM. SERVS., OCR PRIVACY BRIEF: SUMMARY OF THE HIPAA PRIVACY RULE 1–3, 19 (2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/YS28-UGP8] (citing 45 C.F.R. § 160.103 (2022)).

108. *Id.* at 4. "Individually identifiable health information" includes information which relates to: (1) "the individual's past, present[,] or future physical or mental health or condition"; (2) "the provision of health care to the individual"; or (3) "the past, present, or future payment for the provision of health care." *Id.* The information is typically identifiable by "name, address, birth date, [or] Social Security Number." *Id.*

109. *Id.* at 3.

110. LINEBAUGH, *supra* note 106, at 3. Third parties that provide technological services to the health care providers must also comply with the Breach Notification Rule and the Security Rule. *Id.*

111. *Id.* at 2.

information' for a HIPAA-covered transaction."[112] Prior to sharing any protected health information, covered entities must "enter into a written contract," a business associate agreement, "that provides 'satisfactory assurances' the business associate will 'appropriately safeguard the information.'"[113] In addition, the business associate agreement must "'[e]stablish the permitted and required uses and disclosures of protected health information by the business associate,' and it may not authorize the business associate to use or further disclose the [protected health information] in a manner that, if done by a covered entity, would violate HIPAA's requirements."[114]

For purposes of telemedicine, the issue that arises involves the Privacy Rule's application to business associates. If a provider uses a video conferencing provider, the video conferencing provider (as a business associate) would have to comply with HIPAA's Privacy Rule because of the disclosure of protected health information between provider and patient during video conferencing services. In response to the COVID-19 pandemic, HHS Office for Civil Rights issued a Notice where it indicated that it is using "its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency."[115] The Notice permits health care providers to "use any [available] non-public facing remote communication product" to communicate with patients.[116] This includes popular applications, such as Zoom, Skype, Apple FaceTime, or Google Hangouts, that allow for video chats.[117] It does not

112. *Id.*

113. *Id.*

114. *Id.* (first alteration in original) (quoting 45 C.F.R. § 164.504(e)(2)(i) (2022)).

115. Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, 85 Fed. Reg. 22,024, 22,025 (Apr. 21, 2020) (to be codified at 42 C.F.R. pts. 160, 164).

116. *Id.* "A non-public facing remote communication product is one that, as a default, allows only the intended parties to participate in the communication." U.S. DEP'T OF HEALTH & HUM. SERVS., WHAT IS A "NON-PUBLIC FACING" REMOTE COMMUNICATION PRODUCT? (2020), https://www.hhs.gov/hipaa/for-professionals/faq/3024/what-is-a-non-public-facing-remote-communication-product/index.html [https://perma.cc/434E-FETH]. Typically, non-public facing communication platforms

> employ end-to-end encryption, which allows only an individual and the person with whom the individual is communicating to see what is transmitted. The platforms also support individual user accounts, logins, and passcodes to help limit access and verify participants. In addition, participants are able to assert some degree of control over particular capabilities, such as choosing to record or not record the communication or to mute or turn off the video or audio signal at any point.

*Id.*

117. Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, 85 Fed. Reg. at 22,025. HHS Office for Civil Rights explains that "[p]roviders are encouraged to notify patients that these third-

include, however, Facebook Live, Twitch, TikTok, or other video communication applications that are public facing.[118] The Notification also encourages health care providers to seek additional privacy protections by entering into business associate agreements[119] ("BAAs") with HIPAA compliant technology vendors.[120] It mentions several providers that will enter into HIPAA BAAs including Skype for Business, Zoom for Healthcare, and Cisco Webex Meetings.[121] These changes made it easier for health care providers to quickly pivot to providing telemedicine services without worrying about HHS Office for Civil Rights pursuing the provider for HIPAA violations. At the same time, however, these changes put patient information at risk. It is possible that medical records could be illegally shared with or stolen by third parties and could result in the use of patient information to obtain unwanted and unnecessary services.

All of these waivers were essential for the expanded use of telemedicine during the Public Health Emergency. Collectively, however, these provisions will likely contribute to telemedicine fraud. Once the Public Health Emergency expires, Medicare's pre-waiver rules will go back into effect unless lawmakers act to make some or all of the Public Health Emergency changes permanent. OIG Deputy Director Christi A. Grimm has recognized that expanding telemedicine access has offered "opportunities to increase access to services, decrease burdens for both patients and providers, and enable better care, including enhanced mental health care."[122] But she cautions that policies need to be designed to "achieve these goals and . . . not [be] compromised by fraud, abuse, or misuse."[123] Thus, it is imperative that the Government address issues concerning fraud when they consider the future of telemedicine regulation.

---

party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications." *Id.*

118. *Id.* Public facing remote communication products "are designed to be open to the public or allow wide or indiscriminate access to the communication." U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 116.

119. HIPAA's requirements apply to covered entities and their "business associates." LINEBAUGH, *supra* note 106, at 2. "A business associate is defined as any person who, on behalf of a covered entity, 'creates, receives, maintains, or transmits protected health information' for a HIPAA-covered transaction." *Id.* (quoting 45 C.F.R. § 160.103(1)(i) (2022)).

120. *See* Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, 85 Fed. Reg. at 22,025.

121. *Id.*

122. Press Release, Off. of Inspector Gen., U.S. Dep't of Health & Hum. Servs., Statement of Principal Deputy Inspector General Grimm on Telehealth (Feb. 26, 2021), https://oig.hhs.gov/coronavirus/letter-grimm-02262021.asp [https://perma.cc/9MJ2-3E6V].

123. *Id.*

## II. HEALTH CARE FRAUD AND DETECTION

Prior to the COVID-19 pandemic, the DOJ had already begun investigating and prosecuting telemedicine fraud. The surge in the use of telemedicine during COVID-19 will likely heighten the DOJ's focus on rooting out telemedicine fraud. This Part will focus on the Government's tools in the fight against telemedicine fraud. It will first analyze the civil and criminal statutes used in health care fraud cases and how they apply to telemedicine fraud cases. Next, it will examine the use of data analytics to detect health care fraud.

### *A. PRIMARY FRAUD STATUTES*

#### 1. Civil False Claims Act

One of the most important tools for rooting out health care fraud is the civil False Claims Act ("FCA").[124] In 2020, the DOJ recovered more than $2.2 billion in FCA settlements with over $1.8 billion related to health care fraud recoveries.[125] The FCA is prominent in health care fraud prosecutions because every time health care providers treat Medicare or Medicaid patients, they submit a claim to the Government for payment.[126] Thus, providers submit "large numbers of small claims, often amounting to thousands of claims over the course of a year."[127] In total, "Medicare . . . handles more than [one] billion claims per year."[128] The FCA allows the Government to recoup its losses for false or fraudulent claims made by health care providers. The FCA is violated whenever any person "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim."[129]

---

124. *See* 31 U.S.C. § 3729. The FCA was enacted in 1863 and "was originally aimed principally at stopping the massive frauds perpetrated by large contractors during the Civil War." United States v. Bornstein, 423 U.S. 303, 309–10 (1976). There is also a criminal False Claims Act, see 18 U.S.C. § 287, which makes it unlawful to knowingly present, or cause to be presented, false or fraudulent claims paid by the Government. *See id.* Criminal penalties include imprisonment up to five years and fines. *Id.*

125. HEALTH CARE FRAUD REPORT, *supra* note 10, at 8; Press Release, U.S. Dep't of Just., Justice Department Recovers Over $2.2 Billion from False Claims Act Cases in Fiscal Year 2020 (Jan. 14, 2021), https://www.justice.gov/opa/pr/justice-department-recovers-over-22-billion-false-claims-act-cases-fiscal-year-2020 [https://perma.cc/R5T6-BTT3].

126. In the health care fraud context, a claim is a request for payment for health care that is accompanied with the necessary information from the health care provider. 42 C.F.R. § 162.1101(a) (2022).

127. Timothy Stoltzfus Jost & Sharon L. Davies, *The Empire Strikes Back: A Critique of the Backlash Against Fraud and Abuse Enforcement*, 51 ALA. L. REV. 239, 247 (1999).

128. OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., 2021 TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING HHS 11 (2021), https://oig.hhs.gov/reports-and-publications/top-challenges/2021/2021-tmc.pdf#page=12 [https://perma.cc/H538-B9Y5].

129. 31 U.S.C. § 3729(a)(1)(A). Knowingly is defined under the statute and means that a person "has actual knowledge of the information," or "acts in deliberate ignorance" or a "reckless disregard of the truth or falsity of the information." *Id.* § 3729(b)(1). A claim means

Thus, liability is attached to the claim for payment rather than the underlying fraudulent activity. Any person who violates the FCA "is liable to the United States Government for a civil penalty of not less than [$12,537] and not more than [$25,076] . . . plus 3 times the amount of damages [(treble damages)] which the Government sustains because of the act of that person."[130]

The FCA is unique in that private citizens, known as "relators," can use their knowledge of a provider's fraud to bring *qui tam* suits in the name of the Government.[131] These whistleblowers are incentivized to bring suits because they are entitled to between fifteen and thirty percent of the recovery if the suit is successful.[132] The amount that relators receive depends on whether the Government decides to intervene in the lawsuit or allow the relator to pursue it and the extent of the relator's contribution to the prosecution.[133] Relators file the suit under seal and the Government has sixty days to determine whether to take over the case as its own or to leave the case to the relator to litigate.[134] If the DOJ intervenes in the case, it has primary responsibility for the prosecution of the case and can settle the action without the approval of the relator if "the . . . settlement is fair, adequate, and reasonable under all the circumstances."[135]

There are several types of FCA cases that one would expect to occur in the telemedicine context. First, there are claims under the FCA for billing for items or services not actually rendered.[136] Thus, the provider would submit a bill to Medicare or Medicaid that claims the health care provider performed services, such as a patient consultation, via telemedicine when in fact the health care provider did not furnish any services to the beneficiary. There may also be situations where technical difficulties during the telemedicine visit

---

> any request or demand . . . for money or property . . . that[:] (i) is presented to an officer, employee, or agent of the United States; or (ii) is made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a Government program or interest [and if the Government will provide or reimburse any portion of the money or property requested].

*Id.* § 3729(b)(2).

130. *Id.* § 3729(a)(1)(G); 28 C.F.R. § 85.5 (2022) (adjusting the penalty for violations of the FCA).

131. 31 U.S.C. § 3730(c).

132. *Id.* § 3730(d).

133. *Id.*

134. *Id.* § 3730(b)(2). If the Government has good cause, it can move the court for an extension of the 60-day time period. *Id.* § 3730(b)(3).

135. *Id.* § 3730(c)(1)–(2).

136. MED. LEARNING NETWORK, CTRS. FOR MEDICARE & MEDICAID SERVS., MEDICARE FRAUD & ABUSE: PREVENT, DETECT, REPORT 12 (2021), https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Fraud-Abuse-MLN4649244.pdf [https://perma.cc/7C36-3AZK].

prevent the health care provider from rendering services, but the provider still bills for those services.

Second, a provider might bill for medically unnecessary services or items provided.[137] Under federal law, Medicare Parts A and B will not pay for services unless those services are "reasonable and necessary for the diagnosis or treatment of illness or injury or to improve the functioning of a malformed body member."[138] Therefore, if a laboratory submits a claim for reimbursement for medically unnecessary laboratory tests, that is an actionable violation of the FCA. Most of the telemedicine scams discussed in this Article involve one or both of these first two types of FCA cases.

Third, DME providers may submit claims that were generated "pursuant to a prohibited telephone solicitation."[139] The Social Security Act only allows DME suppliers to make unsolicited phone calls in three specific situations: (1) The beneficiary gave written permission; (2) the supplier has provided a covered item to the individual and is only contacting the individual concerning that covered item; or (3) the supplier has furnished a covered item to the individual within the fifteen-month period preceding the contact.[140] If the DME supplier submits a claim in violation of the rule, no payment may be made for the covered item or service.[141] It is considered a false claim for purposes of the FCA.[142] DME suppliers have also violated the law by "us[ing] independent marketing firms to make unsolicited calls to Medicare beneficiaries."[143] All of the telemedicine scams involving DME suppliers utilize marketing firms to collect the beneficiary information needed for the billing scheme.

Fourth, telemedicine providers may submit bills for excessive services or items provided.[144] In this situation, the patient likely has some need for services or items, but not enough to justify the quantity of services or items billed by the telemedicine provider.

Fifth, providers might have coding errors or engage in upcoding.[145] Accurate coding is crucial in telemedicine because of all of the pre–Public Health Emergency reimbursement constraints on the type of provider, geographic location of patient, originating site, and type of service provided. The

137. *Id.*

138. 42 U.S.C. § 1395y(a)(1)(A).

139. OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., UPDATED SPECIAL FRAUD ALERT: TELEMARKETING BY DURABLE MEDICAL EQUIPMENT SUPPLIERS (2010), https://oig.hhs.gov/documents/special-fraud-alerts/868/fraudalert_telemarketing.pdf [https://perma.cc/NPG2-WTWM].

140. 42 U.S.C. § 1395m(a)(17)(A).

141. *Id.* § 1395m(a)(17)(B).

142. OFF. OF INSPECTOR GEN., *supra* note 139.

143. *Id.*

144. MED. LEARNING NETWORK, *supra* note 136, at 7.

145. *Id.*

reimbursement codes vary based on these and many other factors. "Upcoding is when a provider assigns an inaccurate billing code to a medical procedure or treatment to increase reimbursement."[146] For example, if a nurse conducts the telemedicine appointment, but the doctor's office submits the claim as if the doctor conducted the appointment because designating the doctor as the provider leads to a higher reimbursement, that would be upcoding.

