DePaul University
University Libraries

DePaul Journal of Health Care Law

Volume 24
Issue 2 *2023*

Article 3

# Telehealth Fraud and Abuse Before and "After" the Pandemic: Are Things Going to Get Better?

Natalia Shamuel
*DePaul University College of Law*, depaul.jhcl@gmail.com

Follow this and additional works at: https://via.library.depaul.edu/jhcl

 Part of the Health Law and Policy Commons

## Recommended Citation

Natalia Shamuel, *Telehealth Fraud and Abuse Before and "After" the Pandemic: Are Things Going to Get Better?*, 24 DePaul J. Health Care L. (2023)
Available at: https://via.library.depaul.edu/jhcl/vol24/iss2/3

This Article is brought to you for free and open access by the College of Law at Digital Commons@DePaul. It has been accepted for inclusion in DePaul Journal of Health Care Law by an authorized editor of Digital Commons@DePaul. For more information, please contact digitalservices@depaul.edu.

# Telehealth Fraud and Abuse Before and "After" the Pandemic: Are Things Going to Get Better?

Natalia Shamuel

## I. Introduction

When the world shut down due to the deadly COVID-19 pandemic, there was a lot of uncertainty. Doctors' offices were closed, and in-person visits were no longer allowed in order to limit face-to-face contact and stop the spread of the ongoing virus. In March 2020, scientists, doctors, and the public had a lot to learn about this new virus, but one thing everybody knew was that people still needed medical care. Hospitals were overcrowded due to the hundreds of thousands of COVID-19 patients needing hospital beds. Although many people were getting infected with COVID-19, people still needed to see their dermatologists, pediatricians, and family physicians. When the world shut down, the spotlight was placed on telemedicine. The stay-at-home order was the perfect ingredient for telemedicine to do what it was meant to do, provide care through technology.

Telehealth and telemedicine are not new creations, the use of telecommunication to provide medical care has been in effect since the early 1900s.[1] Technology and telehealth have come a long way since then, and with the leniency of seeing patients via video chat or over the phone, comes a wide selection of fraudulent activities.[2] Healthcare fraud via telemedicine and telehealth is extremely prevalent in this COVID era, accounting for seventeen percent of outpatient visits, thirty-eight times more than pre-COVID.[3] Because of this, state and federal government legislators are acting against telehealth fraud and abuse by healthcare providers via takedowns and new healthcare legislation and policies.[4] This paper will take a deep dive into telehealth and

---

[1] Thomas S. Nesbitt, *The Evolution of Telehealth: Where Have We Been and Where Are We Going?* (Nov. 20, 2012), https://www.ncbi.nlm.nih.gov/books/NBK207141/

[2] *New HHS Study Shows 63-Fold Increase in Medicare Telehealth Utilization During the Pandemic* (Dec. 3, 2021) https://www.cms.gov/newsroom/press-releases/new-hhs-study-shows-63-fold-increase-medicare-telehealth-utilization-during-pandemic

[3] Oleg Bestenyy, et al., *Telehealth: A quarter-trillion-dollar post-COVID-19 reality?* (July 9, 2021), https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality

[4] *Id.*

telemedicine, outlining groundbreaking telehealth fraud takedowns by the DOJ, telehealth laws that were implemented before the COVID-19 pandemic, and new ways that the government is taking action against the increase in the use of telehealth and telemedicine.

Part II of this article will outline the differences between telehealth and telemedicine. Those two words, often used interchangeably, have two very different meanings, and it is easy for them to get confused. I will discuss the differences and provide correct context in which each word is used. Part III of this article will outline various forms of telehealth and telemedicine fraud and abuse. This will include examples of telehealth fraud and brief discussions of telehealth takedowns by the Department of Justice. These takedowns include fines and penalties imposed on individuals who were caught in telehealth fraud schemes. Part IV of this article will display telehealth regulations that were implemented pre-COVID-19. As previously discussed, telehealth has been around since long before the pandemic, and telehealth fraud is not a new issue. Part IV will outline how the government has been monitoring and cracking down on telehealth since before the public health emergency. Part V will provide an overview of the analysis of new governmental regulations that have been or will be imposed on telehealth providers to protect against telehealth fraud. Part VI will briefly discuss why it is important that these new regulations are imposed. Part VII will discuss the first method of governmental regulation on telehealth fraud during COVID-19, whistleblowers and enhanced whistleblower protections. Part VIII will discuss the next government regulation, phased OIG audits on telehealth companies. Part IX will briefly discuss the potential return to the Ryan Haight Act of 2008. Finally, Part X will discuss new state telehealth licensing requirements as well as a discussion regarding the Office of Inspector General's evaluation on the telehealth monitoring practices of state's that offer mental health services via telehealth.

