ALSTON & BIRD

WWW.ALSTON.COM

Health Care / Health Care Litigation ADVISORY ■

NOVEMBER 5, 2020

Telehealth Turbulence: Explosive Expansion Coincides with Emerging Enforcement Priorities

*by **Jason Popp**, **Sean Sullivan**, and **Andrew Liebler***

As the COVID-19 pandemic continues, health care providers around the county have broadly embraced telehealth. This delivery model allows providers to safely see more patients per day from remote settings. Telehealth has enjoyed vocal support from the U.S. Surgeon General, the Department of Health and Human Services (HHS), and the administrator for the Centers of Medicare and Medicaid Services (CMS). This support has been magnified by substantially relaxed regulation during the pandemic and ongoing public health emergency (PHE) and by financial stimulus aimed at expanding telehealth capacity. But as the telehealth floodgates have opened, telehealth liability pitfalls are rapidly surfacing.

A series of recent "takedowns" coordinated by the Department of Justice (DOJ), HHS Office of Inspector General (HHS-OIG), and FBI have yielded nearly $6 billion in recoveries related to telehealth.

A Relaxed Regulatory Environment and Financial Stimulus Has Led to a Telehealth Explosion

The COVID-19 pandemic necessitated a rapid transition to remote health care delivery. To promote telehealth, HHS and CMS made various changes to the Medicare regulatory landscape, including relaxing certain regulations and temporarily waiving others. In addition, Congress, through the CARES Act, provided various forms of financial stimulus to promote telehealth uptake. A few highlights of these efforts include:

- **Qualifying Practitioners and Sites:** For the duration of the PHE, any health care professional who can bill Medicare may furnish Medicare telehealth services to all patients in all settings (including physical, occupational, and speech therapists), as clinically appropriate. For the duration of the PHE, these services may now be provided anywhere in the U.S., and no preexisting patient relationship is required.
- **Licensure Flexibility:** During the PHE, practitioners do not need to be licensed in the state where they furnish services, provided that they have a valid license in another state where they are enrolled in Medicare, are contributing to relief efforts, and are not affirmatively excluded in any state. While state law still applies, and the practitioner should be legally permitted under state law to provide services where the patient is located, most states have also loosened licensure to some extent during the PHE.

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

- **Virtual Direct Supervision:** Direct supervision, typically required for "incident to" services, and supervision of medical residents performing procedures may now occur through the supervising physician's virtual presence with real-time audio-video technology.
- **Controlled Substances:** The PHE constitutes an ongoing exception to the Ryan Haight Act, which allows practitioners to prescribe controlled substances through a telemedicine encounter alone.
- **Telephone Evaluation and Management:** Telephonic evaluation and management services, which are normally not covered by Medicare, are now reimbursable. This allows any practitioner who can independently bill Medicare to now provide reimbursable, non-face-to-face, audio-only patient consultations.
- **Deductible and Copay Waivers:** Typically, the provision of a deductible or copay waiver to a patient may raise anti-kickback concerns. However, during the PHE, telehealth providers may now waive patient deductibles and copayments.
- **Billing Codes:** CMS has approved new billing codes for the reimbursement of telehealth services. CMS has also announced that it will allow Medicare Advantage plans to use telehealth to help set payment rates.
- **Financial Stimulus (FCC):** The expansion of telehealth services was buttressed by the CARES Act, which set aside $200 million for use through the Federal Communications Commission (FCC) to help medical groups install technology needed to fund and sustain telehealth demands. This funding was allocated to health organizations through an application process, which is now complete. Among funding recipients are major hospitals and health networks.
- **Financial Stimulus (HHS & IHS):** The CARES Act also set aside $27 billion for the HHS Public Health and Social Services Emergency Fund to respond to the COVID-19 pandemic by, among other things, developing telehealth access and infrastructure. In addition, the Act set aside $1.032 billion for the Indian Health Service department to, among other things, increase telehealth capacity.

All of these actions have coincided with, and contributed to, a boom in the use of telehealth. However, although the recent regulatory flexibilities have not yet directly resulted in adverse enforcement related to telehealth provided under the relaxed regulatory environment, the recent growth of telehealth has been accompanied by an increase in fraud enforcement activity.

Telehealth Fraud Prosecutions Become Enforcement Priority

On September 30, 2020, the DOJ and HHS-OIG announced their largest-ever health care fraud enforcement action. This so-called "health care fraud takedown" featured criminal charges against 345 defendants across 51 federal judicial districts for the submission of over $6 billion in false and fraudulent claims to federal health care programs. Of that total, more than $4.5 billion was connected to telehealth fraud.

