THOMSON REUTERS

Westlaw®

Telehealth's moment: The effect of COVID-19, first wave enforcement actions, and what lies ahead for compliance and enforcement in healthcare's hottest area

By Ty Howard, Esq., and Janus Pan, Esq., *Bradley Arant Boult Cummings LLP*

DECEMBER 30, 2020

INTRODUCTION

If 2020 has been defined by COVID-19 pandemic, the healthcare industry in 2020 might be defined by a related single issue — telehealth. Those phenomena are obviously connected. While telehealth has been around in varying forms for years, COVID-19 accelerated its growth, use, and acceptance in unprecedented ways.

With that growth comes changes. Reimbursement rules have evolved as telehealth has grown and become more accepted. We expect that trend to continue into next year. Likewise, compliance and enforcement will evolve as rapid industry changes occur, a phenomenon just now emerging with telehealth.

> While state Medicaid rules varied from state to state, reimbursement was likewise often limited based on geographic and modality factors.

Below we review the key changes in telehealth reimbursement, the effect of COVID-19, and the early stages of compliance and enforcement — and what the next wave of enforcement may look like in 2021 and beyond.

TELEHEALTH BACKGROUND

Telehealth, telemedicine, and related terms (collectively, "telehealth") refer to the exchange of medical information from one site to another through electronic communication to improve a patient's health.[1] The Centers for Medicare and Medicaid Services ("CMS") reimburses telehealth services under Medicare and Medicaid fee schedules, and commercial payors reimburse telehealth services by waiving patients' cost-sharing obligations.

CMS commonly describes telehealth and similar services as: "full telehealth visits," where patients use telecommunication technology for office, hospital visits and other services that otherwise occur in-person; "virtual check-ins," where patients communicate with practitioners through synchronous discussion over a telephone or exchange of information through video or images; and "e-visits," where patients have non-face-to-face patient-initiated communications with doctors through online patient portals.

But telehealth services also manifest in other forms, including remote monitoring, store-and-forward technologies, and synchronous and asynchronous chart review and consultations.

A COMPLEX LEGAL LANDSCAPE

Telehealth potentially implicates many different legal and regulatory authorities. First, federal fraud-and-abuse laws (and in many cases, their state-law counterparts) are at issue, including the Anti-Kickback Statute, 42 U.S.C. § 1320a-7b(b); the Stark Law, 42 U.S.C. § 1395nn; healthcare fraud, 18 U.S.C. § 1347; and many other more general-application statutes such as the False Claims Act, 31 U.S.C. § 3729 et seq.

Second, differing reimbursement rules apply — rules that, as described below, are changing rapidly. And finally, there are state-specific regulations and medical-profession-related laws that could be implicated by telehealth services, depending on the jurisdiction, the service, and the healthcare provider involved.

REIMBURSEMENT RULES

Much of the legal landscape turns on reimbursement issues, particularly from government insurers. Historically, CMS reimbursed telehealth services to increase service access to rural communities.

The general rules reflected this focus: qualified practitioners could be reimbursed for telehealth services provided to beneficiaries who were from certain rural areas with documented shortages of healthcare services, who obtained those services at a designated originating site (e.g., a hospital or skilled nursing facility) and through a two-way audio/video communication, and who obtained telehealth services covered by a limited range of CPT codes.

While state Medicaid rules varied from state to state, reimbursement was likewise often limited based on geographic and modality factors.

TELEHEALTH REIMBURSEMENT CHANGES AND THE PUBLIC HEALTH EMERGENCY

In 2020, CMS waived certain telehealth reimbursement rules to broaden access to all patients in response to the COVID-19 Public Health Emergency ("PHE"), currently set to end on January 20, 2021, unless extended by the U.S. Department of Health and Human Services ("HHS") Secretary.[2]

The below chart summarizes major changes in Medicare reimbursement for telehealth services in light of CMS' promulgated COVID-19 waivers and rules.