## II. Telehealth vs. Telemedicine

Telehealth is a broad term used to describe the mode of communication in which providers will render healthcare services.[5] These telehealth technologies often refer to telecommunication technology and electronic information.[6] Telehealth may also refer to general video chatting, images, streaming devices, or other communication methods used via the internet.[7] Although telehealth refers to the mode of communication used, broadly, telehealth refers to remote and sometimes non-clinical communications, including services rendered "beyond the doctor-patient relationship."[8]

Telemedicine refers to a narrower class of telecommunicated health care services. Telemedicine refers to the actual delivery of care via telehealth.[9] Telemedicine services will often include clinical care, diagnosing patients via telehealth, or monitoring the status of an existing patients progress in said clinical services.[10]

The focus throughout this paper will be on telehealth, although telemedicine fraud does occur (and will be mentioned throughout this article as well), as you will see through the DOJ takedowns, a vast majority of healthcare fraud and abuse that comes from telehealth and telemedicine is through providers using telehealth more broadly. As of 2020, the Center for Medicare and Medicaid Services (CMS) expanded the horizons of telehealth and telemedicine.[11] Because the False Claims Act is in response to fraud that occurs between physicians and

---

[5] *What's the Difference between telemedicine and telehealth?*, AM. ACADEMY OF FAMILY PHYSICIANS, https://www.aafp.org/news/media-center/kits/telemedicine-and-telehealth.html (last visited Dec. 12, 2021).
[6] Ron Cresswell, *Common Telehealth Fraud Schemes You Should Know About* (Apr. 13, 2020) https://www.acfeinsights.com/acfe-insights/common-telehealth-fraud-schemes-you-should-know-about
[7] *Id.*
[8] *Telehealth, Telemedicine, and Telecare: What's What?*, FED. COMM. COMM'N., https://www.fcc.gov/general/telehealth-telemedicine-and-telecare-whats-what
[9] *Id.*
[10] *Id.*
[11] *Medicare Telemedicine Health Care Provider Fact Sheet*, CENTERS FOR MEDICARE & MEDICAID SERVICES (Mar. 17, 2020), https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet

government funded insurance providers,[12] it is important to note that CMS now includes visits that would generally be considered in-person visits to be billed to Medicare as telehealth visits so that the patient does not have to physically go to their doctor's office.[13] Currently, the Consolidated Appropriations Act (CAA) of 2023 allows providers some leeway in their telehealth services. [14] These freedoms include continued billing to Medicare for services provided via telehealth "regardless of where the patient or provider is located" and is set to expire in 2024.[15]

## III. Types of Fraud Happening Via Telemedicine

The Department of Justice (DOJ) has identified telehealth fraud and abuse as a high priority area for regulation.[16] Between February of 2020 and April of 2020, the number of Medicare visits held via telehealth increased from 0.1% to 43.5%, leading up to about half of all Medicare visits being through telehealth.[17] In Chicago, Illinois, the percent of Medicare visits held via telehealth increased from 0.0% to 52.4% within the same time frame.[18] It is important that the DOJ engages in takedowns such as the cases that will be described in this paper because as the use of telehealth continues, it only makes sense that fraud and abuse is likely to increase.

Many telehealth fraud and abuse schemes fall under False Claims Act violations, including: improper billing and coding to Medicare or insurance providers, billing for visits that did not

---

[12] 31 U.S.C. § 3729.
[13] Medicare Telemedicine Health Care Provider Fact Sheet, *supra* note 11.
[14] Thomas B. Ferrante & Rachel B. Goodman, *Public Health Emergency Ends May 11: What Telehealth Companies Need to Know*, FOLEY & LARDNER LLP (Feb. 7, 2023), https://www.foley.com/en/insights/publications/2023/02/public-health-emergency-ends-may-11-telehealth
[15] *Id.*
[16] Kyle Y. Faget, et al., *A Target on Telehealth: Government Action Against Telehealth Fraud in the Wake of COVID-19*, FOLEY & LARDNER LLP (July 15, 2021), https://www.foley.com/en/insights/publications/2021/07/target-on-telehealth-government-action-fraud
[17] Arielle Bosworth, et al., *Medicare Beneficiary Use of Telehealth Visits: Early Data From the Start of The COVID-19 Pandemic*, DEP'T HEALTH & HUM. SERVS. (July 28, 2020) https://aspe.hhs.gov/sites/default/files/private/pdf/263866/hp-issue-brief-medicare-telehealth.pdf
[18] *Id.*

actually happen, or receiving illegal kickbacks, specifically through the act of buying or selling Durable Medical Equipment (DME) in violation of the Anti-Kickback Statute.[19] Many telehealth fraud schemes, however, involve providers who will bill for medically unnecessary durable medical equipment (DME) for patients that do not actually need the devices being ordered.[20] Billing for medically unnecessary services or devices is a fraudulent way in which providers will attempt to gain high reimbursements from Medicare or other insurance companies.[21]

In September 2020, the DOJ charged 86 criminal defendants with submitting up to $4.5 billion in false and fraudulent claims submitted to Medicare.[22] These defendants used telehealth and telemedicine to pay doctors and nurses to order various medical equipment's such as DME, genetic testing, and medications.[23] These orders were made without having seen the patient, or, if the physician had seen the patient, it was through a brief phone call.[24] After the equipment was ordered for patients that either did not exist or did not need the equipment, medical device companies and pharmacies ordered the devices in exchange for money or bribes, violating the federal Antikickback statute.[25] Individuals involved in cases such as these help us understand the ways in which providers will use the title and protection of telehealth as a mask to engage in telehealth fraud.

