PG Bulletin
December 16, 2020

Enforcement 2020: Telehealth Providers Move to the Top of OIG's Watch List

Joshua M. Robbins (Buchalter)
Anne M. Brendel (Goodwin)

This article is brought to you by AHLA's Health Information and Technology Practice Group.

When the 2019 Novel Coronavirus (COVID-19) hit the United States, the health industry shifted its care delivery platform from in-office to online and venture capitalists invested heavily in telehealth technology platforms that were already booming from a couple of years prior. Now that the digital health gold rush has slowed down, and many health care providers have transitioned most (if not all) patient visits from their offices to their computers, providers may be due for a compliance check-up themselves.

Undoubtedly, providers who rushed to stay afloat during the initial outbreak of COVID-19 by building or strengthening their telehealth infrastructure to continue to provide services to patients in their homes and decrease the risk of spreading the virus may not have obtained legal counsel's review of related arrangements. In addition, health technology companies largely unfamiliar with health care's complex regulatory regime are entering the telehealth space at lightning speed.

In September 2020, the Department of Health and Human Services Office of Inspector General (OIG) participated in a 2020 Nationwide Telefraud Takedown, resulting in charging over 345 defendants (telemedicine executives, practitioners, telemedicine companies, pharmacies, and laboratories) across the nation with participating in fraud schemes involving more than $6 billion in alleged federal health care program losses.[1] In the wake of the takedown, telehealth providers would be well-advised to take a step back and ensure their policies and procedures are compliant. As part of that nationwide sweep, the U.S. Department of Justice and the OIG have alleged $4.5 billion in false and fraudulent claims related to telehealth, submitted by more than 86 criminal defendants in 19 judicial districts. More cases are likely to follow. Providers seeking to avoid or mitigate liability in future government actions should consider a proactive approach to compliance in this space.

Benefits and Risks of Telehealth

Telehealth is unique in its extraordinary capacity for patient outreach, including patients living in rural or remote areas or those who have difficulty travelling. A virtual practice is not limited to patients who call or come into the provider's office or to referrals. Rather,

subject to state residence and insurance limitations, telehealth services are accessible by anyone at any time. This provider- and consumer-friendly feature has become critical during the pandemic and has led to an explosion in demand.

The government has responded accordingly. Following HHS' declaration of a public health emergency as the result of the COVID-19 outbreak last January, the Centers for Medicare & Medicaid Services (CMS) waived several reimbursement requirements that had previously posed hurdles for providers. In particular, CMS waived the interactive telecommunications systems requirement, expanded the types of practitioners authorized to provide and receive payment for telehealth services, and added reimbursable telehealth services.[2]

But there is a darker side to telehealth: the same convenience and ease of access that makes it attractive to patients can create an increased risk of billing mistakes and fraud. The elimination of face-to-face provider-patient meetings, and the substitution of electronic records for in-person sign-in sheets and physical signatures, creates new means to falsify service records and support medical necessity determinations. Moreover, the increased geographic scope and efficiency that telehealth provides massively increases the potential volume of a practice, making it easier to make innocent billing and documentation errors and for unscrupulous providers to rack up false claims.

Consider, for example, the various small-scale "pill mills" (providers, clinics, and pharmacies that inappropriately prescribed or dispensed astronomical amounts of controlled substances) contributing to the opioid addiction crisis in the Appalachian region and elsewhere. The explosion of telehealth could lead to even more widespread issues, particularly following the Drug Enforcement Administration's temporary exemptions to the Ryan Haight Act's requirement to conduct an in-person examination before prescribing controlled substances.[3] Via telehealth, patients can more easily obtain prescriptions by searching for providers online, and providers are more accessible to patients. Such access has increased potential for misuse on both sides. For example, patients may obtain multiple prescriptions for controlled substances and fill them at various pharmacies more quickly online than in-person. While providers are capable of prescribing and dispensing controlled substances more quickly than ever, this volume and ease could leave some providers more susceptible to focusing on increased revenues instead of medical necessity or appropriate care requirements.