Medicare Reimbursement Requirement	Pre-COVID	Post-COVID
Rural Originating Site	Patients must be at rural originating site, such as physician's office or hospital (42 C.F.R. § 410.78 (b)(3)-(4)).	Practitioners can provide telehealth services to any Medicare beneficiary at any location, including when the provider and beneficiary do not have a prior existing relationship. For most specialties, CMS still requires that the telehealth medium contain both audio and visual capabilities (e.g., not merely a cell phone call). Providers can also use code modifiers to receive telehealth reimbursement equivalent to in-person services. CMS pays for patient-initiated, non-face-to-face "e-visits," including audio-only visits.[3]
Covered Telehealth CPT Codes	Medicare covers telehealth CPT code for that year (42 U.S.C. § 1395m(m)(4)(F)).	CMS' Telehealth Service PHE list contains eligible CPT codes for audio-only services. Approximately 240 codes are available for reimbursement if provided via telehealth, including evaluation and management services, behavioral health, and patient education services, some of which may be provided on an audio-only basis.[4]
Physician Telehealth License	Physicians must be licensed to practice telehealth under the state law of the distant site location (42 U.S.C. § 1395m(m)(4)(F)).	CMS temporarily waives requirements for physicians to be licensed in the patient's state if they instead enroll in Medicare, have a valid license in the state where they enroll in Medicare, are furnishing services in the state with an emergency, and are not excluded from practicing in that state or any other state that is part of the emergency.[5]
Physician Supervision	Physicians must directly supervise telehealth services (42 C.F.R. § 410.26(b)(5)).	Physicians may supervise using live video.[6]
Billing Practitioner	Only the consulting physician who controls the medical exam may bill Medicare (42 C.F.R. § 414.65(a); 42 C.F.R. § 410.26(b)(5)).	Nearly all types of Medicare-enrolled practitioners can now bill for telehealth services. CMS pays for brief video or phone patient-initiated "virtual check-ins" that are not related to a medical visit in the past week.[7]
Medicare Advantage Organization Services	Medicare Advantage organizations may only furnish telehealth services that are not covered under 42 U.S.C. § 1395m by using contracted providers; "[c]overage of benefits furnished by a non-contracted provider through electronic exchange may only be covered as a supplemental benefit" (42 C.F.R. § 422.135(d)).	CMS informed Medicare Advantage organizations that if they cover telehealth services beyond prior-approved CMS services, CMS will exercise its enforcement discretion until it determines no longer necessary.[8]
Nursing Facility Resident Subsequent Visits	A physician must see nursing facility residents at least once every 30 days for the first 90 days after admission, and at least once every 60 days thereafter (42 C.F.R. § 483.30(c)).	Physicians may furnish subsequent nursing visits via telehealth once every 14 days in the nursing facility setting.[9]
Stark Law	The physician self-referral law (also known as the "Stark Law") prohibits a physician from making referrals for certain healthcare services payable by Medicare if the physician (or an immediate family member) has a financial relationship with the entity performing the service (42 U.S.C. § 1395nn).	Some of the restrictions regarding when a group practice can furnish medically necessary designated health services (DHS) in a patient's home are loosened. For example, any physician in the group may order medically necessary DHS that is furnished to a patient by one of the group's technicians or nurses in the patient's home contemporaneously with a physician service that is furnished via telehealth by the physician who ordered the DHS.[10]

CMS separately issued a FAQ document in June 2020 granting states broad authority to utilize telehealth within their Medicaid programs. States would use Social Security Act Section 1915(c)'s Appendix K authority to waive existing Medicaid telehealth restrictions.[11]

As of October 2020, all 50 states and the District of Columbia's Medicaid programs reimburse for live video telehealth services; 21 states' Medicaid programs reimburse for remote patient monitoring; 18 states' Medicaid programs reimburse for store-and-forward telemedicine services; and 27 states and the District of Columbia's Medicaid programs permit the home to serve as an "originating site" under certain circumstances.[12]

Commercial payors also waived patient cost-sharing obligations in 2020. Anthem and UnitedHealthcare Group waived cost-sharing for telehealth visits through December 31, 2020.[13]

Aetna increased its payments for telephone-only visits from March to September 2020, but reduced such payments after September 2020 and also stopped the waiver of cost-sharing obligations for in-network telemedicine visits in June 2020.