---

[19] Erica Benites Giese, et al., *Telemedicine Fraud During COVID-19*, JD Supra (July 6, 2020), https://www.jdsupra.com/legalnews/telemedicine-fraud-during-covid-19-30585/
[20] Cresswell, *supra* note 6.
[21] *Medicare Fraud and Abuse: Prevent, Detect, Report*, CTR. FOR MEDICARE & MEDICAID SERVS. (Jan. 2021) available at https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Fraud-Abuse-MLN4649244.pdf
[22] NATIONAL HEALTH CARE FRAUD AND OPIOID TAKEDOWN RESULTS IN CHARGES AGAINST 345 DEFENDANTS RESPONSIBLE FOR MORE THAN $6 BILLION IN ALLEGED FRAUD LOSSES, U.S. DEP'T OF JUSTICE (Sept. 30, 2020), https://www.justice.gov/opa/pr/national-health-care-fraud-and-opioid-takedown-results-charges-against-345-defendants
[23] *Id.*
[24] *Id.*
[25] *Id.*

In April 2020, the DOJ charged a Georgia resident in a similar telehealth fraud DME scheme.[26] Charlene Frame, the defendant in this case, was the owner and operator of two telemedicine companies and was found guilty of conspiracy in attempt to pay medical providers in exchange for orders of DME.[27] Frame then conspired to sell the equipment to medical device companies and bill Medicare for reimbursements under the impression that the DME was ordered and obtained for patients that were never seen.[28]

In September 2019, the DOJ charged defendants for violating federal antikickback statutes and false claims act violations for paying doctors to prescribe genetic testing to elderly and disabled patients, tests that were not medically necessary.[29] Similar to previous telemedicine fraud cases, these doctors either never saw their patients or only had brief telephone conversations with them.[30] The defendants in this takedown targeted elderly individuals by working with fraudulent telemedicine companies to disguise their actions as telemedicine visits rendering clinical care to elderly patients.[31]

Finally, on August 10, 2021, the DOJ released another takedown involving $784 million in healthcare fraud by a telemedicine company in Florida.[32] The owner of the telemedicine company, Creaghan Harry and his co-conspirators were charged with soliciting kickbacks from

---

[26] TELEMEDICINE COMPANY OWNER CHARGED IN $60 MILLION FRAUD SCHEME, U.S. DEP'T OF JUSTICE. (Apr. 23, 2020), https://www.justice.gov/usao-sdga/pr/telemedicine-company-owner-charged-60-million-fraud-scheme
[27] *Id.*
[28] *Id.*
[29] 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, U.S. DEP'T OF JUSTICE. (Sept. 27, 2019), https://www.justice.gov/opa/pr/federal-law-enforcement-action-involving-fraudulent-genetic-testing-results-charges-against
[30] *Id.*
[31] *Id.*
[32] TELEMEDICINE COMPANY OWNER CHARGED IN SUPERSEDING INDICTMENT FOR $784 MILLION HEALTH CARE FRAUD, ILLEGAL KICKBACK AND TAX EVASION SCHEME, U.S. DEP'T OF JUSTICE (Aug. 10, 2021), https://www.justice.gov/opa/pr/telemedicine-company-owner-charged-superseding-indictment-784-million-health-care-fraud

DME suppliers.[33] Harry would pay physicians to write prescriptions and orders for DME, including braces and medications, that were medically unnecessary.[34] These suppliers provided orders placed by Harry and his companies that totaled up to $784 million billed to Medicare.[35] Of that $784 million, Medicare paid around $247 million.[36] Harry, in an attempt to disguise the kickbacks that were being received, ordered the DME suppliers to bill subsidiaries of his telemedicine companies, with owners residing not only in the United States but also in foreign countries.[37] That money would then be transferred from those subsidiary accounts into Harry's telemedicine company.[38] Along with the kickbacks, Harry also falsely claimed that he was receiving ten million dollars per year from patients receiving services via his telemedicine company.[39] If convicted, Harry will face a maximum sentence of twenty years in prison.[40]

These cases fall within the broad telehealth schemes coined by the DOJ as "Operation Double Helix," relating to fraudulent telemedicine billing for medically unnecessary genetic testing, and "Operation Brace Yourself," relating to fraudulent telehealth billing for medically unnecessary DME to Medicare and other insurance companies for patients that may have never been spoken to. These cases also helps us understand how easy it has been for telehealth and telemedicine company owners to provide remuneration to physicians and nurses with the intent of receiving high reimbursements from Medicare. Hiding behind the guise of telecommunication, it has become easier for healthcare providers to pretend that a patient was seen or to pretend that a phone call occurred with a patient where the provider and the patient discussed the patients need.

---

[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*

In reality, as seen in the DOJ takedowns described above, conversations never occur and providers are receiving benefits from insurance companies for their fraudulent behaviors. As a result, government officials have implemented new restrictions, regulations, and policies to attempt to combat the increase in telehealth fraud.

