Articles + Publications | October 14, 2020

Fraud Emerges as Telemedicine Surges: Compliance Guidance for Telemedicine Providers

WRITTEN BY

Allison DeLaurentis | Miranda Hooker | Sharon R. Klein | Jason A. Kurtyka

Who Needs to Know

All telemedicine providers.

Why It Matters

Telemedicine providers – whether they are established or new to the space – should examine the type of conduct DOJ has recently focused on and adapt their compliance systems accordingly. Providers should also consider the cybersecurity dimension of a robust compliance system and ensure that their network is protected from malicious cyber actors exploiting deficiencies in many popular telework platforms.

The Centers for Medicare and Medicaid's (CMS) decision to expand telemedicine in response to the COVID-19 pandemic has fundamentally changed provider-patient interactions. Relaxed telemedicine regulations present health care providers with a tremendous opportunity to improve patient care. But, as an uptick in Department of Justice (DOJ) prosecutions of telemedicine arrangements indicates, telemedicine fraud and abuse risks abound. Telemedicine providers — whether they are established or new to the space — should examine the type of conduct recently focused on by DOJ and adapt their compliance systems accordingly. Providers should also consider the cybersecurity dimension of a robust compliance system and ensure that their network is protected from malicious cyber actors exploiting deficiencies in many popular telework platforms.

CMS Expands Telemedicine Services Due to COVID-19

Prior to the COVID-19 global pandemic, Medicare reimbursable telemedicine services were relatively limited. But, when CMS relaxed the requirements for reimbursement in March 2020 due to the pandemic, the use of telemedicine services soared. In fact, CMS reported that in April 2020, nearly half (43.5% or 1.28 million per week) of Medicare primary care visits were conducted via telemedicine compared to just .1% in February. And there are signs that patients and providers have little interest in returning to the pre-COVID-19 status quo: The global telemedicine market — valued at $24.9 billion in 2016 — is predicted to reach $113 billion by 2025.

Recent Telemedicine Fraud Takedown

DOJ has also turned its attention to investigating and prosecuting fraud in telemedicine services. Recently, DOJ charged 86 defendants in 19 judicial districts with $4.5 billion in fraud loss related to alleged nationwide kickback schemes involving telemedicine. The announcement of these prosecutions coincided with DOJ's announcement of its new National Rapid Response Strike Force, which will target cases involving major health care providers that

operate in multiple jurisdictions — including those seeking to exploit the COVID-19 pandemic through health care fraud schemes.

Though this recent, widespread takedown stemmed from conduct that took place long before COVID-19 upended the world, it serves to show that DOJ is focused on telemedicine as a hotbed for fraud and abuse, and this focus will only sharpen with the recent surge in telemedicine services. Likewise, CMS has also committed to monitoring program integrity implications of telemedicine to confront fraud and abuse.

Potential Telemedicine Fraud Schemes

Telemedicine fraud and abuse can take a variety of different forms, ranging from false claims stemming from inaccurate billing and coding to complex kickback schemes. The following exemplify risk areas that have, or are anticipated to, invite government scrutiny:

- **Up-Coding Time and Complexity:** CMS recently stated that it would closely monitor reimbursement requests to detect instances where providers inflate the time spent rendering telemedicine services. Failure to accurately bill for the precise time spent on telemedicine services, and to account for the complexity of those services, in order to increase reimbursements could result in False Claims Act liability.

- **Misrepresenting the Virtual Service Provided:** Medicare now reimburses for several types of virtual interactions, including telemedicine visits, virtual check-ins, telephone visits, and e-visits. It is critical that providers understand the requirements for each type of interaction, which CPT codes apply, and how to bill for them.

- **Billing for Services Not Rendered:** Submitting claims for services not provided, or not provided effectively, poses a significant enforcement risk. Even if a provider attempts to provide services in good faith, but technical difficulties prevent them from doing so, services should not be billed. Likewise, if a telemedicine appointment occurs, but the patient clearly cannot fully see or hear, or otherwise benefit from the appointment, the services could be considered wasteful.

- **Kickbacks:** The recent takedown included prosecutions of multiple kickback schemes executed via telemedicine. The defendants allegedly employed a variety of marketing tactics to make unsolicited contact with beneficiaries and ultimately prescribed or referred them for unnecessary genetic testing, prescription medications, or durable medical equipment for which the defendants received kickbacks.

In this environment, both dedicated telemedicine companies and providers, who only just recently integrated telemedicine into their practices, should be attuned to the ever-changing regulatory environment and sharpen their focus on compliance. The following are critical compliance initiatives that telemedicine providers should consider to mitigate enforcement risk:

- **Background and Conflicts Checks:** Given the significant expansion of telemedicine services in the recent months, telemedicine companies have likely experienced intense, rapid growth. Hiring surges increase the risk that appropriate scrutiny is not applied to new hires. Individual rogue providers, who accept kickbacks or are involved in inappropriate referral arrangements, could invite Anti-Kickback Statute liability on an otherwise compliant company. In addition to screening candidates for exclusion, disciplinary, and licensure issues, telemedicine companies should consider comprehensive background and conflict checks to ensure that the members of their expanding, remote work force do not carry any indicia of unethical behavior.

- **Training:** For either experienced telemedicine companies, or practitioners new to this space, training is a critical

component of an effective compliance program. Billing and coding requirements in this area have changed and will likely continue to evolve. Entities providing telemedicine services should ensure that their clinicians and their administrative staff receive regular training on the various telemedicine services and how to code and bill them appropriately.

- **Monitoring:** DOJ has long used data analytics to identify potential fraud, and it surely will continue to do so going forward. Telemedicine companies and providers of all kind should closely monitor their bills and charts for patterns and outliers. Spotting potential issues in real time provides an opportunity to evaluate whether billing is appropriate and to implement measures to prevent future issues. These monitoring activities may be more critical than usual in a remote environment, where employees may be less likely to ask questions or confirm the right way to do something.

- **Reporting and Investigations:** Telemedicine companies should have mechanisms in place for reporting and investigating suspected noncompliant behavior.

Cybersecurity Risks

In addition to the internal risks outlined above that come with increased virtual care, telemedicine companies should also guard their systems against external malicious cyber actors. In April, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the U.K.'s National Cyber Security Centre (NCSC) issued a joint warning that cyber criminals are exploiting COVID-19 to launch cyberattacks. Not only are cyber actors using coronavirus or COVID-19-related emails or URLs to facilitate phishing schemes or distribute malware, the agencies also warned that hackers are taking advantage of known vulnerabilities in virtual private networks (VPNs) and communication platforms like Zoom and Microsoft Teams. Telemedicine companies should take the following steps to prevent or mitigate a security breach:

- When utilizing VPNs and teleconferencing technologies for telework capabilities, work with your information security team to ensure security measures are properly in place to prevent known vulnerabilities.

- Meetings using teleconferencing technologies should never use public settings, and instead should require passwords or the use of a waiting room to control the admittance of guests.

- Strict screen-sharing settings should be utilized to ensure unauthorized individuals cannot commandeer any meeting.

- Ensure all software, including remote access and meeting applications, are up to date.

- Ensure telework policies address requirements for physical and information security.

RELATED INDUSTRIES + PRACTICES

- Digital Health
- Health Care + Life Sciences
- Privacy + Cyber
- White Collar Litigation + Investigations