However, Aetna extended its cost-sharing waiver for outpatient behavioral and mental health counseling telehealth services through December 31, 2020.[14] Humana has also waived all out-of-pocket costs for telehealth visits through December 31, 2020.[15]

Cigna's cost-sharing waivers for telehealth services end either on December 31, 2020 or at the end of the COVID-19 PHE (January 20, 2021), depending on the specific Cigna plan and whether the visit is related to COVID-19.[16] However, Cigna also permanently extended its new telemedicine policy to reimburse live video services for select CPT and HCPCS codes.[17]

'TELEHEALTH FRAUD' AND THE FIRST WAVE OF ENFORCEMENT

To date, most cases that have been termed "telehealth" or "telemedicine" fraud have usually involved fraudulent billing schemes with medically unnecessary durable medical equipment ("DME"), compounded medications, and cancer genomic ("CGx") testing.

For example, the U.S. Department of Justice's ("DOJ") "Operation Brace Yourself" (April 2019),[18] "Operation Double Helix" (September 2019),[19] and national healthcare "takedown" (November 2020) all spawned such cases that have been referred to as telemedicine or telehealth fraud.

But the terminology is misleading. In most of those cases, telehealth is a tangential, not defining, feature of the fraud. Many of the DME and CGx scams are no more "telemedicine fraud," than a bank robbery in which the robbers facilitate their crime through a getaway car is "automobile fraud."

In other words, telemedicine may have facilitated the crime, but it was not central to it. In fact, some cases do not even rise to the level of tangential telehealth involvement, as there is no actual telemedicine at all, just fraudulent billing after a nonexistent physician evaluation, whether done via a telehealth platform or otherwise.

Take for example the prototypical telemedicine scheme. While the schemes vary, all involve three elements:

(1) harvesting beneficiaries,

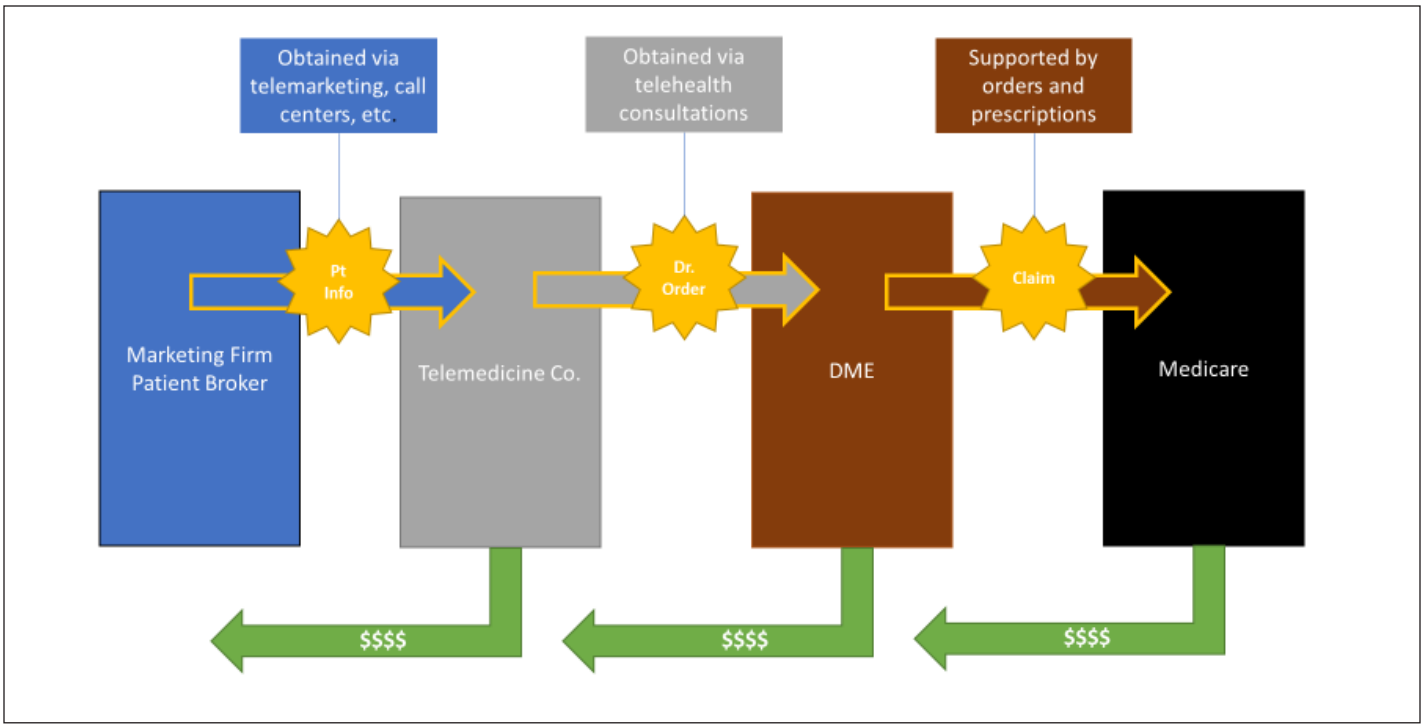
(2) obtaining the required documentation for a claim (usually a doctor's order), and