## IV. Telehealth Regulations Pre-COVID

Telehealth and telemedicine fraud are not new to the pandemic. Along with DOJ takedowns, Congress implemented restrictions that limited the way physicians could use telemedicine and telehealth when rendering care to their patients. A notable example of this is the Ryan Haight Act of 2008.

Ryan Haight was 18-years old when he passed away from a Vicodin overdose.[41] Vicodin is a controlled substance, meaning there are a lot of restrictions that come with prescribing it. Ryan Haight was prescribed Vicodin via telemedicine by a doctor that had never conducted an in-person evaluation of Ryan and was delivered virtually (to his doorstep) through an online pharmacy.[42] After Ryan's passing, Congress enacted the Act to restrict physicians from prescribing controlled substances via telemedicine.[43] Specifically, the Ryan Haight Act requires a physician to conduct at least one in-person evaluation of a patient before prescribing controlled substances via telemedicine.[44] The Act also requires that the reasoning for the prescription be medically legitimate.[45]

---

[41] Dr. Maheu, *Telehealth Opioids and Ryan Haight Act: Update* (May 21, 2021), https://telehealth.org/ryan-haight-act/
[42] Cody Haight, *A Post Pandemic Ryan Haight Act May Create Uncertainty for Telemedicine* (Mar. 11, 2021), https://www.legitscript.com/2021/03/11/a-post-pandemic-ryan-haight-act-may-create-uncertainty-for-telemedicine/
[43] *Id.*
[44] *Id.*
[45] *Id.*

The purpose of the Ryan Haight Act was to restrict physicians from prescribing controlled substances to patients without first having conducted an in person evaluation.[46] However, the Act was temporarily waived in response to the COVID-19 public health emergency declaration.[47] While the waiver still requires the prescribing physician to conduct an evaluation of the patient via telehealth, such as a video conference,[48] it became easier for physicians to engage in fraud again. It is very possible for physicians to overprescribe controlled substances, contributing to the Opioid crisis, but it is also possible again for physicians to bill insurance companies for medically unnecessary prescriptions, or to bill insurance companies for more expensive brand names rather than generic prescriptions of controlled substances that could be given to patients. The waiver on the Ryan Haight Act was set to expire at the end of 2021;[49] however, there had been no mention by congress as to whether the waiver is going to be a permanent implementation, or if the Ryan Haight Act will come into play again. At the time of publication of this article though, the Biden Administration has announced its intent to end the COVID-19 public health emergency on May 11, 2023.[50] What does this mean for the Ryan Haight Act? The in-person requirement to prescribe a controlled substance is likely to return, making it more difficult to prescribe via telemedicine.[51]

The regulations of telehealth prior to COVID-19 were few and far between. Now that the world is in a state of emergency, the government has been closely monitoring telehealth and telemedicine fraud.

---

[46] Maheu, *supra* note 41.
[47] *Id.*
[48] *Id.*
[49] *Alliance Joins Letter to Hill in Support of Temporary Extension of DEA Waiver in COVID Relief Package*, CONNECTWITHCARE.ORG (Dec. 15, 2020), https://connectwithcare.org/alliance-joins-letter-to-hill-in-support-of-temporary-extension-of-dea-waiver-in-covid-relief-package/
[50] Ferrante & Goodman, *supra* note 14.
[51] *Id.*

## V. New Telehealth Regulations and What It Means Going Forward

In addition to DOJ takedowns, state and federal government legislators and officials are implementing various precautionary measures. While these takedowns are large and result in charging fraudulent actors with billions of dollars in false claims, it is important for the government to act on telehealth and telemedicine fraud before it gets to the point of billion-dollar settlements. These new regulations and policies include enhanced whistleblower protections, OIG Audits to monitor Medicare services being rendered via telehealth,[52] the potential return to previous telehealth restrictions, state licensing requirements and state-specific executive orders, such as Illinois allowing out-of-state providers to render telehealth services to Illinois residents without an Illinois medical license,[53] as well as the DOJ National Rapid Response Strike Force.

Telehealth and telemedicine allow providers to inconspicuously "render" care to patients and write it off as a consultation or evaluation when billing to Medicare or other insurance providers. The ease and convenience of telehealth is beneficial to many for good reasons, but it is also beneficial to many for illegal reasons as well. The cases described in this paper demonstrate how physicians can bill Medicare and cost the government billions of dollars in false claims and kickbacks.

It is important that the federal government specifically enacts new legislation and policies to crack down on telehealth fraud and abuse. Telehealth fraud has now accounted for billions of dollars in settlements and false claims to Medicare and other insurance companies because of the ease of telehealth. Enhanced whistleblower protections will be a crucial part in putting the

---

[52] *Audits of Medicare Part B Telehealth Services During the COVID-19 Public Health Emergency*, OFFICE OF INSPECTOR GEN., https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000556.asp (last visited Dec. 12, 2021).

[53] *U.S. States and Territories Modifying Requirements for Telehealth in Response to COVID-19*, https://www.fsmb.org/siteassets/advocacy/pdf/states-waiving-licensure-requirements-for-telehealth-in-response-to-covid-19.pdf (last updated Nov. 12, 2021).

government on notice when telehealth and telemedicine fraud is occurring because the government needs to protect the people who are willing to come forward. Relators bringing qui tam action against providers or patients who suspect their provider may be engaging in fraud should feel comfortable to bring these issues to light. If individuals are worried that retaliation may occur if they speak up, it will be difficult for the DOJ, the HHS, or the CMS (Centers for Medicare & Medicaid Services) to investigate and charge individuals with telehealth fraud and abuse.