In the telehealth takedown, charges were pressed against 86 defendants in 19 judicial districts, including four telehealth company executives. In one case, the government charged telehealth executives with allegedly

paying doctors and nurse practitioners to order medically unnecessary durable medical equipment (DME), genetic and diagnostic testing, and medications. The patients these requests were made for had allegedly received little or no consultation with providers, or in some cases, had only brief telephone conversations with them. The government alleges that in exchange for this business generation, DME manufacturers and laboratories also paid kickbacks to telehealth executives and companies.

As is common in health care fraud cases, the CMS Center for Program Integrity also announced that it has taken administrative actions relating to telehealth fraud, revoking the Medicare billing privileges of 256 medical professionals for their alleged involvement in telehealth schemes.

This takedown is a continuation of DOJ enforcement activity in the area, including the 2019 "Operation Brace Yourself" telehealth and DME takedown. That aptly named enforcement effort, which targeted billing for orthotic braces, was connected to over $1 billion in suspected fraudulent Medicare billing. This 2019 action included criminal charges against 24 individuals, including telehealth employees and executives, who allegedly operated a scheme through which DME companies hired a foreign firm to market orthotic braces to Medicare patients regardless of need. Those device companies allegedly then paid telehealth doctors kickbacks to prescribe unnecessary orthotics with little or no patient interaction. In addition to criminal charges, more than 100 DME companies were suspended or excluded from Medicare as part of the takedown.

The takedown is also joined by a third telehealth takedown ("Operation Rubber Stamp"), announced October 7, 2020. Led by the U.S. Attorney for the Southern District of Georgia, that effort targets over $1.5 billion in alleged fraudulent billings relating to billing for unnecessary DME, testing, and medication provided to patients following telehealth consultations. The scheme targeted by this takedown is similar to others, but was allegedly driven by the collection and sale of patient data to DME providers, labs, and pharmacies.

Emerging Areas of Risk and Theories of Liability

These and other telehealth fraud actions indicate a few key areas of telehealth risk and theories of liability that are certain to persist as telehealth continues to grow:

- **Telehealth Marketing:** A key issue in recent cases is the use of marketing programs used to generate reimbursable billings. In one case, the government scrutinized marketing efforts made by a genetic testing company to seniors, capitalizing on the seniors' fear of developing cancer. These efforts were made directly to patients, rather than through physicians, through the use of telemarketing and in-person, recruiter-based marketing at health fairs. The company allegedly conspired with, and paid kickbacks to, telehealth companies that supplied physicians who would order cancer genomic (CGx) tests despite the lack of a medically necessary need for them. In another case, nationwide telemarketing was used in a similar scheme to generate patient "leads" for reimbursable orthotics. Notably, this same telemarketing-based lead generation, targeted at Medicare beneficiaries, has been a component of disputes between telehealth companies and private insurers as well.
- **Unnecessary Medical Services:** Recent telehealth "takedown" cases frequently involve suspected billing for unnecessary medical services. For example, in the genetic testing cases, the government

alleged that the particular tests themselves were medically unnecessary because they could not be used to diagnose patients and were prescribed without regard to patient symptoms or need. These cases made up a substantial portion of the $2.1 billion September 2019 takedown and a part of the 2020 takedown as well. In Operation Brace Yourself, prosecutors scrutinized the provision of orthotic braces to patients where little or no patient examination occurred or need for the equipment existed. These prosecutions are often data-driven and uncovered by enforcement authorities through monitoring of billing and prescribing patterns.

- **Improper Referrals and Relationships:** The telehealth fraud cases charged by the government in the last two years are often built on a series of alleged kickbacks. Commonly, two kickbacks are alleged—one kickback payment from a laboratory or device manufacturer to a telehealth company, and one from the telehealth company to prescribing physicians. Additionally, marketers involved in generating Medicare beneficiary leads have been charged and prosecuted for receiving kickbacks as a part of these purported conspiracies. These multiparty cases are also typically prosecuted as conspiracies.
- **Individual Executive Liability:** The government has also shown a willingness to prosecute corporate executives in their individual capacities. For example, a series of September 2019 indictments against 35 individuals included charges against telehealth executives and owners of marketing and testing companies. The indictments of telehealth executives in particular illustrate the central organizational and operational role the government believes that telehealth companies play in these schemes.
- **Upcoding and Billing:** While not a centerpiece of the record-setting frauds prosecuted in the DOJ's recent takedowns, common forms of health care fraud such as upcoding and billing fraud remain prevalent. For example, the tiered reimbursement rates for telehealth services present the opportunity to bill virtual check-in appointments as more fulsome telehealth visits subject to higher reimbursement rates.
- **Vulnerable Patient Populations:** Operation Brace Yourself, Operation Rubber Stamp, and other recent telehealth enforcement actions have uncovered an unfortunate trend of purported telehealth companies targeting elderly and other vulnerable patient populations, often through unsolicited telephone call schemes common among telemarketing companies.