(3) submitting the fraudulent claim with that documentation for reimbursement. A marketing firm or patient broker often locates and harvests beneficiaries.

This can be done through call centers (often overseas), telemarketers, and other types of solicitation such as at a health fair. Next, that beneficiary information needs to be combined with the documentation necessary to support claims for payment. That documentation is typically a doctor's order of some sort for a piece of DME equipment or a prescription for a compounded cream or laboratory testing.

To obtain that information efficiently and in high volumes, telehealth visits or consults are performed between the beneficiary and a contracting telemedicine healthcare provider. Finally, that beneficiary information, combined with the supporting information, must be submitted for reimbursement.

In the DME example, the DME company receives the reimbursed funds from the payor, as illustrated in the below chart.



As shown, the telemedicine company enables healthcare providers to connect with patients, usually through a technology platform. The healthcare providers are generally independent contractors who contract with the telemedicine company to provide patient consultations for a flat fee. The degree to which the healthcare providers are informed and understand their role in the larger scheme varies widely.

> If telehealth enforcement follows the pattern of other areas, a shift will occur to more nuanced fact patterns, involving more gray area between appropriate and sanctionable conduct.

In the most transparent schemes, there is effectively no telemedicine aspect at all. The beneficiary information is collected by the call center; doctors' orders or prescriptions are created; and the physician then simply signs off without any interaction with the patient.

Other variations may involve the physician reviewing the notes of the intake personnel, listening to a recorded call with the patient, having an audio-only consultation with the patient, or conducting an audio- and video-based consultation before signing off on the necessary order.

The basis for criminal liability in such cases is no different than in any other fraudulent billing scheme. In general, liability is based on the lack of medical necessity (the DME, testing, or other service was not medically necessary for the patient) or a kickback theory (the claim for the DME, testing or other service was tainted by a kickback given or received) or both.

Telemedicine is only relevant to these schemes in that use of technology allows the volume and speed of the billing scheme to increase significantly.

We refer to these early telemedicine fraud cases as the "first wave" of enforcement because they are the initial enforcement actions coming to light.

First-wave cases usually share some common features: They are somewhat novel in that they exploit previously unknown compliance gaps or other new opportunities. The conduct is usually not very nuanced and often is clearly criminal. The losses associated with the misconduct can be quite high because the systems to detect the particular misconduct may not be established yet.

In sum, these cases represent low-hanging fruit — the equivalent of "phantom patient" cases in healthcare fraud generally. Similar first-wave enforcement has been seen in other areas, including cases involving misconduct within compounding pharmacies, home health, hospice, and many industries or subindustries outside of healthcare.

WHAT'S THE NEXT WAVE IN TELEHEALTH ENFORCEMENT?