OIG Audits are also important because via auditing Medicare services rendered via telehealth and monitoring the services that are being billed as medically necessary for patients that have actually been seen by the physician, the government will be able to catch telehealth fraud on a larger scale. These audits, I believe, will be a crucial part in combating telehealth fraud and abuse in this new era. COVID-19 has instilled uncertainty in a lot of individuals, and it is important that patients are getting the care they need from physicians that care about helping them. If physicians are using patients who prefer telehealth, such as the elderly or low-income individuals who can't afford to drive or take public transportation to the doctor's office, then not only are patients not getting the care they need but Medicare and other private and public insurance companies are going to be losing insurmountable amounts of money.

Perhaps one of the most interesting and important is returning to pre-covid regulations that have been waived because of the public health emergency. This portion of the federal government action, such as waiving the Ryan Haight Act, also ties in with state licensing requirements and state legislation that have been implemented. States are easing restrictions to allow more providers to render telehealth services to out-of-state patients. In Illinois, out-of-state providers, in response to the pandemic, may see a patient via telehealth so long as they have a previously established

relationship.[54] These waivers make it easier for providers to see more patients, which may also make it easier for providers to claim they saw more patients to Medicare. If providers are allowed more access to patients, then it is possible that they may be more inclined to fraudulently bill to Medicare since it may be more difficult for Medicare or other patient insurance providers to know if the physician actually saw the patient or if the physician saw the patient for a legitimate reason. Easing restrictions will only make it easier for health care providers to submit false claims, to give kickbacks to other providers so that they use certain telehealth companies, to up-code for prescriptions, and much more.

On the other hand, if states make these executive orders permanent, it is entirely possible that health care providers may be less inclined to engage in fraud and abuse. If providers are given more leeway and there are less restrictions on their practice, it is possible that providers will no longer feel the need to engage in fraud because they now have a larger pool of patients to see.

**VI. Why Are New Regulations Important?**

Telehealth and telemedicine have been in use for many years. The convenience and ease of seeing a health care provider from the comfort of one's own home is appealing to both patients and providers. The COVID-19 pandemic was the perfect recipe for telehealth and telemedicine to grow and be used for what it truly was made for. While the DOJ has engaged in very large takedowns due to telehealth fraud and abuse, Congress and local governments have enacted legislation and policies to combat and punish telehealth and telemedicine fraud. The government is working harder now more than ever to combat telehealth and telemedicine fraud during the pandemic. Through audits, whistleblower protections, new legislation, and waiving old legislation, the government is using every tool in its box to combat a very prevalent and rapidly growing issue.

---

[54] *Id.*

## VII. Whistleblowers

Whistleblowing is allowed and encouraged in the event of a False Claims Act (FCA) violation as the federal government often rewards whistleblowers for their actions. [55] The False Claims Act is a federal statute that was signed into Congress in 1863.[56] The statute was amended 100 years later to not only increase the amount of damages imposed on violators of the Act, but also to increase the rewards provided to whistleblowers.[57] The FCA has become an enormously successful method of punishing health care fraud in the United States.[58] Examples of false claims are magnified in the DOJ cases discussed earlier.

Whistleblowers play a crucial part in cracking down on telehealth fraud.[59] In 2020, $2.2 billion in FCA "settlements and judgments" were recovered, with more than $1.6 billion coming from "whistleblower-initiated cases." [60] With an exponential increase in the usage of telehealth for doctor's appointments, it is increasingly difficult for the OIG, CMS, and other government entities to identify fraud claims from legitimate ones.[61] Currently, under the False Claims Act, the government will allow whistleblowers to receive fifteen to thirty percent of the damages that the government receives.[62] While this monetary recovery may incentivize employees or other individuals to come forward with fraud and abuse claims, it can still be concerning to whistleblowers that they may not be protected by the law.[63]

---

[55] *The False Claims* Act, WHISTLEBLOWERS.ORG, https://www.whistleblowers.org/protect-the-false-claims-act/ (last visited Jan. 28, 2022).
[56] *The False Claims Act*, JUSTICE.GOV, https://www.justice.gov/civil/false-claims-act (last updated Feb. 2, 2022).
[57] The False Claims Act, *supra* note 55.
[58] *Id.*
[59] *Telemedicine fraud: How whistleblowers can report it and get rewarded*, PHILLIPS & COHEN, https://www.phillipsandcohen.com/whistleblower-resources/telemedicine-fraud-how-whistleblowers-can-report-it-and-get-rewarded/ (last visited Jan. 28, 2022).
[60] The False Claims Act, *supra* note 55.
[61] *Telemedicine fraud: How whistleblowers can report it and get rewarded*, *supra* note 59.
[62] *Id.*
[63] *Warren, Speier, Raskin, Introduce Legislation to Protect Whistleblowers During the COVID-19 Pandemic*, ELIZABETH WARREN, (Feb. 4, 2021), https://www.warren.senate.gov/newsroom/press-releases/warren-speier-raskin-introduce-legislation-to-protect-whistleblowers-during-the-covid-19-pandemic.