Sixth, providers might unbundle a bill to submit separate claims for what was essentially one procedure or item.[147] For example, if a laboratory runs several tests on a patient's blood it should be submitted as one bill with a global billing code that encompasses the various tests, but the laboratory might claim that the tests were run on multiple days and submit separate bills that each contain a billing code for the applicable test. Although the global billing code for multiple tests would provide a higher reimbursement than the billing code for one test, it is less than would result from claiming each test separately.[148] Unbundling the bills in this manner allows the provider to claim a greater reimbursement for the service provided.

### 2. Anti-Kickback Statute

The Federal health care program AKS,[149] which is often at the forefront of criminal health care fraud enforcement efforts, was enacted to prevent

---

146. *Id.*

147. FED. BUREAU OF INVESTIGATION, HEALTH CARE FRAUD, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/health-care-fraud [https://perma.cc/WS32-EJSZ]; MED. LEARNING NETWORK, *supra* note 136, at 7.

148. LAURA F. LAEMMLE-WEIDENFELD, AM. HEALTH L. ASS'N, LEGAL ISSUES IN HEALTH CARE FRAUD AND ABUSE 435–36 (5th ed. 2020).

149. 42 U.S.C. § 1320a–7b(b). The Anti-Kickback statute provides:

> (b)(1) Whoever knowingly and willfully solicits or receives any remuneration (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in kind—
>
> (A) in return for referring an individual to a person for the furnishing or arranging for the furnishing of any item or service for which payment may be made in whole or in part under a Federal health care program, or
>
> (B) in return for purchasing, leasing, ordering, or arranging for or recommending purchasing, leasing, or ordering any good, facility, service, or item for which payment may be made in whole or in part under a Federal health care program,
>
> shall be guilty of a felony and upon conviction thereof, shall be fined not more than $100,000 or imprisoned for not more than five years, or both.
>
> (2) Whoever knowingly and willfully offers or pays any remuneration (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in kind to any person to induce such person—
>
> (A) to refer an individual to a person for the furnishing or arranging for the furnishing of any item or service for which payment may be made in whole or in part under a Federal health care program, or

payments to doctors in exchange for patient referrals to other health care providers.[150] The concern with these types of payments is that the health care provider may make care decisions based on financial incentives rather than the best interests of the patient.[151] There is also the concern that "financial rewards to providers for patient referrals might drive up [federal health care] program costs by encouraging the provision of unnecessary or inordinately expensive medical care."[152]

The AKS makes it unlawful to: (1) knowingly and willfully[153]; (2) offer or pay, solicit or receive; (3) any remuneration; (4) to induce the referral of an individual to another person or entity "for the furnishing of any item or service," or to induce the purchasing or ordering of such item or service; (5) payable "in whole or in part" by a federal health care program, such as Medicare and Medicaid.[154] As a criminal statute, intent is an essential element of an AKS violation. When evaluating intent, courts will often apply the one purpose test: If one purpose of the payment is to obtain referrals, then the requisite intent is established even if there may be other, legitimate reasons for the remuneration.[155] Remuneration is broadly defined as "anything of value."[156]

Criminal conviction under the AKS may lead to a criminal fine of up to $100,000 and/or up to ten years imprisonment, as well as mandatory exclusion from participation in Medicare and Medicaid (an administrative sanction).[157] Exclusion is the most powerful penalty because it can put an

---

> (B) to purchase, lease, order, or arrange for or recommend purchasing, leasing, or ordering any good, facility, service, or item for which payment may be made in whole or in part under a Federal health care program,
>
> shall be guilty of a felony and upon conviction thereof, shall be fined not more than $100,000 or imprisoned for not more than 10 years, or both.

*Id.*

150. *See id.*

151. BARRY R. FURROW, THOMAS L. GREANEY, SANDRA H. JOHNSON, TIMOTHY STOLTZFUS JOST & ROBERT L. SCHWARTZ, THE LAW OF HEALTH CARE ORGANIZATION AND FINANCE 707 (6th ed. 2008).

152. *Id.*

153. *Id.* Importantly, the Affordable Care Act explains that a defendant "need not have actual knowledge of . . . or specific intent to commit a violation of" the anti-kickback statute. The Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, §6402(f)(2), 124 Stat. 119, 1008 (codified as amended at 42 U.S.C. § 1320a–7b(h) (2010)).

154. 42 U.S.C. § 1320a–7b(b)(1) to –7b(b)(2).

155. United States v. Greber, 760 F.2d 68, 69 (3d Cir. 1985).

156. *See, e.g.*, United States *ex rel.* McDonough v. Symphony Diagnostic Servs., Inc., 36 F. Supp. 3d 773, 777–78 (S.D. Ohio 2014) (explaining that for purposes of the AKS, remuneration is "anything of value").

157. 42 U.S.C. § 1320a–7(a) to –7b(b).

entity out of business. Due to the risk of exclusion, many entities settle their cases with the Government.[158]

The language of the AKS is incredibly broad and criminalizes many potentially beneficial business practices and compensation arrangements.[159] Accordingly, AKS contains a number of statutory exceptions[160] and safe harbors[161] that designate commercial arrangements as legal that would otherwise violate the plain language of AKS.[162] If a provider engages in a transaction that satisfies all of the elements of a safe harbor provision, the Government will not prosecute the provider even if unlawful intent is present.[163]

The AKS is a criminal statute, but in addition to criminal liability, AKS allegations are also brought in conjunction with claims under the Civil Monetary Penalties Law[164] and the FCA.[165] There is no private right of action under the AKS, but whistleblowers can sue for AKS violations through the FCA.[166] The AKS violation means that the claims are considered "false" for purposes of the FCA even if the items or services were provided as claimed.[167] Together, these

158. *See generally* Katrice Bridges Copeland, *Enforcing Integrity*, 87 IND. L.J. 1033 (2012) ("By entering into these civil administrative settlements, the pharmaceutical manufacturers are able to avoid the collateral consequences of criminal conviction. Importantly, . . . the manufacturer will not be excluded from participation in federal health care programs."). These settlements are reached through Corporate Integrity Agreements, negotiated by OIG. *Id.* at 1042–44. The health care provider pays a fine, agrees to remedial measures such as hiring a compliance officer, and in exchange, OIG does not seek exclusion of the provider from participation in federal health care programs. *See* OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., CORPORATE INTEGRITY AGREEMENTS, https://oig.hhs.gov/compliance/corporate-integrity-agreements [https://perma.cc/4ZRM-AZAH].

159. LAEMMLE-WEIDENFELD, *supra* note 148, at 31 (explaining that "common arrangements [such] as joint ventures, space and equipment leases, discounts on goods and services, physician recruitment incentives, management and personal services contracts, physician practice acquisition, and even employment arrangements" must be examined in the context of AKS).

160. 42 U.S.C. § 1320a–7b(b)(3)(A)–(K).

161. 42 C.F.R. § 1001.952 (2022).

162. In 1987, Congress required HHS to create regulatory safe harbors. Medicare & Medicaid Patient & Program Protection Act of 1987, Pub. L. No. 100–93, 101 Stat. 680, 682, 697 (1987). Congress explained that "the breadth of [AKS] created uncertainty among health care providers as to which commercial arrangements are legitimate, and which are" prohibited. S. REP. NO. 100-109, pt. 3, at 27 (1987).

163. *See* Medicare and State Health Care Programs: Fraud and Abuse; Issuance of Advisory Opinions by the OIG, 62 Fed. Reg. 7350, 7351 (Feb. 19, 1997) (codified at 42 C.F.R. pt. 1008).

164. 42 U.S.C. § 1320a–7a. The Civil Monetary Penalties Law includes a prohibition against offering or transferring remuneration to a Medicare or state health care program beneficiary that a "person knows or should know is likely to influence" beneficiary selection of a "particular provider . . . for which payment may be made, in whole or in part" by Medicare or a state health care program. *Id.* § 1320a–7a(a)(5).

165. 31 U.S.C. §§ 3729–3733.

166. *See* 42 U.S.C. § 1320a–7b(g).

167. The Patient Protection and Affordable Care Act ("Affordable Care Act"), Pub. L. No. 111-148, § 6402(f)(1), 124 Stat. 119, 759 (2010), provided that "a claim that includes items or services resulting from a violation of [the AKS] constitutes a false or fraudulent claim" for purposes of the FCA. 42 U.S.C. § 1320a–7b(g).

laws and regulations have resulted in massive liabilities for many health care providers.[168]

Kickback exposure can arise in telemedicine cases whenever a telemedicine company offers laboratory services, DME, or prescriptions by affiliated providers. For example, if there is a financial relationship between the health care provider who orders orthotics and the DME supplier that fulfills the order, that could run afoul of the AKS. All of the telemedicine fraud schemes to date involve these types of kickbacks.[169] In kickback situations, it could be that the provider is furnishing a good or service that the provider would not have furnished but for the kickback because the service is unnecessary. It is also possible that the provider is furnishing a good or service that is necessary but, in the absence of a kickback, a competitor would provide the service. While the former appears more egregious because it will increase program costs and lead to overutilization, either situation will be enough to make out a false claim based on a violation of the AKS. The Government need not demonstrate patient harm or monetary loss to federal health care programs as a prerequisite to recovery under the AKS.[170]

### *B. FRAUD DETECTION*

The HHS OIG is responsible for the oversight of Medicare and Medicaid.[171] OIG conducts investigations into Medicare and Medicaid fraud, waste, and abuse.[172] OIG also imposes administrative sanctions on health care providers that have committed prohibited acts such as health care fraud.[173] Traditionally, OIG utilized a "pay-and-chase" model where they attempted to recover fraudulent claims after the Government paid them.[174] Increasingly, however, OIG is using predictive analytics[175] to identify fraudulent claims prior to payment.

---

168. LAEMMLE-WEIDENFELD, *supra* note 148, at 31–33 (providing examples of multimillion dollar settlements over the past 20 years such as Pfizer's 2009 settlement for $1 billion that was brought under the FCA for violations of the AKS).

169. *See, e.g.*, *supra* Section II.A.

170. OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., FRAUD & ABUSE LAWS, https://oig.hhs.gov/compliance/physician-education/fraud-abuse-laws [https://perma.cc/G9WT-VNBC].

171. Statement of Organization, Functions, and Delegations of Authority, 83 Fed. Reg. 55553, 55553–54 (Nov. 6, 2018).

172. OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., OFFICE OF INSPECTOR GENERAL 1 (2022), https://oig.hhs.gov/documents/root/1037/About-OIG-Fact-Sheet-June2022.pdf [https://perma.cc/TB9D-32XK].

173. *See* 42 U.S.C. § 1320a–7a (authorizing OIG to seek civil monetary penalties and exclusion from participation in federal health care programs for a variety of health care fraud violations).

174. U.S. GOV'T ACCOUNTABILITY OFF., GAO–13–104, MEDICARE FRAUD PREVENTION: CMS HAS IMPLEMENTED A PREDICTIVE ANALYTICS SYSTEM, BUT NEEDS TO DEFINE MEASURES TO DETERMINE ITS EFFECTIVENESS 5, 9–10 (2012), https://www.gao.gov/assets/gao-13-104.pdf [https://perma.cc/N4MV-CVBD].

175. Predictive analysis focuses on statistics to predict outcomes. *Id.*

Rooting out health care fraud has always been "a resource-intensive endeavor."[176] Indeed, every Medicare or Medicaid claim includes "dozens of pieces of information to regulators, including the patient's name and date of birth, the place and date of service, the current procedural terminology (CPT) code that describes the service provided, and the supporting diagnosis code."[177] The OIG uses the claims data proactively to identify patterns of fraud and reactively to corroborate or refute allegations of fraud.[178] OIG does this through data analytics which is "the process of examining data sets to draw conclusions and identify patterns about the information they contain."[179]

In 2011, CMS's Center for Program Integrity launched its Fraud Prevention System.[180] "The [Fraud Prevention System] uses predictive analytics—sophisticated mathematical and statistical algorithms and models—to identify suspicious behavior."[181] The Fraud Prevention System examines information from multiple Medicare and other data sources to predict fraudulent billing patterns or trends.[182] The Fraud Prediction System runs predictive models on all Medicare Part A and Part B fee-for-service claims prior to payment to identify suspicious billing patterns.[183] Once the system identifies suspicious activity, it "automatically generates and prioritizes leads for review and investigation."[184] Investigations of Fraud Prevention

176. Joan H. Krause, *Following the Money in Health Care Fraud: Reflections on a Modern-Day Yellow Brick Road*, 36 AM. J.L. & MED. 343, 348 (2010) (explaining that because reimbursement is based on proper documentation, it is possible "to hide wrongdoing within a complex set of documents or electronic communications").

177. Jason Mehta & Jennifer A. Short, *Big Data Makes Big Cases: How Data Analytics Is Shaping False Claims Act Enforcement*, 67 FED. LAW. 43, 43 (2020).

178. *Id.* at 43–44.

179. Julian L. André & Justin P. Murphy, *The Growing Role of Data Analytics in Healthcare Enforcement*, THE NAT'L L. REV (Jan. 15, 2022), https://www.natlawreview.com/article/growing-role-data-analytics-healthcare-enforcement [https://perma.cc/4J46-44H2].

180. CTRS. FOR MEDICARE & MEDICAID SERVS., U.S. DEP'T OF HEALTH & HUM. SERVS., REPORT TO CONGRESS FRAUD PREVENTION SYSTEM FIRST IMPLEMENTATION YEAR 1 (2012), https://www.cms.gov/About-CMS/Components/CPI/Widgets/Fraud_Prevention_System_Report_toCongress1stYear.pdf [https://perma.cc/UW9L-WJ3F].

181. *Id.* at 4.