Government Reaction

As the recent DOJ/OIG takedown makes clear, the government has not been blind to these risks. Auditors and investigators are casting a wary eye on telehealth providers whose conduct indicates patterns of abuse. One government tool that has been increasingly employed is data analytics. CMS and its contractors use sophisticated software programs to identify patterns in ordering and billing that indicate possible fraud

or other misconduct, such as unusually high utilization of certain procedures or reimbursement codes.[4]

Providers who are statistical outliers in terms of production and revenue are thus prime targets for investigation. And when the government finds what it believes to be fraud, it may even use the comparative data to prosecute. In several recent cases, DOJ has introduced evidence of statistical comparisons between defendant providers and other, "typical" peers to show misconduct—an approach that courts have upheld.[5]

This technique can lead to investigations of providers even if they have done nothing wrong. And when the government scrutinizes someone for suspected fraud or other serious offenses, it may instead uncover more routine regulatory violations, which can have their own consequences. This is certainly true in the case of telehealth, which involves a host of unique compliance issues.

Below, we outline a few key compliance problems and recommendations, in light of OIG's new laser focus on telehealth providers.

Common Compliance Problems

Practicing telehealth triggers certain additional legal state and federal obligations for providers, including obtaining and documenting verbal consent from patients before using telehealth features and ensuring appropriate safeguards for electronic communications that are consistent with the Health Insurance Portability and Accountability Act's Security Rule. While HHS' Office for Civil Rights has temporarily relaxed its enforcement against telehealth agencies during the pandemic, telehealth companies will not be off its radar forever.[6]

Telehealth providers that choose to expand their practices across state lines must also take care to comply with each state's laws, as applicable. States have varied rules that include:

(1) limitations and requirements related to prescribing drugs and ordering durable medical equipment via telemedicine (the focus of the 2020 Nationwide Telefraud Takedown);

(2) nurse practitioner supervision requirements and limitations on the number of nurses that can be supervised at one time;

(3) corporate practice of medicine prohibitions;

(4) fee-splitting restrictions; and

(5) licensure requirements.

HHS has recommended that states temporarily waive their licensure requirements for providers with licenses in good standing with other states amid COIVD-19.7 Violating these rules may subject telehealth providers to sanctions by the professional licensing boards, criminal liability, and/or civil penalties. Among other things, compliance failures combined with inaccurate certifications of compliance can lead to claims of overbilling or even violations of the federal False Claims Act or its state equivalents.8 Provider-employees or -contractors who become aware of these issues can potentially file whistleblower claims based on them, a trend that has increased over time. Legal counsel can help providers navigate these rules in states prior to launching telemedicine services to address restrictions and limitations and create state-specific policies and procedures.

Benefits of a Proactive Approach

Providers who expanded their practices online and health technology companies that recently entered the telehealth space should have their policies and procedures, including their websites' governance documents and policies, reviewed by counsel to determine whether they are comprehensive and whether updates are warranted. With counsel's assistance, providers without a compliance program should create one by:

(1) implementing written policies and procedures;

(2) appointing a Compliance Officer;

(3) conducting trainings and educational programs; and

(4) creating reporting and auditing mechanisms.

Providers with compliance programs that have not been reviewed recently should conduct a comprehensive review and implement any necessary updates.

If a compliance issue is suspected, counsel can assist with an internal audit to uncover issues and to correct them before a governmental investigation or enforcement action.