In 2021, a law was introduced to Congress that would impose enhanced whistleblower protections in the face of the COVID-19 pandemic.[64] This proposed legislation is named "The COVID-19 Whistleblower Protection Act."[65] The purpose of this Act is to encourage and ensure protection against Whistleblowers reporting violations against the CARES (Coronavirus Aid, Relief, and Economic Security) Act, which provided $200 million to the COVID-19 telehealth program.[66] Healthcare providers may join the CARES Act program by submitting documentation so long as they are a non-profit or public-eligible provider, allowing them to receive reimbursements for services.[67] The funds provided from the program can be used by telehealth providers to purchase equipment necessary for providing telehealth services.[68] If an employee or other individual suspects that a telehealth provider is using these funds for telehealth fraud, such as improper diagnoses or fake telephone calls, the new Whistleblower Protection Act will provide the whistleblower with enhanced protections, so they can feel safe reporting these fraudulent actions.[69]

**VIII. OIG Audits**

Each year, the Office of Inspector General Department of Health and Human Services will perform audits on companies that are contracted with the OIG in order to monitor and reduce fraud and abuse.[70] The OIG has acknowledged the dramatic increase in telehealth fraud and abuse in the

[64] COVID-19 Whistleblower Protection Act, H.R. 846, 117th Cong. (2021).
[65] *Id.*
[66] *Telemedicine fraud: How whistleblowers can report it and get rewarded*, *supra* note 59.
[67] *Id.*
[68] *Id.*
[69] Warren et al, *supra* note 63.
[70] *Office of Audit Services*, OFFICE OF INSPECTOR GENERAL, https://oig.hhs.gov/about-oig/office-audit-services/ (last visited Jan. 28, 2022).

wake of the COVID-19 pandemic.[71] Because of this, the OIG is implementing new oversight programs that will assess the way that telehealth is being used during the pandemic.[72]

One of the OIG's plans involves a two-phase audit program.[73] This program will involve auditing Medicare Part B programs.[74] Medicare Part B covers services and products including preventative health and medically necessary services, which includes services and products that are used to diagnose or treat medical conditions, such as Durable Medical Equipment.[75] Durable Medical Equipment, as displayed in the DOJ Takedowns discussed earlier, include equipment used for various blood tests.[76]

The first phase of the OIG audit plan will focus on whether the services being potentially offered through telehealth visits meet the proper Medicare requirements.[77] These assessments will include oversight of physician evaluations and illness management, as well as mental health services.[78] The OIG will especially focus on mental health services because of the CARES Act.[79] This Act, in conjunction with other CMS and HHS authorizations, allowed temporary waivers for Medicare recipients to be eligible to receive "psychotherapy" or mental health services via telehealth.[80] The purpose of this first phase is to ensure that these services, not previously rendered

---

[71] *Principal Deputy Inspector General Grimm on Telehealth*, OFFICE OF INSPECTOR GENERAL (Feb. 26, 2021), https://oig.hhs.gov/coronavirus/letter-grimm-02262021.asp?utm_source=oig-home&utm_medium=oig-hero&utm_campaign=oig-grimm-letter-02262021

[72] *Id*.

[73] *Audits of Medicare Part B Telehealth Services During the COVID-19 Public Health Emergency* (2021), OFFICE OF INSPECTOR GENERAL, https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000556.asp.

[74] *Id*.

[75] *What Part B* Covers, https://www.medicare.gov/what-medicare-covers/what-part-b-covers (last visited, Jan. 28, 2022).

[76] *Durable medical equipment (DME) coverage*, https://www.medicare.gov/coverage/durable-medical-equipment-dme-coverage (last visited, Jan. 28, 2022).

[77] *Audits of Medicare Part B Telehealth Services During the COVID-19 Public Health Emergency*, *supra* note 52.

[78] *Id*.

[79] *See generally, Audits of Medicare Part B Telehealth Services During the COVID-19 Public Health Emergency*, *supra* note 52.

[80] *Id*.

for Medicare recipients, are complying with Medicare and not being used for healthcare fraud and abuse.[81]

The second phase of the OIG audit plan will include audits on telehealth services regarding "distant and originating site locations, virtual check-in services, remote patient monitoring, use of telehealth technology, and annual wellness visits" to ensure that these services and programs are complying with Medicare requirements.[82] Essentially, the OIG audit plan will focus on two separate elements of telehealth during COVID-19.[83] The first phase will focus on actual services rendered, including services not previously allowed to be rendered to Medicare patients over telehealth prior to COVID-19.[84] The second phase will focus on the mode of delivering those services, including the actual telehealth technologies and the physical and virtual locations of the telehealth "offices."[85] Both phases will ensure that these telehealth providers are complying with Medicare requirements and are not engaging in fraud.[86] The results of these audits are frequently updated on the OIG's website.[87]