182. *Id.*

183. *Id.* at 4, 42. There are three distinct categories of model that have varying levels of complexities. First, there are rule-based models, which are designed to identify potentially fraudulent claims and behaviors as well as target fraud that is related to specific services, such as DME suppliers. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 174, at 13. Second, there are anomaly-detection models which are designed to pinpoint abnormal provider patterns by analyzing "data collected over a period of time, and comparisons of those patterns to established behaviors that have been determined to be reasonable." *Id.* at 13–14. Third, there are predictive models, which are designed "to use historical data to identify patterns associated with fraud, and then use these data to identify certain potentially fraudulent behaviors when applied to current claims data." *Id.* at 14. Predictive models are the most complex because they "require detection of several patterns of behavior that individually may not be suspicious but, when conducted together, can indicate fraudulent activity." *Id.*

184. CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 180, at 5.

System leads may result in CMS taking a variety of administrative actions "including implementation of claims processing edits, claim denials, prepayment review, payment suspensions, revocation of Medicare billing privileges, and referral to law enforcement."[185]

The use of data analytics makes OIG less reliant on *qui tam* whistleblower complaints and has already led to a significant increase in the number of DOJ initiated FCA cases.[186] In 2020, the DOJ initiated more than twice as many health-care-related FCA cases than it did in 2019, resulting in the most DOJ initiated FCA cases on record.[187] The number of health care related *qui tam* FCA cases in 2020 remained relatively unchanged from 2019, with less than a one percent increase in the number of cases.[188]

## III. TELEMEDICINE FRAUD

Prior to the COVID-19 pandemic, federal health care fraud enforcement in the area of telemedicine was already on the rise. The Government's enforcement efforts have been directed at what they term "telefraud," which are scams that inappropriately leverage the reach of telemarketing schemes.[189] The schemes rely upon unscrupulous medical providers who conduct sham remote visits for the purpose of billing fraudulently for DME or genetic tests. The conspirators in the scams include telemedicine company executives, medical providers, marketers, and business owners who work collectively to trick hundreds of thousands of unsuspecting Medicare beneficiaries. The expansion of telemedicine coverage during the Public Health Emergency and the possibility that it will become permanent once the Public Health Emergency ends means that these types of scams could become more prevalent. This Part will explain how these scams work and discuss some of the most prominent takedowns of these scams in the past several years. It will also analyze the scams through the lens of the Fraud Triangle.

### *A. TELEMEDICINE SCAMS (TELEFRAUD)*

In most of the fraudulent schemes, either telemedicine executives or DME suppliers or laboratories have a relationship with a marketing company. The marketing company targets Medicare and Medicaid recipients through

185. *Id.* at 4–5.

186. André & Murphy, *supra* note 179.

187. U.S. DEP'T OF JUST., CIV. DIV., FRAUD STATISTICS – OVERVIEW: OCTOBER 1, 1986 – SEPTEMBER 30, 2020, https://www.justice.gov/opa/press-release/file/1354316/download [https://perma.cc/FE52-74T9].

188. *See id.* In 2020, there were 456 health-care-related *qui tam* cases compared to 117 DOJ initiated health-care-related FCA cases. *Id.* In 2019, there were 450 health-care-related *qui tam* cases compared to fifty-seven DOJ initiated health-care-related FCA cases compared to 450 *qui tam* cases. *Id.* Thus, the ratio of *qui tam* to DOJ initiated cases has gone from approximately eight to one to approximately four to one in the course of one year.

189. Press Release, Off. of Inspector Gen., *supra* note 122 (distinguishing telefraud from other telehealth fraud schemes).

call centers, direct mail, television ads, and internet pop-up ads.[190] The marketing company gathers Medicare or Medicaid information from the recipients.[191] At that point, the marketing company provides the information to the telemedicine company or the DME supplier or laboratory.[192] Health care providers who work for the telemedicine company then prepare orders or write prescriptions for unnecessary laboratory tests or DME such as knee braces.[193] The health care providers may have spoken with the beneficiaries briefly through a telemedicine visit or not at all.[194] The DME companies or laboratories then send the orthotic braces or perform tests on the beneficiary.[195] The DME companies or laboratories submit claims to Medicare for reimbursement.[196] The telemedicine company may or may not submit claims for reimbursement for the telemedicine consultation.[197] The DME companies or laboratories pay the telemedicine company,[198] and the telemedicine company pays the providers for writing the orders and prescriptions.[199] Either the telemedicine company or the DME companies or laboratories pay the marketing company.[200] Telemedicine allows the schemes to be conducted on a very large scale because in-person doctor visits are not necessary.

The "telefraud" schemes have been so prevalent that on July 20, 2022, OIG took the extraordinary step of issuing a Special Fraud Alert to warn practitioners of the danger of entering into arrangements with telemedicine companies.[201] In the Special Fraud Alert, OIG decries the use of kickbacks to recruit practitioners into fraudulent schemes that typically involve practitioners ordering medically unnecessary items and services for patients with whom they have "ha[d] limited, if any, interaction."[202] The Special Fraud Alert includes

190. OFF. OF INSPECTOR GEN., *supra* note 12.

191. *Id.*

192. *Id.*

193. *Id.*

194. *Id.*

195. *Id.*

196. *Id.*

197. *Id.*

198. *Id.*

199. *Id.*

200. *See id.*

201. SPECIAL FRAUD ALERT, *supra* note 18, at 1. From 1994 to 2022, OIG has only issued twelve Special Fraud Alerts, with some being updates to earlier Special Fraud Alerts. OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., SPECIAL FRAUD ALERTS, BULLETINS, AND OTHER GUIDANCE, https://oig.hhs.gov/compliance/alerts [https://perma.cc/4CJK-95XR].

202. SPECIAL FRAUD ALERT, *supra* note 18, at 1. OIG explains that:

> Such payments are sometimes described as payment per review, audit, consult, or assessment of medical charts. Telemedicine Companies often tell Practitioners that they do not need to contact the purported patient or that they only need speak to the purported patient by telephone. In addition, Practitioners are not given an opportunity to review the purported patient's real medical records. Furthermore,

an illustrative list of eight "suspect characteristics" of agreements between practitioners and telemedicine companies which could demonstrate "a heightened risk of fraud and abuse."[203] For example, they note that it is suspicious if the patients have been "recruited" by the telemedicine company or obtained through internet advertising.[204] Further, it is also suspicious if the telemedicine company is restricting the practitioner's treatment options by only furnishing a particular product or service such as genetic testing.[205] OIG was careful to note that the "Special Fraud Alert is not intended to discourage legitimate telehealth arrangements" and that many practitioners used telemedicine during the Public Health Emergency to provide appropriate treatment to their patients.[206]

---

> the Telemedicine Company may direct Practitioners to order or prescribe a preselected item or service, regardless of medical necessity or clinical appropriateness. In many cases, the Telemedicine Company sells the order or prescription generated by Practitioners to other individuals or entities that then fraudulently bill for the unnecessary items and services.

*Id.*

203. SPECIAL FRAUD ALERT, *supra* note 18, at 4–5. The eight suspicious characteristics include:

- The purported patients for whom the Practitioner orders or prescribes items or services were identified or recruited by the Telemedicine Company, telemarketing company, sales agent, recruiter, call center, health fair, and/or through internet, television or social media advertising for free or low out-of-pocket cost items or services.
- The Practitioner does not have sufficient contact with or information from the purported patient to meaningfully assess the medical necessity of the items or services ordered or prescribed.
- The Telemedicine Company compensates the Practitioner based on the volume of items or services ordered or prescribed, which may be characterized to the Practitioner as compensation based on the number of purported medical records that the Practitioner reviewed.
- The Telemedicine Company only furnishes items and services to Federal health care program beneficiaries and does not accept insurance from any other payor.
- The Telemedicine Company claims to only furnish items and services to individuals who are not Federal health care program beneficiaries but may in fact bill Federal health care programs.
- The Telemedicine Company only furnishes one product or a single class of products (e.g., durable medical equipment, genetic testing, diabetic supplies, or various prescription creams), potentially restricting a Practitioner's treating options to a predetermined course of treatment.
- The Telemedicine Company does not expect Practitioners (or another Practitioner) to follow up with purported patients nor does it provide Practitioners with the information required to follow up with purported patients (e.g., the Telemedicine Company does not require Practitioners to discuss genetic testing results with each purported patient).

*Id.* (footnotes omitted).

204. *Id.* at 4.

205. *Id.*

206. *Id.*

Several recent examples of scams uncovered by the DOJ demonstrate the magnitude of these schemes. On April 9, 2019, the DOJ announced charges against twenty-four defendants, including executives "of five telemedicine companies, the owners of dozens of . . . DME[] companies[,] and three licensed medical professionals, for their participation in health care fraud schemes" with over $1.2 billion in losses.[207] They called the takedown Operation Brace Yourself, and its focus was on DME companies paying bribes and kickbacks to medical professionals working with telemedicine companies to order unnecessary back, shoulder, wrist, and knee braces for Medicare beneficiaries.[208]

One of the defendants, who ultimately pled guilty to conspiracy to commit health care fraud and filing a false tax return, was Kelly Wolfe.[209] The case against Kelly Wolfe and her company, Regency, Inc., a DME billing and consulting company, began as a *qui tam* action by a former Regency employee.[210] Wolfe and Regency worked with a group of telemarketing companies owned by Patsy Truglia (who was also charged and pled guilty)[211] and a telemedicine company called Comprehensive Telcare as part of the scheme.[212] Wolfe and her co-conspirators used Regency to establish dozens of DME shell companies in the names of straw owners for Truglia with the purpose of spreading DME claims across several entities to evade Medicare scrutiny.[213] Truglia's telemarketing companies targeted Medicare beneficiaries and collected information about them.[214] Comprehensive Telcare then "utilized an internet-based platform that employed computer-programmed macros to create bogus supporting medical practitioner orders," which their medical providers signed electronically in exchange for bribes without any

207. Press Release, U.S. Dep't of Just., *supra* note 24.

208. *Id.*; U.S. FED. BUREAU OF INVESTIGATIONS, BILLION-DOLLAR MEDICARE FRAUD BUST (2019), https://www.fbi.gov/news/stories/billion-dollar-medicare-fraud-bust-040919 [https://perma.cc/Z7A5-QMV7].

209. Press Release, U.S. Dep't of Just., Florida Businesswoman Pleads Guilty to Criminal Health Care and Tax Fraud Charges and Agrees to $20.3 Million Civil False Claims Act Settlement (Feb. 4, 2021), https://www.justice.gov/opa/pr/florida-businesswoman-pleads-guilty-criminal-health-care-and-tax-fraud-charges-and-agrees-203 [https://perma.cc/F8PP-EU77].

210. *Id.*; Settlement Agreement at 2–13, United States *ex rel.* Albright v. Regency, Inc., No. 19-cv-00686 (M.D. Fla. Jan. 21, 2021).

211. Press Release, U.S. Dep't of Just., South Florida Man Sentenced to 15 Years for Consecutive Health Care Fraud Conspiracies (Feb. 2, 2022), https://www.justice.gov/usao-mdfl/pr/south-florida-man-sentenced-15-years-consecutive-health-care-fraud-conspiracies [https://perma.cc/WBV6-JHQK] (noting that a judge sentenced Truglia to fifteen years in prison and that he was also ordered to pay $18.3 million to the affected government health care programs).

212. Second Superseding Information at 1–14, United States v. Truglia, No. 20-cr-00058 (M.D. Fla. Oct. 4, 2021).

213. Plea Agreement at 31–32, United States v. Wolfe, No. 21-cr-00028 (M.D. Fla. Jan. 27, 2021); Plea Agreement at 22–23, *Truglia*, No. 8-20-cr-00058 (M.D. Fla. Oct. 4, 2021).

214. Plea Agreement, *Wolfe*, *supra* note 213, at 31–32; Plea Agreement, *Truglia*, *supra* note 213, at 22–23.

contact with Medicare beneficiaries.[215] The telemedicine vendor would then transmit signed DME orders to Regency and the other DME fronts.[216] Regency and the other DME fronts then billed Medicare for the unnecessary DME equipment in exchange for five percent of paid claims.[217] Wolfe and her co-conspirators "submitted well over $400 million in illegal DME claims to Medicare and the Civilian Health and Medical Program of the" Department of Veteran Affairs.[218] In addition to the criminal charges, Wolfe and her company have agreed to pay over $20.3 million for FCA violations.[219]

Later that same year, the DOJ announced indictments in Operation Double Helix, which involved a scheme where genetic testing laboratories paid illegal kickbacks and bribes to medical professionals working with telemedicine companies in exchange for ordering expensive and medically unnecessary cancer genetic tests.[220] The "defendants fraudulently billed Medicare more than $2.1 billion for these . . . tests."[221]

As part of Operation Double Helix, the DOJ indicted Jamie Simmons, owner of telemedicine company MedSymphony, LLC.[222] Through MedSymphony, Simmons supplied fraudulent orders for cancer genomic testing[223] to be used to support Medicare claims by three laboratories for Medicare beneficiaries supplied by two marketing companies.[224] The doctors' orders for cancer genomic testing were written by doctors working for MedSymphony, and Medicare only reimbursed for cancer genomic testing when (1) the beneficiary had cancer and (2) the beneficiary's treating physician determined that the testing was needed for the treatment of the beneficiary's cancer.[225] But the MedSymphony "doctors were not treating the beneficiaries for cancer or symptoms of cancer, did not use the test results in the treatment of the beneficiaries, had no physician-patient relationship or, at times, any contact with the beneficiaries, and did not conduct a proper

215. Plea Agreement, *Truglia*, *supra* note 213, at 22–24.

216. *Id.*; Plea Agreement, *Wolfe*, *supra* note 213, at 31–34.