If the current telemedicine cases constitute the first wave, what comes in the next wave? A "wave" is, of course, inexact and really just a construct for how enforcement develops and evolves over time. And waves are not exclusively sequential;

in any area, there will always be cases that involve seemingly brazen or clear misconduct.

But if telehealth enforcement follows the pattern of other areas, a shift will occur to more nuanced fact patterns, involving more gray area between appropriate and sanctionable conduct. For telehealth, we expect that to mean several potential trends:

- More cases will be premised on the actual reimbursement rules for telehealth specifically, rather than on broader criminal conduct;
- More regulatory and civil enforcement as opposed to just criminal prosecutions will occur. For example, expect that prosecutors will increasingly turn to the civil False Claims Act to combat alleged misconduct. With their lower standards of proof, many civil and regulatory provisions will ensnare conduct that might not rise to criminal wrongdoing.
- In the near term, telehealth enforcement may also overlap with enforcement of COVID-related programs, as the two areas may be factually intertwined.
- More broadly, as telehealth becomes less of a specialty within healthcare and just another means of healthcare delivery, telehealth practitioners and companies will face all the typical compliance landmines associated with their substantive area of practice.
- The technological advances that allow telehealth to increase the volume of billable events and generally improve efficiency in healthcare delivery will concurrently increase the enforcement security.
- And finally, the continued rapid changes — in reimbursement rules, licensure requirements, technology, and other regulatory authority — will create an even more challenging compliance environment for telehealth companies and will require regular monitoring to avoid enforcement mishaps.

CONCLUSION

Telehealth has great promise, much of which is yet to be realized as technology and medical practices continue to evolve. But for practitioners and telehealth companies, telehealth also carries increasing risk. Balancing that promise and the risk, particularly in a fast-changing compliance environment, will ultimately determine telehealth's winners and losers — in 2021 and beyond.

Notes

[1] "Medicare Telemedicine Health Care Provider Fact Sheet," CMS.gov (Mar. 17, 2020), available at https://go.cms.gov/38cQdzY.

[2] "Determination that a Public Health Emergency Exists," U.S. Dept. of Health and Human Srvcs. (Jan. 31, 2020) (renewed Oct. 2, 2020), available at https://bit.ly/3gMGHay; "Public Health Emergency Declaration," U.S. Dept. of Health and Human Srvcs. (Nov. 26, 2019), available at https://bit.ly/3oVZCCE.

[3] "Medicare Telemedicine Health Care Provider Fact Sheet," CMS.gov (Mar. 17, 2020), available at https://go.cms.gov/34fSAkl; "COVID-19 Emergency Declaration Blanket Waivers for Health Care Providers," CMS.gov (Dec. 1, 2020), available at https://go.cms.gov/34fSCIZ; "Hospitals: CMS Flexibilities to Fight COVID-19," Ctrs. for Medicare and Medicaid Srvcs. (Nov. 4, 2020), available at https://go.cms.gov/3r0WdEb; "Medicare and Medicaid Programs; Policy and Regulatory Revisions in Response to the COVID-19 Public Health Emergency," Interim Final Rule, Ctrs. for Medicare and Medicaid Services (CMS-1744-IFC) (Mar. 26, 2020), available at https://go.cms.gov/34dEShE.

[4] "List of Telehealth Services," Ctrs. for Medicare and Medicaid Srvcs. (Oct. 14, 2020), available at https://go.cms.gov/3r1lQ71; see also CY2021 Medicare Physician Fee Schedule Final Rule (Dec. 2, 2020), Ctrs. for Medicare and Medicaid Srvcs., available at https://bit.ly/2KpGXAe (prepublication copy); see also Cubanski, Juliette and Freed, Meredith, "FAQs on Medicare Coverage and Costs Related to COVID-19 Testing and Treatment," Kaiser Family Foundation (Dec. 4, 2020), available at https://bit.ly/3ae2sPl.

[5] "Telehealth Coverage Policies in the Time of COVID-19," Ctr. for Connected Health Policy (Sept. 15, 2020), available at https://bit.ly/34fSUQ5.