**IX. Potential Return to Pre-Covid Restrictions**

The previously mentioned Ryan Haight Act of 2008, which made it illegal for providers to prescribe controlled substances to a patient without an initial in person consultation, was waived in 2020 in response to the COVID-19 pandemic.[88] There has been no mention by Congress if the waiver will continue into 2022 or if the Ryan Haight Act will again be implemented; however, states have already taken matters into their own hands.[89] Florida proposed a bill in 2021 that will

---

[81] *Id.*
[82] *Audits of Medicare Part B Telehealth Services During the COVID-19 Public Health Emergency*, *supra* note 52.
[83] *See generally, Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] Haight, *supra* note 42.
[89] *Id.*

allow physicians to prescribe controlled substances via telehealth,[90] contradicting the previously enacted federal Ryan Haight Act. Conversely, in Minnesota, controlled substances in classes two through four still cannot be prescribed via telemedicine.[91]

There is importance in the restrictions of the Ryan Haight Act. For example, in-person consultations prior to prescribing controlled substances via telehealth can ensure that the medication is being prescribed for a legitimate purpose within the scope of the physicians practice, and to ensure the physician is complying with relevant laws.[92]

**X. State Licensing Requirements and Telehealth Regulations**

In response to the COVID-19 pandemic, the HHS and state governments implemented new telehealth waivers.[93] These waivers apply to states that did not previously allow out-of-state providers to render telehealth services to out-of-state patients.[94] The first change that was made to out-of-state telehealth services was an amendment made to the 2005 Public Readiness and Emergency Preparedness Act (PREP Act).[95] In 2020, HHS amended the Act to allow state governments to ease restrictions on certain healthcare measures.[96] The amendment specifically allowed telehealth providers to render services to out-of-state patients in response to the public health emergency.[97] The purpose of this amendment was to allow broader access for patients to telehealth services, and to ensure ease in treating and preventing COVID-19.[98] The amendment

---

[90] *Id.*
[91] *Id.*
[92] Libby Baney, et al., *The Future of Telehealth and the Ryan Haight Act Post-Pandemic* (April 22, 2021), https://nabp.pharmacy/news/blog/the-future-of-telehealth-and-the-ryan-haight-act-post-pandemic/
[93] *U.S. States and Territories Modifying Requirements for Telehealth in Response to COVID-19*, https://www.fsmb.org/siteassets/advocacy/pdf/states-waiving-licensure-requirements-for-telehealth-in-response-to-covid-19.pdf (last Updated Feb. 7, 2023).
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*

applied not only to states that did not already allow out-of-state telehealth services, but also applied to states that did allow it.[99] The amendment allowed the HHS and states to obtain services or products that would help combat the COVID-19 virus.[100]

In 2021, the Act was further amended to clarify that if a healthcare provider is rendering telehealth services to an out-of-state patient, the laws of the state where the healthcare provider is licensed shall be the governing law over the providers services.[101]

As of January 19, 2022, 23 states in the United States continued to use waivers that allow out-of-state physicians to provide telehealth services to out-of-state patients, and 19 states had implemented either long-term or permanent waivers.[102] For example, in March 2020, Illinois released an executive order allowing out-of-state providers not licensed to practice in Illinois to render telehealth services to patients that reside in Illinois as long as there was already an existing relationship between the patient and the physician.[103] On January 4, 2022, Illinois updated the executive order implementing further restrictions on out-of-state telehealth providers.[104] The new update required telemedicine providers to have an IL medical license to practice telemedicine in the state of Illinois, and those who did not have an Illinois license would therefore be subjecting themselves to Illinois jurisdiction, in the event that the provider should appear in court or be sued.[105] The Illinois waiver was implemented in response to the state's Disaster Proclamation,

---

[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *U.S. States and Territories Modifying Requirements for Telehealth in Response to COVID-19*, *supra* note 93.
[103] Ill. Dep't of Fin. and Pro. Regul., Guidance for Out-of-State Health Care Providers using Telehealth Services in Illinois (Mar. 30, 2020), https://idfpr.illinois.gov/News/2020/2020%2003%2030%20Guidance%20for%20Healthcare%20Providers%20using%20Telehealth%20Services%20in%20Illinois.pdf.
[104] *U.S. States and Territories Modifying Requirements for Telehealth in Response to COVID-19*, *supra* note 93, at 9.
[105] *Id.*

expiring "for established patients only" on May 31, 2022.[106] Illinois's waiver expanded the scope of telehealth services, allowing it to include all forms of healthcare, including mental health.[107] Illinois, along with the 22 other states that implemented similar telehealth waivers, have provided active updates on the status of their executive orders, as well as definitions of telehealth and healthcare services.[108]

Although state and federal governments have been implementing more restrictions, such as audits[109] and whistleblower protections[110] it is possible that easing restrictions may be just as beneficial as tightening restrictions. Moving forward, I predict that with easing restrictions, there may be less incentive for healthcare providers to commit healthcare fraud, including false billing and upcoding, because they will be able to reach a broader set of patients. Although in Illinois, the waiver stated that providers may only render services to patients with whom they already have a previously established relationship,[111] other states that did not have this requirement meant that providers could not render services and bill to Medicare or Medicaid for a vastly large number of patients, both in the state in which they are licensed to practice and out-of-state as well.