217. Plea Agreement, *Wolfe*, *supra* note 213, at 34; Plea Agreement, *Truglia*, *supra* note 213, at 23.

218. Press Release, U.S. Dep't of Just, *supra* note 209.

219. Exhibit A Settlement Agreement at 4, Albright v. Regency, Inc., No. 19-cv-00686 (M.D. Fla. Feb. 19, 2021).

220. Press Release, U.S. Dep't of Just., 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 [https://perma.cc/X3WU-X7FJ].

221. *Id.*

222. Indictment at 8, United States v. Simmons, No. 19-cr-60273 (S.D. Fla. Sept. 27, 2019).

223. *Id.* at 6 ("Cancer genomic ("CGx") testing used DNA sequencing to detect mutations in genes that could indicate a higher risk of developing certain types of cancers in the future. CGx testing was not a method of diagnosing whether an individual presently had cancer.").

224. *Id.* at 8, 11.

225. *Id.* at 7.

telemedicine visit, and often never contacted the beneficiaries."[226] Along with his co-conspirators, Simmons caused the three laboratories to submit more than $56 million in claims for fraudulent cancer genomic tests.[227] Simmons pleaded guilty to one count of conspiracy to commit health care fraud[228] and was sentenced to thirty-five months imprisonment and ordered to pay over $2.5 million in restitution.[229]

In Fall 2020, the DOJ announced the largest health care fraud takedown in its history, which resulted in charges against 345 defendants who were responsible for $6 billion in losses.[230] The telemedicine portion of the takedown, Operation Rubber Stamp, was responsible for $4.5 billion in losses.[231]

As part of Operation Rubber Stamp, the DOJ charged two nurse practitioners with conspiracy to commit health care fraud for their involvement in telefraud. Mark Allen Hill, a nurse practitioner licensed in several states who was a Medicare provider, worked for a telemedicine company called Integrated Support Plus, Inc. ("Integrated").[232] As a nurse practitioner in the state of Montana, Hill was able to prescribe DME to patients without oversight by a licensed physician.[233] The DME providers had arrangements with telemarketing companies and telemedicine companies: They paid the telemarketing companies for a set number of completed brace orders signed by medical providers and paid the telemarketing companies a fixed price for each brace; then, the telemarketing companies would make and receive calls from Medicare beneficiaries and determine whether the beneficiaries were eligible to receive braces.[234] They would then obtain the needed medical information from the beneficiaries and fill out the brace prescriptions, and they would send the unsigned brace prescriptions and payment to Integrated to obtain a Medicare provider's signature.[235] Integrated paid Medicare providers, including Hill, to review and sign brace prescriptions.[236] Hill did "so regardless of medical necessity, in the absence of a pre-existing medical provider-patient relationship, without a physical examination, and frequently based solely on a short telephonic conversation" with the beneficiary or without any conversation with the beneficiary at

226. *Id.* at 11.

227. *Id.* at 12.

228. *See* Agreed Factual Basis for Guilty Plea at 3, *Simmons*, No. 19-cr-60273 (S.D. Fla. Feb. 28, 2020); Judgment in a Criminal Case at 1, *Simmons*, No. 19-cr-60273 (S.D. Fla. Oct. 27, 2020), ECF No. 54.

229. Judgment in a Criminal Case, *supra* note 228, at 1.

230. Press Release, U.S. Dep't of Just., *supra* note 16.

231. *Id.*

232. Indictment at 2, United States v. Hill, No. 20-cr-00067 (D. Mont. Sept. 3, 2020), ECF No. 4.

233. *Id.* at 4.

234. *Id.* at 7.

235. *Id.*

236. *Id.* at 7–8.

all.[237] The DME companies then submitted claims to Medicare using the signed brace prescriptions.[238] Neither Hill nor Integrated billed Medicare for the telemedicine consultations with beneficiaries.[239] Hill participated in this scheme from October 2017 until April 2019.[240] He signed roughly 7,097 brace orders.[241] The scheme led to the submission of over $10 million in false and fraudulent claims to Medicare.[242] After a guilty plea, Hill was sentenced to nine months in jail and three years of supervised release.[243] He was also ordered to pay over $5 million in restitution.[244]

On May 25, 2021, the DOJ announced an indictment in the first pandemic-related telemedicine takedown.[245] Leonel Palatnik, co-owner of Panda Conservation Group, LLC ("Panda"), a Texas company that owned and operated testing laboratories, was indicted "for his role in a $73 million conspiracy to defraud Medicare by paying kickbacks to a telemedicine company to arrange for doctors to authorize medically unnecessary genetic testing."[246] The DOJ explained that "[t]he scheme exploited temporary amendments to telehealth restrictions enacted during the COVID-19 pandemic that were intended to ensure access to care for Medicare beneficiaries."[247] For marketing purposes, Panda used the brand name the Health Awareness Project "to target Medicare beneficiaries interested in genetic testing and to obtain their insurance information and DNA material for testing at Panda's laboratories."[248] Palatnik then offered and paid kickbacks and bribes of $50,000 per month to Michael Stein, through his entity 1523 Holdings, LLC ("1523"), in exchange for Stein arranging for telemedicine providers to order genetic testing for the targeted Medicare beneficiaries.[249] Stein then referred the Panda-recruited patients to health care providers in exchange for them ordering medically unnecessary genetic testing.[250] The health care

237. *Id.* at 8.

238. *Id.* at 7.

239. *Id.* at 10.

240. *Id.* at 8–9.

241. Press Release, U.S. Dep't of Just., Nurse Practitioners Sentenced to Prison for Health Care Fraud (July 30, 2021), https://www.justice.gov/usao-mt/pr/nurse-practitioners-sentenced-prison-health-care-fraud [https://perma.cc/K5UT-W578].

242. Indictment, *supra* note 232, at 11.

243. Press Release, U.S. Dep't of Just., *supra* note 241.

244. *Id.*

245. *See* Indictment at 1, United States v. Stein, No. 21-20321 (S.D. Fla. May 25, 2021).

246. Press Release, U.S. Dep't of Just., Laboratory Owner Pleads Guilty to $73 Million Medicare Kickback Scheme (Sept. 1, 2021), https://www.justice.gov/opa/pr/laboratory-owner-pleads-guilty-73-million-medicare-kickback-scheme-0 [https://perma.cc/6MNA-U335]; Plea Agreement at 6–7, United States v. Palatnik, No. 21-cr-20321 (S.D. Fla. Aug. 31, 2021); Indictment at 12, *Stein*, No. 21-20321 (S.D. Fla. May 25, 2021).

247. Press Release, U.S. Dep't of Justice, *supra* note 246.

248. Agreed Factual Basis for Guilty Plea at 2, *Palatnik*, No. 21-cr-20321 (Aug. 31, 2021).

249. *Id.*

250. Indictment, *supra* note 245, at 10–11.

providers used the Medicare beneficiary information provided by Stein and Palatnik to have telemedicine consultations through Stein's companies and order genetic testing.[251] Oftentimes, the health care providers were not treating the beneficiaries for any specific medical condition, had no prior relationship with the beneficiaries, and did not use the results of the genetic tests in the treatment of the beneficiaries.[252] In many cases, the health care providers did not actually have telemedicine consultations with the beneficiaries.[253]

Unlike the pre-Public Health Emergency schemes, the health care providers billed Medicare $1 million for telemedicine consultations.[254] These claims were false under the law because they "were obtained through kickbacks and bribes, medically unnecessary, ineligible for reimbursement, and not provided as represented."[255] From April 1, 2020 to December 31, 2020, the Panda laboratories billed Medicare more than $90 million for genetic tests procured through kickbacks.[256] To conceal the scheme, Palatnik, Stein, and their co-conspirators executed a sham contract that provided payments of $50,000 per month from Panda to 1523 as "purported IT and consultation services."[257] On September 1, 2021, the DOJ announced that Leonel Palatnik pleaded guilty to one count of conspiracy to defraud the United States and "offer kickbacks and one count of paying a kickback" in violation of the AKS.[258] On November 9, 2021, Palatnik was sentenced to eighty-two months in prison and ordered to pay over $61 million in restitution.[259]

---

251. *Id.*

252. *Id.* at 10–12. The indictment explains that the health care providers who ordered the testing were required to certify that "I am the patient's treating physician and this order is based upon Medicare's requirement that the testing is not ordered for the purpose of screening but for the diagnosis and treatment of the patient's individual medical condition." *Id.* Medicare does not cover diagnostic testing that "[was] not reasonable and necessary for the diagnosis or treatment of illness or injury or to improve the functioning of a malformed body member." 42 U.S.C. § 1395y(a)(1)(A). Even if the diagnostic testing was necessary for the treatment of an illness, Medicare required that all "diagnostic laboratory tests . . . must be ordered by the physician who is treating the beneficiary, that is, the physician who furnishes a consultation or treats a beneficiary for a specific medical problem . . . . Tests not ordered by the physician who is treating the beneficiary are not reasonable and necessary." 42 C.F.R. § 410.32(a) (2022).

253. Indictment, *supra* note 245, at 11.

254. *Id.* at 12.

255. *Id.*; *see supra* Section II.A.

256. Agreed Factual Basis for Guilty Plea, *supra* note 248, at 3.

257. *Id.* at 2.

258. Press Release, U.S. Dep't of Just., *supra* note 246.

259. Press Release, U.S. Dep't of Just., Laboratory Owner Sentenced to 82 Months in Prison for COVID-19 Kickback Scheme (Nov. 9, 2021), https://www.justice.gov/opa/pr/laboratory-owner-sentenced-82-months-prison-covid-19-kickback-scheme [https://perma.cc/E8XC-FE3R]; OFF. OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUM. SERVS., SEMIANNUAL REPORT TO CONGRESS: OCTOBER 1, 2021–MARCH 31, 2022, at 13 (2022), https://oig.hhs.gov/reports-and-publications/archives/semiannual/2022/2022-spring-sar.pdf [https://perma.cc/ZH7G-HPZB].

In the pre-Public Health Emergency telemedicine schemes, the health care provider's ability to prescribe or order DME and laboratory tests via telemedicine facilitated the fraudulent conduct. In most of the cases, however, the telemedicine providers never billed for their consultations with the Medicare beneficiaries. The fraudsters probably believed that by not billing for the telemedicine consultations, they reduced their chance of getting caught since the telemedicine visits (to the extent they took place) were not in compliance with the strict reimbursement rules. Specifically, it is unlikely that the telemedicine visits complied with the geographic restrictions or originating site requirements and many of the consultations may have happened by phone which was not reimbursable prior to the Public Health Emergency. Telemedicine is only important in these billing schemes because the use of technology substantially increased the number of beneficiaries who could be drawn into the fraudulent billing in a short amount of time. Indeed, the billing scheme of sending unnecessary DME equipment to Medicare beneficiaries has been around for a long time.[260]

In the one scam that took place during the Public Health Emergency, however, the providers billed for the telemedicine consultations. The Public Health Emergency waivers removed the restrictions on reimbursement for telemedicine visits. Thus, the fraudsters were probably not concerned that submitting claims for the telemedicine consultations would reveal the fraud to the Government. Given the Public Health Emergency waivers, future telemedicine schemes will probably turn on the reimbursement rules in addition to or instead of kickbacks and the provision of unnecessary services.

### *B. EXPLAINING TELEMEDICINE SCAMS THROUGH THE FRAUD TRIANGLE*

There are innumerable factors that could motivate someone to engage in health care fraud. Most of the people who commit fraud, whether in the health care context or otherwise, are not career criminals.[261] Largely, the people who commit fraud are trusted employees. Some people commit white-collar crimes to maintain their social status. But it is particularly difficult to understand why someone engages in fraud when someone similarly situated

260. OFF. OF INSPECTOR GEN., *supra* note 139. *See, e.g.*, Press Release, U.S. Fed. Bureau of Investigation, Owner of Durable Medical Equipment Company and Two Others Convicted in $11 Million Health Care Fraud Scheme (Feb. 21, 2013), https://archives.fbi.gov/archives/sanantonio/press-releases/2013/owner-of-durable-medical-equipment-company-and-two-others-convicted-in-11-million-health-care-fraud-scheme [https://perma.cc/8ZPV-L4FJ] (explaining that the owners of the DME business admitted that they used marketers to obtain information about Medicare and Medicaid beneficiaries that they used to fraudulently bill Medicare and Medicaid for DME that was either never prescribed or was prescribed but never delivered and that they attempted to obtain referrals from doctors in exchange for gifts).

261. *See* Joe McGrath, *Why Do Good People Do Bad Things? A Multi-Level Analysis of Individual, Organizational, and Structural Causes of White-Collar Crime*, 43 SEATTLE U. L. REV. 525, 540–41 (2020) ("[Donald] Cressey's work demonstrated that . . . those engaged in wrongdoing will often be law abiding, as will their colleagues, but they rationalize or 'neutralize' their wrongdoing.").

does not. Perhaps the best way to explain the expected uptick in fraud in telemedicine is through the frame of the Fraud Triangle. The Fraud Triangle theory is used to describe why some individuals in positions of trust commit occupational fraud.

The origins of the theory trace back to the 1950s when American criminologist Donald Cressey developed a three-pronged theory to explain why some people in positions of trust commit embezzlement while others do not.[262] Under his theory, the three factors common to the embezzlers were: (1) a non-shareable financial problem;[263] (2) an opportunity for trust violation;[264] and (3) rationalization of the planned violation.[265] Cressey believed that all three elements were required for someone to violate a position of trust and commit embezzlement.[266] Although Cressey's theory

---

262. Leandra Lederman, *The Fraud Triangle and Tax Evasion*, 106 IOWA L. REV. 1153, 1155–57 (2021) (explaining that the theory originated from Cressey's work on embezzlement). Cressey explained:

> Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware that this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their conduct in that situation verbalizations which enable them to adjust their conceptions of themselves . . . as users of the entrusted funds or property.