Best Practices to Minimize Risk

The surge in telehealth use throughout the industry presents substantial opportunities to deliver health care efficiently, safely, and to more patients than ever before. Recent prosecutions and enforcement activity illustrate many areas of risk that telehealth participants should account for in taking advantage of these opportunities. In particular, a handful of practical steps can assist telehealth participants in avoiding these issues:

- **Evaluate Marketing Methods and Partners:** Telehealth participants that conduct their own marketing or use third parties to guide marketing efforts should evaluate their marketing programs in light of the government's focus in this area. In particular, participants should consider both the nature and content of marketing efforts to ensure that they are both legally appropriate and do not create an appearance of impropriety.

- **Review Compensation Arrangements with Providers:** Telehealth providers should ensure that existing policies and procedures related to relationships with referral sources and fraud and abuse are effective and cover all areas of telehealth service offered. Providers should also review and consider the nature of their compensation relationships with referral sources to ensure that they comply with the Anti-Kickback Statute and Stark Law.
- **Evaluate Utilization, Prescribing, and Billing Trends:** Enforcement authorities commonly uncover and develop health care fraud cases by mining and analyzing utilization, prescribing, and billing data. Telehealth providers should be aware of the data generated by their activities and actively monitor this information for compliance purposes.
- **Monitor Regulatory and Enforcement Landscapes:** Substantial regulatory changes have given way to broad telehealth utilization this year. But it remains to be seen how long these changes will persist and what regulatory flexibilities will be permanent, if any. Telehealth providers should be cognizant of these changes, and enforcement activity in this area, in tailoring their ongoing business practices.

Looking Forward

The massive growth of telehealth and the benefits realized by those who embrace remote health care suggest that telehealth enforcement activity will continue through and after the pandemic. A key question remains whether, and to what extent, the relaxed regulatory environment for telehealth will persist once the pandemic ends. CMS has indicated that it will place "a strong emphasis" on program integrity and cost in considering whether to make any telehealth flexibility changes permanent. But the contours of this regulatory landscape remain uncertain, and many of the flexibilities will require congressional action to last beyond the pandemic. Alston & Bird will continue to closely monitor this regulatory environment and the enforcement activity around it to keep telehealth stakeholders informed.

Alston & Bird has formed a multidisciplinary response and relief team to advise clients on the business and legal implications of the coronavirus (COVID-19). You can view all our work on the coronavirus across industries and subscribe to our future webinars and advisories.

You can subscribe to future *Health Care* and *Litigation* advisories and other Alston & Bird publications by completing our **publications subscription form**.

Alston & Bird has launched the **Digital Transformation of Health Care**, a new initiative that advances our commitment to an industry approach to providing legal services in the health care space. Our health care and technology teams can assist with establishing or significantly growing telehealth capabilities and navigating the regulatory landscape.

If you have any questions, or would like additional information, please contact any of the following:

Health Care Team

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Justin Chavez
404.881.7898
justin.chavez@alston.com

Joyce Gresko
202.239.3628
joyce.gresko@alston.com

Elinor A. Hiller
202.239.3766
elinor.hiller@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Michael H. Park
202.239.3630
michael.park@alston.com

Heidi A. Sorensen
202.239.3232
heidi.sorensen@alston.com

Robert D. Stone
404.881.7270
rob.stone@alston.com

Sean Sullivan
404.881.4254
sean.sullivan@alston.com

Health Care Litigation Team

Brian D. Boone
704.444.1106
202.239.3206
brian.boone@alston.com

R. Joseph Burby IV
404.881.7670
joey.burby@alston.com

Mark T. Calloway
704.444.1089
mark.calloway@alston.com

Kimberly K. Chemerinsky
213.576.1079
kim.chemerinsky@alston.com

Daniel G. Jarcho
202.239.3254
daniel.jarcho@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

Edward T. Kang
202.239.3728
edward.kang@alston.com

Meredith Jones Kingsley
404.881.4793
meredith.kingsley@alston.com

Andrew J. Liebler
404.881.4712
andrew.liebler@alston.com

Wade Pearson Miller
404.881.4971
wade.miller@alston.com

Paul N. Monnin
404.881.7394
paul.monnin@alston.com

Jason D. Popp
404.881.4753
jason.popp@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Samuel R. Rutherford
404.881.4454
sam.rutherford@alston.com

Frank E. Sheeder
214.922.3420
frank.sheeder@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

© ALSTON & BIRD LLP 2020

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: 3700 Hulen Street ■ Building 3 ■ Suite 150 ■ Fort Worth, Texas, USA, 76107 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333