[6] "Telehealth Coverage Policies in the Time of COVID-19," Ctr. for Connected Health Policy (Sept. 15, 2020), available at https://bit.ly/3gQuzoR.

[7] "COVID-19 Emergency Declaration Blanket Waivers for Health Care Providers," CMS.gov (Dec. 1, 2020), available at https://go.cms.gov/3r0Wnvh; "Medicare Telemedicine Health Care Provider Fact Sheet," CMS.gov (Mar. 17, 2020), available at https://go.cms.gov/34dFaoK.

[8] Memorandum from Centers for Medicare and Medicaid Services to All Medicare Advantage Organizations, Part D Sponsors, and Medicare-Medicaid Plans (Mar. 10, 2020), Ctrs. for Medicare and Medicaid Srvcs., available at https://go.cms.gov/34gmTHt.

[9] CY2021 Medicare Physician Fee Schedule Final Rule, Section II.D.4 (Dec. 2, 2020), Ctrs. for Medicare and Medicaid Srvcs., available at https://bit.ly/383t2rK (prepublication copy).

[10] "Physicians and Other Clinicians: CMS Flexibilities to Fight COVID-19," CMS.gov, available at https://go.cms.gov/3nnceCm (last accessed: Dec. 14, 2020).

[11] "COVID-19 Frequently Asked Questions (FAQs) for State Medicaid and Children's Health Insurance Program (CHIP) Agencies," Pages 34-39, Ctrs. for Medicare and Medicaid Srvcs. (June 30, 2020), available at https://bit.ly/3oUodaN.

[12] "State Telehealth Laws and Reimbursement Policies At a Glance," Ctr. for Connected Health Policy (Fall 2020, available at https://bit.ly/37ZyaNe.

[13] "Information from Anthem for Care Providers about COVID-19 (Updated October 9, 2020)," Anthem (Oct. 9, 2020), available at http://anthem.ly/2KpNkDF; "Talk to a doctor from home using telehealth services," UNITEDHEALTHCARE, available at https://bit.ly/3afHyPU.

[14] "COVID-19: Telemedicine FAQs," Aetna, available at https://aet.na/37iM5iv (last accessed: Nov. 24, 2020).

[15] "Humana expands coverage for telehealth care through 2020," Humana, available at https://huma.na/3mo0n5w (last accessed: Nov. 24, 2020).

[16] "Cigna's response to COVID-19," Cigna (Oct. 30, 2020), available at https://bit.ly/2KnSSOS.

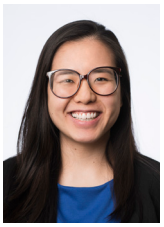
[17] "Reimbursement Policy," Cigna (Jan. 1, 2021), available at https://bit.ly/3r1K6af.

[18] "Billion-Dollar Medicare Fraud Bust," FBI.gov (Apr. 9, 2019), available at https://bit.ly/3oVs2g8.

[19] "Nineteen defendants charged in largest healthcare fraud scheme in Southern District history," U.S. Dept. of Justice (Sep. 27, 2019), available at https://bit.ly/2KtcocV.

This article was published on Westlaw Today on December 30, 2020.

ABOUT THE AUTHORS



TyHoward (L) is a partner in **BradleyArant Boult Cummings'** office in Nashville, Tennessee, and chairs the firm's Government Enforcement and Investigations Practice Group. He applies his perspective as a former state and federal prosecutor to defending and counseling businesses and individuals involved in government investigations, compliance matters, False Claims Act and whistleblower cases, related business litigation, and white-collar criminal matters. He can be reached at thoward@bradley.com. **JanusPan** (R) is an associate in Bradley's Healthcare Practice Group. Her practice focuses on assisting health care entities in transactional and regulatory matters, and she advises clients on Medicare and Medicaid reimbursement and hospital mergers and acquisitions. Pan also has experience with government investigations of health care entities and compliance considerations. She can be reached at jpan@bradley.com. This article reflects the situation at the time it was written based on the rapidly changing nature of the COVID-19 pandemic.