DONALD CRESSEY, OTHER PEOPLE'S MONEY: A STUDY IN THE SOCIAL PSYCHOLOGY OF EMBEZZLEMENT 30 (Patterson Smith Publishing Corp. ed. 1973) (1953).

263. CRESSEY, *supra* note 262, at 30. Cressey referred to five general types of non-shareable problems: (1) violation of ascribed obligations; (2) problems resulting from personal failure; (3) problems resulting from business reversals (such as economic depression); (4) problems related to status-gaining; and (5) problems resulting from employer-employee relations (such as feeling underpaid or overworked). *Id.* at 33–76. Cressey emphasized, however, that "the . . . types of non-shareable problems are not discrete." *Id.* at 66. He explained that the common denominator was that:

> [B]ecause of activity prior to the defalcation, the approval of groups important to the trusted person had been lost, or a distinct feeling that present group approval would be lost if certain activity were revealed, with the result that the trusted person was effectively isolated from persons who could assist him in solving problems arising from that activity.

*Id.*

264. *Id.* at 30. In describing an opportunity for a trust violation, Cressey explained that "the trust violator must have a certain amount of knowledge or information about trust violation in general, and specifically he must be aware that the violation of his trust will aid in the solution of the problem." *Id.* at 91.

265. *Id.* at 30–34. Cressey explained that through rationalization, "the potential trust violator identifies the possibilities for resolving the problem by violating his position of trust and defines the relationship between the non-shareable problem and the illegal solution in language which enables him to look upon trust violation (a) as essentially non-criminal" (borrowing the money rather than stealing it), "(b) as justified, or (c) as a part of a general irresponsibility for which he is not completely accountable." *Id.* at 93.

266. *Id.* at 31 ("[T]he presence of a non-sharable financial problem will not in itself guarantee that the behavior in question will follow. The entire process must be present."). Cressey explained "that the ideas inherent in these three types of expressions are not discrete and that

faced some criticism,[267] the accounting community embraced the theory and adapted it over time to explain occupational fraud. The three factors have evolved over time and now include: (1) incentives or pressure to commit fraud; (2) a perceived opportunity; and (3) rationalization of the act.[268]

The first factor—incentives or pressure to commit fraud—is the motivation for the crime.[269] It is generally understood to be financial in nature. The individual may have a personal financial problem, such as credit card or gambling debt, or a professional financial problem, such as an unattainable sales goal, that she cannot solve through legitimate means. The inability to solve the financial problem through legitimate means, leads the person to consider fixing the problem through illegal means.

The second factor—perceived opportunity—is the individual's belief that she has the ability to override internal controls, meaning the measures the company put in place to prevent or detect fraud.[270] Thus, the individual believes that she can use her position of trust to capture the incentive or solve her financial problem without being caught. The third factor—rationalization of the act—is how the individual, who does not consider herself to be a criminal, justifies the crime.[271] Thus, the individual may say that she committed a victimless crime or that she was entitled to the money due to mistreatment by the employer.

As Professor Leandra Lederman has explained:

> Generally speaking, the triangle's first two factors—incentive or pressure and perceived opportunity—may be thought of as in line with the deterrence model, while the third factor—rationalization—accords with behavioral theories of compliance. While increasing compliance norms may help limit convenient rationalizations for cheating (and likely more so than good-government measures) structural systems constrain the opportunity to evade. In addition, enforcement actions reduce the incentive and opportunity to cheat, while buttressing compliance norms. The fraud triangle thus provides a useful frame for showing how traditional economic and behavioral theories can work together.[272]

In telemedicine, the financial incentive to engage in fraud is tremendous. Through telemedicine, providers can justify a greater volume of billing for

---

the theory which we are presenting is in reference to a *process*[,] the result of which is a trust violation." *Id.* at 34.

267. Lederman, *supra* note 262, at 1158–66 (summarizing the methodology of Cressey's study and the common critiques of his work).

268. *Id.* at 1156–57 (tracing the evolution of the theory and noting that the American Institute of Certified Public Accountants ("AICPA") adopted these standards in the early 2000s).

269. *Id.* at 1159–61.

270. *Id.*

271. *Id.*

272. *Id.* at 1207.

products and services because in-person consultations are unnecessary.[273] They use telemarketers to target thousands of Medicare patients and submit reimbursements, and prior to the Public Health Emergency, fraudsters used telemedicine to further their DME or laboratory testing schemes.[274] With the Public Health Emergency waivers, however, individuals stand to gain millions from sham telemedicine visits in addition to their DME or laboratory testing schemes. In terms of perceived pressure, individuals could be living beyond their means, have large expenses or personal debt, or have a gambling or drug addiction.

With respect to opportunity, individuals may believe that the control on Medicare and other payment systems is ineffective. Thus, they believe that the chance of getting caught is low.[275] Historically, there has been a low chance of getting caught prior to payment because OIG relied on a pay-and-chase model of fraud enforcement.[276] The chance of getting caught prior to payment has increased with the use of data analytics but individuals considering fraud may not accurately perceive that shift. Individuals may also think that they have a great chance of getting away with telemedicine fraud because it is not on the Government's radar. Prior to 2019, there had not been any DOJ press releases announcing charges in telemedicine cases.[277] Since that time, there have been several announcements of indictments which indicate that telemedicine fraud has been on the DOJ's radar since 2016 if not earlier.[278] Despite the uptick in enforcement, the expansion of access to telemedicine during the pandemic combined with the relaxation of HIPAA and shared payment rules (aimed at preventing fraud), may convince individuals that they have a new or greater opportunity to commit telemedicine fraud without getting caught. They may wrongly believe that the pandemic will distract the Government from focusing on enforcement activities.

Telemedicine fraudsters may seek to rationalize their conduct by claiming that they are committing a victimless crime.[279] Because health care providers, telemedicine companies, and suppliers that commit this type of fraud do not have pre-existing relationships with Medicare beneficiaries, it is easier to see this as a victimless crime.[280] In justifying their behavior, fraudsters do not consider that taking public funds for private gain takes the funds away from essential services. They do not consider the faceless government a victim. Nor do they consider the impact on beneficiaries who may be billed for services that they did not request or face annual or lifetime

273. *Id.*
274. *See* OFF. OF INSPECTOR GEN., *supra* note 12.
275. Lederman, *supra* note 262, at 1159–61.
276. *See supra* note 174 and accompanying text.
277. *See supra* Section III.A.
278. *See supra* Section III.A.
279. *See supra* note 271 and accompanying text.
280. OFF. OF INSPECTOR GEN., *supra* note 12.

limits on coverage due to fraudulent claims for services that they did not request and/or receive.

The change in telemedicine rules during the Public Health Emergency and the likelihood that some or all of the waivers will remain in place after the Public Health Emergency ends has created the perfect storm for fraud to flourish. Individuals will perceive a greater incentive to commit telemedicine fraud because more money is potentially at stake due to the expansion of access to telemedicine services. They may also believe that they have a greater opportunity to commit fraud because they perceive a low possibility of getting caught due to lax enforcement. Finally, they likely do not believe that their fraudulent activity hurts anyone.

Although telemedicine has been critical to increase access to care during the pandemic, the billions of dollars involved in these telemedicine scams demonstrate that telemedicine poses serious program integrity risks. These large-scale frauds will increase the volume of telemedicine visits which will likely lead to increased costs. In addition, they expose both inappropriate telemedicine practices and financial relationships between providers. This fraud threatens the funds available for legitimate medical needs. It is crucial that these risks be addressed prior to the permanent expansion of telemedicine. The Fraud Triangle will help in assessing whether potential regulations of telemedicine will both prevent fraud and preserve access to care.

## IV. BALANCING FRAUD PREVENTION WITH ACCESS TO CARE

The goals of telemedicine are diametrically opposed to the goals of rooting out health care fraud. Telemedicine is clearly aimed at increasing access to health care services. And, as Professor Dayna Bowen Matthew has stated, "[c]ost containment, not universal access, is the objective of the war on health[]care fraud."[281] Access to health care is a critical issue in the United States. As of 2021, there are more than six-thousand primary care Health Professional Shortage Areas.[282] Rural, economically depressed, and underserved areas face health care provider shortages and have some of the greatest health care needs.[283] Further, "rural residents or urban residents in health[]care

281. Dayna Bowen Matthew, *An Economic Model to Analyze the Impact of False Claims Act Cases on Access to Healthcare for the Elderly, Disabled, Rural and Inner-City Poor*, 27 AM. J.L. & MED. 439, 440 (2001).

282. U.S. DEP'T OF HEALTH & HUM. SERVS., HEALTH WORKFORCE STRATEGIC PLAN 2021, at 12 (2021), https://bhw.hrsa.gov/sites/default/files/bureau-health-workforce/about-us/hhs-health-workforce-strategic-plan-2021.pdf [https://perma.cc/JG24-BGVV].

283. *Id.*

> For example, rural residents tend to have lower life expectancy levels than their urban counterparts, and the per capita availability of primary care physicians to serve rural residents is roughly 19 percent lower than in urban areas. Economically depressed and other underserved areas also face greater challenges in recruiting and retaining health care providers. The COVID-19 pandemic has exacerbated these challenges. Americans in underserved areas may be at higher risk of severe illness from COVID-

access 'deserts' often must travel long distances to access clinical specialists."[284] When access to care is unavailable, it can lead to poor health outcomes.

In crafting policies to prevent health care fraud in telemedicine, we must balance "access to essential health care services" "while ensuring taxpayer dollars are not lost to fraud, waste, and abuse."[285] While it is not year clear what restrictions may end up applying to reimbursement for telemedicine services, telemedicine is here to stay. As such, we must consider the best way to maintain program integrity in this transformed health care delivery landscape.

The large-scale telemedicine scams discussed in the previous Part largely involve kickbacks and billing for medically unnecessary treatment, services, or supplies, and the criminal conduct in those schemes falls squarely in the purview of the AKS and FCA.[286] Thus, once the fraudulent schemes are identified through either data analytics or whistleblower complaints and investigated, the existing health care fraud and abuse laws are sufficiently capacious to address the criminality involved. Therefore, the challenge is not creating a new criminal statute to deal with a unique enforcement problem. Instead, we must find ways to prevent or identify these telemedicine scams prior to payment and the resultant loss to the Government. The best way to ensure program integrity is to prevent fraud before it occurs. It is less expensive to prevent fraud than to detect, investigate, and prosecute it.

This Part will examine preventative measures that the Government could implement to address the problem of telemedicine fraud. It will scrutinize potential limitations on the use of telemedicine, such as prohibiting reimbursement for DME, prescriptions, or laboratory tests in the absence of a pre-existing doctor-patient relationship and limiting reimbursement to providers participating in certain value-based reimbursement plans. It will also assess the use of the Medicare enrollment and reimbursement process to prevent or identify fraudulent activity. This Part concludes that the Government should employ an approach that limits the opportunity to commit fraud and maximizes access to care through telemedicine. Ideally, such an approach should be put into place prior to permanent waiver of any of the pre–Public Health Emergency restrictions on telemedicine.

### *A. PRIOR DOCTOR-PATIENT RELATIONSHIP*

Perhaps the most difficult issue to resolve in crafting anti-fraud regulations for telemedicine is whether to require a pre-existing doctor-patient relationship prior to treatment. According to the American Medical Association, "[a] patient-

> 19, rural health care infrastructure is limited, and rural residents or urban residents in health[]care access "deserts" often must travel long distances to access clinical specialists.

*Id.* (footnotes omitted).

284. *Id.*

285. *Id.*; CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 180, at 1.

286. *See supra* Section II.A.

physician relationship exists when a physician serves a patient's medical needs. Generally, the relationship is entered into by mutual consent between physician and patient (or surrogate)."[287] More specifically, "a patient-physician relationship is generally formed when a physician affirmatively acts in a patient's case by examining, diagnosing, treating, or agreeing to do so."[288] There is no question that telemedicine visits can be helpful to reinforce the doctor-patient relationship because in many situations patients would prefer to have a telemedicine appointment with their regular doctor rather than traveling to urgent care or the emergency room where they would encounter a doctor with whom they have no prior relationship. Thus, telemedicine appointments can further continuity of care. The key question, however, is whether that pre-existing relationship can be established through a telemedicine visit. This dilemma, more than any other, illustrates how the best measures to eliminate health care fraud can fly in the face of the goals of telemedicine.

One of the key reasons that the large-scale fraudulent schemes are successful is because telemarketers can call people with whom they have no prior association, initiate sham telemedicine visits, and direct them to get tests at certain labs, prescriptions from certain pharmacies, or equipment from particular DME providers and then their partner labs, pharmacies, and DME providers bill Medicare. The easiest way to stop this type of fraud is to require a prior doctor-patient relationship with the doctor requesting laboratory tests or writing prescriptions for drugs or DME. Prior to the COVID-19 pandemic, the American Medical Association's position was that "[a] patient-physician relationship should ideally be established before the provision of services via telehealth."[289] If a prior doctor-patient relationship is required, the Medicare

---

287. *Patient-Physician Relationships: Code of Medical Ethics Opinion 1.1.1*, AM. MED. ASS'N, https://www.ama-assn.org/delivering-care/ethics/patient-physician-relationships [https://perma.cc/DJ8D-CPBY].

288. Valarie Blake, *When Is a Patient-Physician Relationship Established?*, 14 AM. MED. ASS'N J. ETHICS 403, 404 (2012) (citing case law to establish that the relationship begins once the physician has agreed to treat the patient).