While individual states are expanding the reach of telehealth services in the wake of the pandemic, there remains a concern that telehealth fraud and abuse may remain undetected.[112] In 2020, the OIG conducted evaluations of 37 states, all of whom provided behavioral health services

---

[106] Ill. Dep't of Fin. and Pro. Regul., Proclamation to Invoke Emergency Powers to Modify Professional License and Certification Statutes and Regulations (Jan. 10, 2022), https://idfpr.illinois.gov/Forms/COVID19/Proclamation%20Out%20of%20State%20Telehealth%201%2010%2022.pdf.

[107] *U.S. States and Territories Modifying Requirements for Telehealth in Response to COVID-19*, *supra* note 93, at 8-9.

[108] *Id*.

[109] *Audits of Medicare Part B Telehealth Services During the COVID-19 Public Health Emergency*, *supra* note 52.

[110] The False Claims Act, *supra* note 55.

[111] *U.S. States and Territories Modifying Requirements for Telehealth in Response to COVID-19*, *supra* note 93, at 9.

[112] U.S. DEPT. HEALTH & HUM. SERVS. OFF. INSPECTOR GEN., OEI-02-19-00401, OPPORTUNITIES EXIST TO STRENGTHEN EVALUATION AND OVERSIGHT OF TELEHEALTH FOR BEHAVIORAL HEALTH IN MEDICAID 8-9 (Sept. 2021).

via telehealth.[113] Behavioral health services are health care services rendered to patients in need of treatment for mental illnesses.[114] The problem that the OIG was inquiring about was whether states providing behavioral telehealth were able to identify what type of behavioral services are provided via telehealth.[115] If the states are unable to identify the types of services being offered, then it is more likely that the states are also unable to closely monitor telehealth, making it difficult to accurately detect fraud and abuse.[116]

The OIG found that while 23 of the 37 states voiced concerns regarding providing fraud and abuse within behavioral telehealth, only 11 states actually implement specific telehealth fraud, waste, and abuse monitoring.[117] The states that did implement these monitoring protocols used various strategies such as "reviewing medical records, analyzing claims data, conducting outlier reports, and investigating complaints."[118] The OIG provided recommendations to CMS on how to combat this issue where states are not properly monitoring telehealth services to fraud and abuse.[119] One of these recommendations included CMS taking matters into their own hands and implementing fraud and abuse monitoring and oversight of states that provide behavioral health services via telehealth.[120] It was suggested that CMS should attempt to analyze the telehealth services in order to identify providers that may be using telehealth incorrectly or that may be billing improperly by looking at outliers in reimbursement claims that may be higher than normal.[121] CMS implementing a monitoring program even for behavioral health services provided via telehealth

---

[113] *Id.*
[114] *Substance Abuse and Mental Health Services Administration*, U.S. DEPT. HEALTH & HUM. SERVS., samhsa.gov/find-treatment (last Updated Feb. 15, 2023).
[115] Opportunities Exist To Strengthen Evaluation and Oversight of Telehealth for Behavioral Health in Medicaid, *supra* note 112.
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*

would be beneficial because CMS, unlike each individual state, has the power to conduct a national overview and can work closely with the states to indicate any common fraud schemes that may be taking place.[122]

## XI. Conclusion

Although federal and state governments are implementing new strategies and regulations to combat telehealth fraud, the use of telehealth is likely here for the long haul.[123] Federal, state, and local governments have a long way to go in terms of regulating telehealth and enforcing regulations that will reduce provider fraud.

There are many ways that telehealth fraud can be combated. DOJ takedowns, regulations, and licensing requirements are only the beginning. I imagine there will be many more takedowns and audits in the years to come as the government is more closely monitoring telehealth fraud specifically. With expanding telehealth regulations and increased chances of either intentional or unintentional fraud, both health care providers should be on high alert for changing laws, rules, and regulations.[124] Maintaining up to date compliance plans that are in accordance with state and federal standards are a good way for health care providers who wish to render services via telehealth ensure they are compliant and are not engaging in telehealth fraud schemes.[125] Overall, it is important to remember that telehealth is a very useful tool for those of us who cannot or simply do not wish to physically go to the doctor's office anymore.[126] It is important that we do not let the bad apples of the telehealth health care industry spoil the incredible invention that is telehealth.

---

[122] *Id.*
[123] *Patients appreciate the convenience of telehealth, but fraud is a concern*, MODERN HEALTHCARE (June 29, 2021, 12:05 PM), https://www.modernhealthcare.com/cybersecurity/patients-appreciate-convenience-telehealth-fraud-concern.
[124] Shilpa N. Gajarawala & Jessica N. Pelkowski, *Telehealth Benefits and Barriers*, 17 The J. for Nurse Practitioners 218, 220 (2021).
[125] *Id.* at 219.
[126] *See generally* Craig Guillot, *6 Reasons Telehealth is Now More Important Than Ever*, HEALTHTECH (May 14, 2020), https://healthtechmagazine.net/article/2020/05/6-reasons-telehealth-now-more-important-ever.