If an internal audit uncovers issues that may have resulted in an overpayment by a government payer, counsel can determine whether the overpayment resulted from the potential violation of a law that triggers civil monetary penalties. In that case, the provider will want to determine whether a self-disclosure under the OIG's Provider Self-Disclosure Protocol is warranted.[9] If the overpayment is determined to have resulted from an arrangement involving a physician, and the Stark law is triggered, the provider will need to determine whether disclosure is warranted under the CMS Voluntary Self-Referral Disclosure Protocol.[10] Counsel may also assist with reporting and returning the overpayment to the government payer pursuant to the Medicare 60-Day Rule, if applicable.[11]

A compliance program can reduce and potentially eliminate criminal conduct by acting as an internal police force. With an effective compliance program, providers can catch compliance issues and criminal conduct before the government does, complete an internal audit, and take corrective actions as necessary. As an additional benefit, government prosecutors or enforcement attorneys will often view an effective compliance program as a mitigating factor that justifies a more lenient approach to resolving any charges or civil claims, including a reduced settlement demand.[12]

What to Do?

Telehealth providers—particularly those with large revenues—should thus take action on these issues *before* the government comes knocking. High volumes not only place a provider on the government's radar, but they can lead to large damages claims or heightened sentencing guidelines.

As usual, an ounce of prevention beats a pound of cure. Having experienced counsel review compliance practices to identify problem areas even when no investigation is pending or expected will help eliminate violations or mitigate the outcome if any slip through the cracks. If a "cure" is what's needed—remedial measures, self-reporting, or repayment—counsel can advise on how much is too little, too much, or just enough.

If the compliance issue progresses further, and a provider is contacted by a government investigator or served a subpoena, an investigative demand, or an indictment, this advice is even more critical. In that case, the provider should immediately speak with counsel experienced in health care enforcement. In addition to managing interactions with the government and preventing catastrophic missteps such as false statements, obstruction of justice, or harmful statements, such counsel can conduct an investigation to evaluate and possibly minimize potential liability.

---

[1] HHS-OIG, 2020 National Health Care Fraud Takedown Fact Sheet, https://oig.hhs.gov/media/documents/2020HealthCareTakedown_FactSheet_9dtIhW4.pdf; HHS-OIG, 2020 National Health Care Fraud Takedown (Oct. 1, 2020). https://oig.hhs.gov/newsroom/media-materials/2020takedown.
[2] CMS, Physicians and Other Clinicians: CMS Flexibilities to Fight COVID-19 (Nov. 4, 2020), https://www.cms.gov/files/document/covid-19-physicians-and-practitioners.pdf.
[3] U.S. Department of Justice, Drug Enforcement Administration, Diversion Control Division, COVID-19 Information Page, https://www.deadiversion.usdoj.gov/coronavirus.html.
[4] *See* CMS, Medicare and Medicaid Integrity Programs, Annual Report (FY 2018), Oct. 1, 2017-Sept. 20, 2018, at Sect. 2.2, https://www.cms.gov/files/document/medicare-and-medicaid-integrity-program-fy-2018-annual-report.pdf.
[5] *See United States v. Melgen*, 967 F.3d 1250 (11th Cir. Jul. 31, 2020).
[6] HHS, Notification of Enforcement Discretion for Telehealth Remote Communications During the COIVD-19 Nationwide Public Health Emergency, Mar. 30, 2020, https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

[7] HHS, Letter to State Governors dated March 4, 2020, https://ncsbn.org/HHS_Secretary_Letter_to_States_Licensing_Waivers.pdf; HHS, Guidance to States: Lifting Restrictions to Extend the Capacity of the Health Care Workforce During the COVID-19 National Emergency Mar. 4, 2020, https://ncsbn.org/HHS_Guidence_to_States_on_Regulations_on_Healthcare_Workers.pdf.
[8] 31 U.S.C. §§ 3729 – 3733.
[9] OIG's Provider Self-Disclosure Protocol, https://oig.hhs.gov/compliance/self-disclosure-info/files/Provider-Self-Disclosure-Protocol.pdf.
[10] CMS, Voluntary Self-Referral Disclosure Protocol, https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/Self_Referral_Disclosure_Protocol.
[11] 81 Fed. Reg. 7654.
[12] *See* U.S. Department of Justice, Justice Manual § 9-28.800, Principles of Federal Prosecution of Business Organizations: Corporate Compliance Programs.