289. ADVOC. RES. CTR., AM. MED. ASS'N, ISSUE BRIEF: STATE TELEHEALTH POLICIES TO ENSURE ACCESS TO HIGH-QUALITY CARE 2 (2021), https://www.ama-assn.org/system/files/202012/issue-brief-state-telehealth-policies.pdf [https://perma.cc/9KB5-VC76]. This relationship can

> be established . . . through: (i) A face-to-face examination, if a face-to-face encounter would otherwise be required in the provision of the same service not delivered via telemedicine; or (ii) A consultation with another physician who has an ongoing patient-physician relationship with the patient. The physician who has established a valid physician-patient relationship must agree to supervise the patient's care; or (iii) Meeting standards of establishing a patient-physician relationship included as part of evidence-based clinical practice guidelines on telemedicine developed by major medical specialty societies, such as those of radiology and pathology. Exceptions include on-call, cross coverage situations; emergency medical treatment; and other exceptions that become recognized as meeting or improving the standard of care.

Administrative Contractors, that process Medicare Part A/B medical and DME claims, could utilize data analytics to sift through prior claims data and detect that the patient had no prior relationship with the doctor.[290] Thus, the Medicare Administrative Contractors would be able to detect the sham claims before paying them.

There is no question, however, that requiring a pre-existing doctor-patient relationship would run counter to the goal of making doctors more accessible, especially to people in rural or underserved areas. It would also harm patients, such as those seeking medication abortion, whose first encounter with the doctor would likely be at the time the patient is seeking the medication.[291] The potential harm to patients would increase if there were also a requirement that the doctor-patient relationship be established during a face-to-face encounter prior to a telemedicine visit. For example, patients may have a difficult time traveling to meet the doctor if they do not own a car or cannot afford transportation to the doctor's office. In addition, this may cause patients to delay care which could further worsen their medical conditions. The doctor-patient relationship is built on trust and a commitment of care between the doctor and the patient. There is nothing inherent about a telemedicine visit that would make it unable to fulfill the AMA's or an individual state's requirements for a doctor-patient relationship. Indeed, all states allow doctors and patients to establish a new doctor-patient relationship through telemedicine.[292]

---

ADVOC. RES. CTR., AM. MED. ASS'N, 50-STATE SURVEY: ESTABLISHMENT OF A PATIENT-PHYSICIAN RELATIONSHIP VIA TELEMEDICINE 1 (2018), https://www.ama-assn.org/system/files/2018-10/ama-chart-telemedicine-patient-physician-relationship.pdf [https://perma.cc/X3BA-MX48].

290. "The Medicare Administrative Contractors (MACs) shall analyze claims to determine provider compliance with Medicare coverage, coding, and billing rules and take appropriate corrective action when providers are found to be non-compliant. . . . The priority for MACs is to minimize potential future losses to the Medicare Trust Funds through targeted claims review while using resources efficiently and treating providers and beneficiaries fairly." CTRS. FOR MEDICARE & MEDICAID SERVS., MEDICARE PROGRAM INTEGRITY MANUAL, ch. 3, § 3.1 (2021), https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/pim83c03.pdf [https://perma.cc/24KE-JFGX].

291. *See* Amrutha Ramaswamy, Gabriela Weigel, Laurie Sobel & Alina Salganicoff, *Medication Abortion and Telemedicine: Innovations and Barriers During the COVID-19 Emergency*, KAISER FAM. FOUND. (June 16, 2021), https://www.kff.org/policy-watch/medication-abortion-telemedicine-innovations-and-barriers-during-the-covid-19-emergency [https://perma.cc/X5VZ-JSXT]. "Medication abortion, also known as medical abortion or abortion with pills, is a pregnancy termination protocol that involves taking two different drugs, Mifepristone and Misoprostol, that can be safely used up to the first 70 days (10 weeks) of pregnancy." *The Availability and Use of Medication Abortion*, KAISER FAM. FOUND. (Apr. 6, 2022), https://www.kff.org/womens-health-policy/fact-sheet/the-availability-and-use-of-medication-abortion [https://perma.cc/S5EA-XD5Y]. Mifepristone is not available at retail pharmacies. *Id.* It can only be obtained directly from a certified medical provider because the FDA requires a Risk Evaluation and Mitigation Strategy to ensure the benefits of the drug outweigh the risks. *Id.* Telemedicine could help to expand access to medication abortion, but many states have taken action to block the use of telemedicine for abortion. *Id.*

292. *See supra* note 289 and accompanying text.

Not surprisingly, the American Telemedicine Association ("ATA") is opposed to requiring prior in-person consults for telemedicine visits.[293] The ATA argues that "[t]here is no clinical evidence for an arbitrary in-person requirement before a patient can access telehealth services."[294] Citing the Federation of State Medical Boards,[295] the ATA maintains that a doctor/patient relationship can be established via a telemedicine visit.[296] Indeed, the Federation of State Medical Boards explains, "[w]here an existing physician-patient relationship is not present, a physician must take appropriate steps to establish a physician-patient relationship[,] . . . and . . . such physician-patient relationships may be established using telemedicine technologies provided the standard of care is met."[297] Similarly, the American Medical Association now argues that there should be some flexibility in how the doctor-patient relationship is established. The American Medical Association states, "for new patients, a relationship can be established via telehealth if it meets the standard of care, including via real-time audio/video."[298]

---

293. AM. TELEMEDICINE ASS'N, PROGRAM INTEGRITY OVERVIEW 2 (2021), https://www.americantelemed.org/wp-content/uploads/2021/03/ATA-Program-Integrity-One-Pager-3-1-21.pdf [https://perma.cc/8KBD-X9U7] ("The ATA would consider additional guardrails for telehealth, specifically as proposed by the OIG, that do not require prior in-person consults, limit access to any modality including audio-only, or otherwise create barriers to patients seeking legitimate and needed care.").

294. AM. TELEMEDICINE ASS'N, OVERVIEW OF THE IN-PERSON REQUIREMENTS 1, https://www.americantelemed.org/wp-content/uploads/2021/06/ATA-Overview-of-In-Person-Requirements-1.pdf [https://perma.cc/HJ63-26XG] (discussing the requirement of an in-person visit six months prior to a Medicare-reimbursed mental health telemedicine visit in the Consolidated Appropriations Act, Pub. L. No. 116-260, div. CC, tit. I, subtit. B, § 123, 134 Stat. 1182, 2956–57 (2020) (codified at 42 U.S.C. § 1395m(m)(7) (2020))).

295. The Federation of State Medical Boards ("FSMB") serves as the primary center for collection, maintenance, and reporting of disciplinary actions taken against physicians by its member boards and other governmental authorities. *About FSMB*, FED'N OF STATE MED. BDS. (2018), https://www.fsmb.org/about-fsmb [https://perma.cc/REV8-JVTE]. Disciplinary actions are reported to the FSMB by state licensing and disciplinary boards, Canadian licensing authorities, the U.S. armed forces, the U.S. Department of Health and Human Services, and the Education Commission for Foreign Medical Graduates. *See id.*

FSMB's membership is composed of the medical boards of all states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, and includes separate osteopathic boards in the United States. *Membership Information*, FED'N OF STATE MED. BDS. (2018), https://www.fsmb.org/about-fsmb/fsmb-member-medical-boards [https://perma.cc/ELU6-C69C].

296. *See generally* AM. TELEMEDICINE ASS'N, *supra* note 294 (discussing in person requirements of establishing the physician-patient relationship).

297. FED'N OF STATE MED. BDS., MODEL POLICY FOR THE APPROPRIATE USE OF TELEMEDICINE TECHNOLOGIES IN THE PRACTICE OF MEDICINE 5 (2014), https://www.akleg.gov/basis/get_documents.asp?session=29&docid=63635 [https://perma.cc/LG8K-PR7C].

298. ADVOC. RES. CTR., *supra* note 289, at 2. It should be noted, however, that prior to the COVID-19 pandemic, the AMA's position was that a doctor-patient relationship must be established via a face-to-face encounter prior to the provision of telemedicine services. *Coverage of and Payment for Telemedicine H-480.946*, AM. MED. ASS'N (2022), https://policysearch.ama-assn.org/policyfinder/detail/telemedicine?uri=%2FAMADoc%2FHOD.xml-0-4347.xml [https://perma.cc/3DJE-A5W5].

Even if we permit the establishment of the doctor-patient relationship via telemedicine, that is not the end of the inquiry. The question becomes whether, for purposes of fraud prevention, different rules should apply when a health care provider is ordering laboratory tests or prescribing medication or DME via telemedicine. In its March 2021 report to Congress, the Medicare Payment Advisory Commission recommended that clinicians be required to provide a face-to-face, in-person visit on the date that the clinician "order[s] a high-cost DME product or a high cost lab test for that beneficiary or within six months before such date."[299] The Medicare Payment Advisory Committee explained that this "would help ensure that a beneficiary needs a product or test based on a needs assessment conducted by a clinician before Medicare pays for it."[300]

If health care fraud were the sole concern, then it would be easy to make the case that there should be a pre-existing doctor-patient relationship that was established during a face-to-face interaction before the provision of telemedicine services where a doctor prescribes drugs or DME or orders a laboratory test. Such a rule could potentially eliminate the large-scale scams. In terms of the fraud triangle, this rule would not lessen the perceived pressure that motivates the misconduct whether that pressure be personal, employment stress, or external. It would, however, lessen the opportunity to commit fraud and greatly increase the likelihood of detection through data analytics. The imposition of in-person visits would also make it more difficult for a provider to rationalize the misconduct by telling herself that the crime is victimless. The provider would no longer be defrauding faceless people with whom she has no prior association.

But health care fraud is not the only concern here. There must be a balancing of interests between fraud prevention and access to care. Access to care is hurt by a rule that requires an in-person visit prior to the prescription or ordering of drugs, DME, and laboratory tests. Beneficiaries in underserved communities may not be able to obtain needed DME or laboratory tests as a result of this rule. They may be incapable of establishing a doctor-patient relationship in person due to the shortage of providers where they live and the need to travel long distances for appointments. Studies have shown that the use of telemedicine during the COVID-19 pandemic was effective at reducing disparities in care.[301] It would be short-sighted to take actions that would undo those needed gains. Until we do more to recruit and train health professionals in rural and underserved areas, rules that limit access to care for the purpose of ending fraud may do more harm than good. Lawmakers need to think carefully about these types of limitations and whether it makes sense to carve out an exception to the limitation for rural and underserved areas.

299. 2021 REPORT TO CONGRESS, *supra* note 8, at 470–71.

300. *Id.*

301. *See supra* notes 283–84 and accompanying text.

### *B. LIMITING REIMBURSEMENT BASED ON HEALTH CARE PAYMENT MODEL*

One avenue to address fraud may include limiting reimbursement for telemedicine visits to providers who have embraced alternative billing arrangements. In the U.S. health care system, most insurers (both public and private) pay health care providers on a fee-for-service basis.[302] Thus, doctors, hospitals, and other health care providers bill separately for each service provided to a patient regardless of patient outcome.[303] Fee-for-service billing encourages over-utilization and disincentivizes efficient care models "because . . . profits . . . increase consistently with greater quantities" of provided services.[304] Similarly, profits increase from more costly services.[305] As a result, "some patients get too much care, some do not get enough, and others get the wrong care."[306] Fee-for-service billing also drives up health care costs due to lack of transparency concerning the cost of health care, lack of accountability for patient outcomes, and the administrative burden on the health care system.[307]

Public policy makers have worked to shift incentives by focusing on value-based reimbursement, which puts the focus on quality of care rather than quantity of care.[308] Under value-based models, providers seek relationships with other providers and organizations to provide continuity of care.[309] Thus, payments are based on health outcomes and cost reductions. The Patient Protection and Affordable Care Act ("Affordable Care Act") created the Medicare Shared Savings Program, which permits providers to receive fee-for-

---

302. Dale B. Thompson, *The Next Stage of Health Care Reform: Controlling Costs by Paying Health Plans Based on Health Outcomes*, 44 AKRON L. REV. 727, 729–30 (2011); Cody Vitello, *Transforming the Way We Pay Doctors*, 19 ADVANCE DIRECTIVE 34, 38–39 (2009).

303. *See* Thompson, *supra* note 302, at 729–30; Vitello, *supra* note 302, at 38–39.

304. Thompson, *supra* note 302, at 730.

305. *Id.*

306. KAITLIN HUNTER, DAVID KENDALL & LADAN AHMADI, THIRD WAY, THE CASE AGAINST FEE-FOR-SERVICE HEALTH CARE 5 (2021), http://thirdway.imgix.net/pdfs/the-case-against-fee-for-service-health-care.pdf [https://perma.cc/2QLK-WQV6].

307. *Id.* at 7–8.

308. CTRS. FOR MEDICARE & MEDICAID SERVS., REPORT TO CONGRESS: FRAUD AND ABUSE LAWS REGARDING GAINSHARING OR SIMILAR ARRANGEMENTS BETWEEN PHYSICIANS AND HOSPITALS AS REQUIRED BY SECTION 512(B) OF THE MEDICARE ACCESS AND CHIP REAUTHORIZATION ACT OF 2015, at 7 (2015) [hereinafter 2015 REPORT TO CONGRESS], https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/Downloads/Report-to-Congress-2015.pdf [https://perma.cc/ZR4A-3287].

309. As OIG has observed, however, "arrangements . . . that improve or maintain quality of care, reduce waste, and/or increase efficiency, may implicate the Federal fraud and abuse laws." *Id.* Thus, "the fraud and abuse laws may serve as an impediment to robust, innovative programs that align providers by using financial incentives to achieve quality standards, generate cost savings, and reduce waste." *Id.* As a result, CMS and OIG have waived the requirements of AKS and other fraud laws to carry out the shared savings program. *Id.* at 7–8. In 2021, CMS implemented a final rule providing safe harbors for value-based reimbursement models. *See supra* notes 160–63 and accompanying text.

service payments and be eligible for additional reimbursements if they meet quality and cost saving benchmarks.[310] The Affordable Care Act also established the Center for Medicare and Medicaid Innovation, which tests alternative payment models ("APMs").[311] APMs use "a payment approach that gives added incentive payments to provide high-quality and cost-efficient care."[312] Some examples of APMs are Accountable Care Organizations,[313] Patient-Centered Medical Homes, and new programs that bundle payments for episodes of care.[314] Providers can participate in more than one APM, and each APM can have different tracks that expose the provider to various levels of risk.[315] APMs may focus on particular provider types, geographic locations, populations, clinical condition, or care episodes.[316]

310. Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 3022, 124 Stat. 119, 395–99 (2010).

311. *Id.* § 3021, 124 Stat. 119, 389–95; QUALITY PAYMENT PROGRAM, CTRS. FOR MEDICARE & MEDICAID SERVS., APMS OVERVIEW, https://qpp.cms.gov/apms/overview [https://perma.cc/JB34-R785].

312. QUALITY PAYMENT PROGRAM, *supra* note 311.

313. An Accountable Care Organization is "a group of doctors, hospitals, and other health care providers, who come together voluntarily in an effort to give coordinated, high-quality care to the patients they serve." U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-104618, MEDICARE: INFORMATION ON THE TRANSITION TO ALTERNATIVE PAYMENT MODELS BY PROVIDERS IN RURAL, HEALTH PROFESSIONAL SHORTAGE, OR UNDERSERVED AREAS 1 (2021) [hereinafter GAO APM TRANSITION REPORT], https://www.gao.gov/assets/gao-22-104618.pdf [https://perma.cc/H2QU-39VS].

314. Kenya Woodruff & Neil Issar, *A Balancing Act: Alternative Payment Models and Physician Compensation*, 30 HEALTH L., 10, 10 (2017).

315. GAO APM TRANSITION REPORT, *supra* note 313, at 6.

> Some tracks may include one-sided risk where the participating providers may share in the savings that are generated from lowering health care costs but assume no financial risk. Other tracks may have two-sided risk models where participants can share in savings and may receive added incentive payments, but also take on increasing levels of financial risk.

*Id.*

316. *Id.*

The Medicare Access and CHIP Reauthorization Act of 2015,[317] established the Quality Payment Program for clinicians.[318] The Quality Payment Program recognizes the role of APMs in furthering CMS's goal to move from fee-for-service to reimbursement models that focus on the quality of care. Beginning in 2019, clinicians who participate in qualified advanced alternative payment models ("A-APMs") receive an incentive payment of five percent of their professional services payments.[319] A-APMs are a CMS-approved subset of APMs where APM entities invest more deeply in value-based care and assume greater revenue risks and rewards. A-APMs must meet three criteria: (1) Participants must use certified electronic health record technology[320]; (2) payments must be based on quality measures[321]; and (3) either the A-APM bears a significant financial risk or is a Medical Home Model[322] expanded under CMS Innovation Center authority.[323] "Most other clinicians participate in the Merit-based Incentive Payment System (MIPS) and receive a positive or negative payment adjustment (or no change) based on their performance in four areas: quality, resource use, advancing care information (formerly

317. *See generally* Medicare Access and CHIP Reauthorization Act of 2015, Pub. L. No. 114-10, 129 Stat. 87 (2015) (providing the Quality Payment Program). The Medicare Access and CHIP Reauthorization Act of 2015 repealed the Medicare Sustainable Growth Rate ("SGR") formula for calculating physician payments. *Id.* § 101, 129 Stat. 87, 89–128.

> The SGR . . . was the product of a congressional effort to constrain growth in Medicare's spending on physician services. The underlying formula was meant to generate reductions in fee-for-service payment rates when Medicare's total spending on physicians' services grew more quickly than a target growth rate. It made allowances for modest fee increases, changes in the number of Medicare beneficiaries, and GDP growth, among other factors.

Jeffrey Clemens & Stan Veuger, *Repeal of the Medicare Sustainable Growth Rate: Direct and Indirect Consequences*, 17 AM. MED. ASS'N J. ETHICS 1053, 1053 (2015). Because actual expenditures grew faster than target expenditures, the Medicare SGR formula reduced Medicare's fee-for-service payment rates. *Id.* Congress was under substantial political pressure from physician organizations over the lowered payment rates and "enact[ed] a series of temporary measures to keep these cuts from materializing." *Id.* The temporary measures required annual or more frequent renewal and over time the gap between the Medicare SGR calculated payment and the temporary measures approached thirty percent. *Id.* at 1053–54.

318. Medicare Access and CHIP Reauthorization Act of 2015, Pub. L. No. 114-10, § 101, 129 Stat. 87, 89–128 (2015). The law requires most physicians, physician assistants, nurse practitioners, clinical nurse specialists, and certified registered nurse anesthetist to participate in the Quality Payment Program through either the Merit-based Incentive Payment System or an Advanced APM. *Id.*

319. MEDICARE PAYMENT ADVISORY COMM'N, *supra* note 54, at 3.

320. 42 C.F.R. § 414.1415(a)(1) (2022).

321. *Id.* § 414.1415(b).

322. *Id.* § 414.1415(c); GAO APM TRANSITION REPORT, *supra* note 313, at 7 n.21 ("A Medical Home Model is an approach to providing comprehensive primary care that facilitates partnerships between patients, clinicians, medical staff, and families. It is a medical practice organized to produce higher quality care and improved cost efficiency.").

323. QUALITY PAYMENT PROGRAM, *supra* note 311.

meaningful use of electronic health records), and clinical practice improvement."[324]

The Medicare Payment Advisory Ie is considering which Medicare changes to telemedicine coverage during the Public Health Emergency should be made permanent. Although the Medicare Payment Advisory Committee recommends that after the Public Health Emergency ends "Medicare should temporarily pay for specified telehealth services provided to all beneficiaries regardless of their location,"[325] they also discuss the possibility of granting broad telemedicine waivers to clinicians in A-APMs.[326] Thus, it is possible that patients in A-APMs could have greater access to telemedicine than those with providers who do not participate in A-APMs. Ostensibly, this would promote value-based care without undermining critical fraud and abuse laws, such as AKS, used to police fee-for-service payments. If a provider is participating in A-APMs, then they are less reliant on fee-for-service billing and will not be incentivized to drive up costs.

There are some problems with this approach. In 2019, only twelve percent of providers in rural, shortage, or underserved areas and only fifteen percent of providers not located in these areas participated in A-APMs.[327] Unfortunately, switching to A-APMs is not just a matter of changing payment options. Providers face a number of challenges in transitioning to A-APMs. Many providers lack the financial resources necessary to finance the upfront costs associated with APMs and A-APMs.[328] Other providers are averse to the financial risk involved in A-APMs or do not have the cash reserves necessary to cover potential losses.[329] Some providers do not have enough Medicare patients to warrant the required investment for APMs.[330]

---

324. MEDICARE PAYMENT ADVISORY COMM'N, *supra* note 54, at 3.

325. 2021 REPORT TO CONGRESS, *supra* note 8, at 458, 463. The temporary continuation should last for one to two years after the end of the Public Health Emergency during which time Medicare can gather more evidence about the impact on "access, quality, and cost" before making any permanent changes. *Id.* at 458.

326. *Id.* at 463–64.

327. GAO APM TRANSITION REPORT, *supra* note 313, at 10.

328. *Id.* at 16. "[The] upfront costs associated with APM participation may include hiring additional staff, developing new care management strategies, and performing analysis to estimate the provider's likely performance in an APM before joining one . . . ." *Id.* at 17.

329. *Id.* at 16. "If providers do not meet certain benchmarks in an Advanced APM, CMS withholds or reduces payment, or providers owe payments to CMS. As such, providers with fewer financial reserves may have a limited ability to participate in APMs that include such downside risks." *Id.* at 17 (footnote omitted).

330. *Id.* at 16. "Additionally, providers who have lower patient volumes could face less predictable spending and utilization patterns and heightened financial risk in an APM . . . ." *Id.* at 18. It may also be difficult to control the cost of care because providers in these areas often must refer patients to other providers for tertiary care (specialized diagnostic and treatment procedures). *Id.* "Providers in rural, shortage, or underserved areas may not be part of a health system that includes specialists and sometimes must refer patients to another practice to receive specialized care, which can result in costs beyond their control . . . ." *Id.*

Another barrier for providers concerns electronic health records. Some providers cannot afford the costs associated with electronic health records or do not have the high-speed internet necessary for electronic health records.[331] Other providers are unable to perform the data analytics and financial modeling that is necessary to provide value-based care.[332] Another concern for providers is that many of them do not have staff members who can manage the transition to APMs and others do not have enough awareness about APMs.[333] Finally, the design and availability of models can act as an impediment to providers transitioning to APMs. Some providers have limited APM options because of the restrictions on the models such as geographic or participant limitations that make it difficult to find a model appropriate in rural, shortage, or underserved communities.[334] With all of these barriers to entry, it is clear that limiting reimbursement for telemedicine services to providers in A-APMs would drastically reduce access to care. The reduction in telemedicine services will be particularly acute in rural and underserved areas.

In terms of the fraud triangle, the use of A-APMs as a limiting principle for telemedicine reimbursement may have no effect on the pressure to commit fraud for some and may increase the pressure on others. A-APMs require providers to take on financial risk based on the quality of the care they provide. Some practitioners may view the value-based payment models as a threat to their livelihood because they will lose the certainty that comes from being paid based on the services they provide. Providers with struggling practices may be more tempted to falsify data to earn incentives or prevent a reduction in payment.

Further, the use of A-APMs changes rather than eliminates the opportunity to commit fraud. The use of A-APMs may reduce the type of fraud discussed in this Article by making it less profitable to write unnecessary prescriptions or orders. If payment is based on care outcome, then unnecessary tests, DME, or drugs increases the cost of care without any corresponding benefit for the care outcome. With respect to the scale of the fraud, there may be mixed results in terms of opportunity. On the one hand, if reimbursement for telemedicine is limited to A-APMs then the universe

331. *Id.* at 16. Certified Electronic Health Record technology is required for A-APMs. *Id.* at 19. Reportedly, "[Electronic Health Record] vendors charge practices the same price regardless of their size . . . [and] vendors charge practices every time they interface their system with another practice's [Electronic Health Records], and these charges can range in the thousands of dollars." *Id.*

332. *Id.* at 16. Both financial modeling and data analysis are needed "to assess performance in an APM." *Id.* at 18. Many providers in rural, shortage, or underserved areas would have to contract with outside firms to conduct the financial modeling and data analysis. *Id.* at 18–19.

333. *Id.* at 16. "[E]xisting staff in small practices in rural, shortage, or underserved areas may already be overburdened with office administration duties," which requires new staff to handle care coordination and data processing. *Id.* at 20. These practices simply do not have the infrastructure that larger practices have that would allow them to participate in A-APMs. *Id.*

334. *Id.* at 16.

of beneficiaries that could be taken advantage of through these schemes is much smaller because such a minute percentage of providers use A-APMs. On the other hand, prior to the expansion of access to telemedicine beyond rural and underserved areas, providers engaged in large scale fraud and attempted to avoid detection by not billing for the telemedicine visit. Utilizing the A-APM payment model would not remove that opportunity.

It is also important to recognize that value-based reimbursement programs carry

> inherent risks of fraud because of the high stakes involved. That is, as [value-based purchasing] either rewards or penalizes providers depending on performance, and subsequent performance results are posted to public information sites, there is substantial financial and reputational value at stake if quality data does not meet the mark.[335]

The accuracy of data is a serious concern in value-based reimbursement.[336] Thus, a provider might falsely certify that it has achieved certain quality metrics that are necessary to obtain incentive payments.[337] That false certification could lead to liability under the FCA.[338] Further, there may be situations where billed services were not received by Medicare beneficiaries even though quality criteria or outcomes were recorded in the medical record.[339] In those situations, the "[data quality] would be compromised and the scores submitted for [value-based purchasing] purposes would be false or fraudulent."[340] Inevitably, those determined to commit fraud will find ways to manipulate claims and care data to maximize reimbursements from the Federal Government. Thus, shifting to A-APMs may reduce fraud based on overutilization or lack of medical necessity but it is not a silver bullet.

Finally, the use of A-APMs may only have a minimal impact on the ability to rationalize telemedicine fraud.[341] One of the goals of value-based reimbursement is to get providers more invested in care outcomes.[342] To the extent that providers become more concerned about the care outcomes of

---

335. PollyBeth Hawk, *Ready or Not: Hospital Value-Based Purchasing Poised to Transform Healthcare Reimbursement Model and Introduce New Fraud Targets Under the False Claims Act*, 22 ANNALS HEALTH L. 43, 58 (2013).

336. *Id.* at 58–64 (explaining how the Government utilizes data mining and auditing to test the quality of data).

337. Anna M. Grizzle, Amy Sanders Morgan & Brian D. Roark, *New Wine in Old Wineskins: Mitigating Fraud and Abuse Risks in Value-Based Reimbursement*, 2017 AM. HEALTH L. ASSOC. CONNECTIONS 22, 24, https://sharepoint.healthlawyers.org/find-a-resource/HealthLawHub/Documents/Compliance/February2017_Feature3.pdf [https://perma.cc/DCN3-A7AK].

338. *Id.*

339. Hawk, *supra* note 335, at 70.

340. *Id.* at 69–70.

341. Lederman, *supra* note 262, at 1159–61.

342. Grizzle et al., *supra* note 337, at 24.

their individual patients, it may become harder for those providers to justify ordering or prescribing unnecessary tests, drugs, or DME. They may be unable to disassociate their fraudulent actions from the patient which would make it more difficult to convince themselves that they are committing a victimless crime. That assumes that the change in payment structure will impact the provider's mindset. It is not entirely clear that is the case. And limiting telemedicine reimbursement to A-APMs will not be a transformative change because such a tiny percentage of providers are enrolled in A-APMs. Further, as discussed above, fraudsters have already found ways to evade the limitations on access to telemedicine.

Ultimately, limiting reimbursement for telemedicine to providers enrolled in A-APMs not only puts fraud concerns before access, but it also fails to account for the way that fraud will change based on the payment model. Lawmakers should reject any rule that would limit telemedicine reimbursement to providers in A-APMs. It may, however, be worth considering limiting telemedicine reimbursement to providers in accountable care relationships. The Center for Medicare and Medicaid Innovation has a goal of having all traditional Medicare beneficiaries and most Medicaid beneficiaries in an accountable care relationship with accountability for quality and cost by 2030.[343] This is a shift from the previous goal to have all Medicare beneficiaries in APMs by 2025. In 2020, sixty-seven percent of Medicare beneficiaries enrolled in Part A or B were in Medicare Advantage plans or in an Accountable Care Organization through a Center for Medicare and Medicaid Innovation model or the Shared Savings Plan.[344] This limitation would not harm access as much as a rule that grants broad flexibility for providers in A-APMs (which have less than fifteen percent of Medicare beneficiaries) but does not grant similar flexibilities to providers in other plans.

### *C. RESTRICTIONS ON MEDICARE ENROLLMENT AND REIMBURSEMENT*

It is important to examine the Medicare enrollment and reimbursement process to determine if there are additional enrollment or reimbursement requirements that can help prevent telemedicine scams. In recent years, CMS has utilized the enrollment process to reduce program fraud. CMS also utilizes its Fraud Prevention System to perform data analytics and discover fraudulent claims.

Historically, there were few barriers to enrollment in Medicare as a provider or supplier. That changed, however, after significant fraudulent actions by non-existent DME providers. In 1997, OIG found that one of every fourteen DME suppliers did not have a verifiable address and forty percent of new

343. CTRS. FOR MEDICARE & MEDICAID SERVS., BACKGROUND ON THE CMS INNOVATION CENTER 2021 STRATEGY REFRESH – PUTTING ALL PATIENTS AT THE CENTER OF CARE (2022), https://innovation.cms.gov/strategic-direction [https://perma.cc/D8XM-QD6C].

344. CTRS. FOR MEDICARE & MEDICAID SERVS., INNOVATION CENTER STRATEGY REFRESH 13 (2021), https://innovation.cms.gov/strategic-direction-whitepaper [https://perma.cc/8S6Q-MX93].

applicants failed to meet supplier standards.[345] Unfortunately, "[t]he ease and low expense of acquiring a supplier number facilitated the entry of abusers into the Program."[346] Beginning in 1996, CMS has required all new providers of health care items and services to submit CMS Form 855 Provider/Supplier Enrollment Application ("CMS-855") to enroll in the program.[347] In 2003, CMS proposed that all providers and suppliers be required to submit an enrollment application, obtain a Medicare billing number, and receive Medicare billing privileges.[348]

In 2006, CMS further expanded the enrollment regulations by requiring, *inter alia*, that enrolled providers and suppliers resubmit and recertify the accuracy of their enrollment information every five years.[349] In addition to the CMS-855 enrollment requirements, DME providers must be accredited by an independent accrediting organization as a condition of initial and continued enrollment in Medicare.[350]

The Affordable Care Act significantly increased CMS's authority to use the Medicare enrollment process to screen out questionable providers and suppliers.[351] The Affordable Care Act program integrity measures include, among other things, "mandated screening procedures, entrance fees, mandatory compliance programs, enhanced oversight, transparency and reporting requirements, various financial disclosure requirements, and limitations and requirements related to ordering DME."[352]

Prior to the Affordable Care Act, provider screening was not a part of the Medicare enrollment process.[353] CMS did not distinguish between the types of providers and suppliers for purposes of conducting background checks.[354] When CMS conducted background checks, it reviewed criminal backgrounds, performed site visits, examined licensure requirements, checked databases, and looked over the Medicare Advantage Organization reports for all enrolling providers and suppliers.[355] In 2011, CMS set forth screening levels for Medicare providers and suppliers based on categorical risk.[356] DME suppliers

345. JUNE GIBBS BROWN, U.S. DEP'T OF HEALTH & HUM. SERVS., OFF. OF INSPECTOR GEN., MEDICAL EQUIPMENT SUPPLIERS: ASSURING LEGITIMACY 5–6 (1997), https://oig.hhs.gov/oei/reports/oei-04-96-00240.pdf [https://perma.cc/WQ4B-BYS2].

346. Adrienne Dresevic & Donald H. Romano, *The Medicare Enrollment Process–CMS's Most Potent Program Integrity Tool*, 23 HEALTH L. 1, 3 (2011).

347. *See generally* 61 Fed. Reg. 37278 (July 17, 1996) (providing the requirements).

348. Dresevic & Romano, *supra* note 346, at 3.

349. 42 C.F.R. § 424.515 (2022).

350. *Id.* § 424.57(c)(22).

351. Dresevic & Romano, *supra* note 346, at 11.

352. *Id.* at 10.

353. *Id.*

354. *Id.*

355. *Id.* at 10.

356. Medicare, Medicaid, and Children's Health Insurance Programs; Additional Screening Requirements, Application Fees, Temporary Enrollment Moratoria, Payment Suspensions

are in the high risk category and must undergo more background screening than providers in limited or moderate risk categories.[357]

In 2019, CMS instituted a final rule that provided program integrity enhancements to the provider enrollment process.[358] The 2019 final rule requires disclosure of current and prior affiliations with other health care providers and suppliers with program integrity concerns.[359] Specifically, it requires providers and suppliers to disclose any current affiliation

> with a provider or supplier that has uncollected debt; has been or is subject to a payment suspension under a federal health care program; has been excluded from Medicare, Medicaid, or [Children's Health Insurance Programs]; or has had its Medicare, Medicaid or [Children's Health Insurance Programs] billing privileges denied or revoked.[360]

CMS then determines whether the disclosed affiliation "poses an undue risk of fraud, waste, or abuse."[361] If CMS finds an undue risk of fraud, CMS will deny the enrollment application or revoke the Medicare enrollment of the provider or supplier.[362]

---

and Compliance Plans for Providers and Suppliers, 76 Fed. Reg. 5862, 5963 (Feb. 2, 2011) (to be codified at 42 C.F.R. pt. 1007). Under the law, Medicare providers and suppliers are divided into limited, moderate, and high risk. 42 C.F.R. § 424.518 (2022). As the risk level increases so do the screening requirements. If a provider is in the limited risk category, the Medicare contractor: (1) verifies that the provider meets Federal and State requirements for that type of provider or supplier; (2) conducts license verifications; and (3) conducts database checks pre- and post-enrollment to verify compliance with the enrollment criteria. *Id.* § 424.518(a)(2). Independent clinical laboratories and diagnostic testing facilities are categorized as moderate risk and require, in addition to the limited risk screening, an on-site visit as part of the screening process. Newly enrolled DME suppliers are in the high categorical risk category. *Id.* § 424.518(c)(1)(ii). In addition to the limited and moderate screening requirements, newly enrolled DME suppliers must provide fingerprints for all individuals with a five percent or greater direct or indirect ownership interest. The contractor will perform a fingerprint-based criminal history check on each individual. *Id.* § 424.518(c)(2).

357. 42 C.F.R. § 424.518(c).

358. Medicare, Medicaid, and Children's Health Insurance Programs; Program Integrity Enhancements to the Provider Enrollment Process, 84 Fed. Reg. 47794, 47794–95 (Sept. 10, 2019). The final rule also expands CMS's denial and revocation authority under 42 C.F.R. §§ 424.530 and 424.535.56. Jessica Gustafson & Adrienne Dresevic, *CMS Greatly Expands Its Authority to Deny and Revoke Providers' and Suppliers' Medicare Enrollment*, 32 HEALTH L. 6, 14 (2019).

359. Medicare, Medicaid, and Children's Health Insurance Programs; Program Integrity Enhancements to the Provider Enrollment Process, 84 Fed. Reg. at 47794.

360. *Id.* at 47794–95. For purposes of the rule, affiliation means: (1) that an individual or entity has a five percent or greater direct or indirect ownership interest; (2) that an individual or entity has a general or limited partnership interest; (3) that an individual or entity exercises control over the day-to-day operations of another entity; (4) an individual has an interest where she is acting as an officer or director of a corporation; and (5) any reassignment relationship under section 424.80. *See* 42 C.F.R. § 424.502 (2022).

361. 42 C.F.R. § 424.519(f).

362. *Id.* § 424.519(g).

CMS should consider adding additional screening requirements related to telemedicine. Currently, CMS-855 does not require any disclosures concerning telemedicine.[363] It will not be enough, however, to require disclosure of affiliations with telemedicine companies that have program integrity concerns because the 2019 final rule would already encompass affiliations with those telemedicine providers. To be most effective, CMS should require providers to disclose any affiliation with a telemedicine company regardless of program integrity concerns. In addition, CMS may also want to consider disclosure of a relationship with any telemedicine company that is responsible for a certain percentage of sales for the provider—whether it be an affiliation, as that term is defined in the regulations, or not. Although it may be cumbersome for a provider to furnish information on every telemedicine provider that they have done business with, this information could prove to be critical for CMS. These disclosure requirements could assist CMS in identifying suppliers that have inappropriate relationships with telemedicine providers. These disclosures could also alert CMS to the need to perform additional audits on particular providers prior to payment.

On the reimbursement end of things, DME reimbursements require the name and provider number of the provider who ordered or prescribed equipment.[364] To battle telemedicine fraud, CMS should consider requiring DME suppliers, laboratories, and pharmacies to indicate whether the DME, lab tests, or drugs were prescribed or ordered during a telemedicine visit. That information could help Medicare Administrative Contractors identify situations where a supplier has submitted a reimbursement claim, but there is no matching claim for reimbursement for telemedicine services. Many of the telemedicine scams prior to the Public Health Emergency involved situations where suppliers submitted claims for reimbursement, but the telemedicine providers did not submit claims. Further, CMS could also require DME providers to supply the name of the telemedicine company. This could assist in data analytics when seeking to identify trends.

CMS may also want to consider additional auditing requirements for DME and laboratory tests. Specifically, it is worth considering patient verification of telemedicine visits and/or DME or laboratory orders prior to reimbursement. This would require a robust patient identity verification system which would likely be very costly. This type of system may prove to be too cumbersome for drug prescriptions due to the volume of prescriptions in Medicare. If it could be implemented in a cost-effective way, however, it could help protect both the patients and Medicare.

---

363. *See supra* notes 345–50 and accompanying text.

364. *See* CTRS. FOR MEDICARE & MEDICAID SERVS., MEDICARE PROGRAM INTEGRITY MANUAL: CHAPTER 5 – DURABLE MEDICAL EQUIPMENT, PROSTHETICS, ORTHOTICS, AND SUPPLIES (DMEPOS) ITEMS AND SERVICES HAVING SPECIAL DME REVIEW CONSIDERATIONS, ch. 5.2–5.7, at 3–14 (2022), https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/pim83c05.pdf [https://perma.cc/9SJ4-WMTV].

With respect to the fraud triangle, these measures will not impact the perceived pressure that providers face to commit fraud. Patient verification of DME and laboratory tests may have a minor impact on rationalization. It may be more difficult to justify this conduct if patients begin questioning the provider about unnecessary DME and laboratory tests. Collectively, these measures are most likely to impact the opportunity to commit fraud. If CMS can weed out suppliers likely to commit fraud through its Medicare enrollment process, then that reduces the opportunity to commit fraud for those who are not entering the program in good faith. For those entering the program in good faith, measures designed to detect fraud prior to payment will diminish the opportunity for fraud. Providers will be aware that due to additional data, it may be more difficult to get away with fraud. Further, verification requirements that go directly to the patient increase the likelihood of getting caught. If providers do not believe that they can evade the auditing and verification process, they are less likely to engage in fraud. There is no doubt, however, that individuals who find themselves under a great amount of perceived pressure will find new ways to commit fraud and will attempt to falsify data to escape detection. An ongoing commitment to assess and reassess fraud prevention and detection will be critical as telemedicine becomes a permanent fixture in health care.

## CONCLUSION

Telemedicine has transformed our health care delivery system by expanding access to health care without increasing the number of providers. It has also assisted in addressing disparities in access to health care in rural and underserved communities. During the height of the COVID-19 pandemic, providers quickly pivoted to remote patient care. Telemedicine was critical for providing care when people were adhering to stay-at-home orders or quarantining. But telemedicine only emerged as a savior during COVID-19 because of waivers of restrictions on reimbursement of telemedicine services. Those waivers only last for the duration of the Public Health Emergency. Once the Public Health Emergency is over, it is unlikely that we can impose the same restrictions on telemedicine that existed prior to the pandemic.

Whenever a segment of the health care industry expands at an accelerated rate there is always a danger that it will be accompanied by a substantial uptick in fraud. Telemedicine is no different. Indeed, fraud has followed the growth in the telemedicine industry like a shadow. Even when telemedicine was highly restricted, fraudsters cleverly evaded Medicare's controls on telemedicine to the tune of hundreds of millions of dollars. With the expansion of access to telemedicine, the threat of telemedicine scams is even greater. As we consider the future of telemedicine, we must seriously consider fraud prevention. Lawmakers should focus on measures that preserve access to care through telemedicine while reducing the opportunity to commit fraud.