COSMOS
Navigate the Compliance Universe

Compliance Today - November 2022

Allison M. Cohen (acohen@bakerdonelson.com,linkedin.com/in/allisonmcohen/) is Shareholder at Baker, Donelson, Bearman, Caldwell & Berkowitz PC, Washington, DC.

Telehealth compliance in the evolving landscape marked by increased OIG scrutiny

By Allison M. Cohen

Telehealth utilization grew significantly over the past few years to maintain access to critical healthcare services during a global pandemic. Numerous federal and state waivers, legislative flexibilities, and executive orders facilitated this growth by lifting some of the more challenging regulatory barriers and thereby making telehealth arrangements easier to structure in a compliant manner. Extensions of the U.S. Department of Health and Human Services' (HHS) public health emergency (PHE), as well as temporary legislation expanding Medicare coverage of telehealth services, have prolonged uncertainty regarding the regulatory landscape for telehealth when all COVID-19-related waivers and flexibilities terminate. At the same time, it is clear that HHS Office of Inspector General (OIG) has telehealth on its radar. To clarify its positions on telehealth compliance, OIG has been issuing guidance and publications to clarify its positions on telehealth compliance. By reviewing and analyzing noteworthy publications and national prosecutions, we can better understand the future of regulatory enforcement concerning telehealth arrangements.

2022 National Health Care Fraud Enforcement Action

The more broadly publicized OIG and the Department of Justice (DOJ) prosecutions have largely focused on schemes involving alleged violations of the federal Anti-Kickback Statute (AKS) [1] and submissions of false claims for the fraudulent provision of telehealth services in violation of the False Claims Act (FCA). OIG's "2022 National Health Care Fraud Enforcement Action" was a coordinated effort by OIG, DOJ, and law enforcement partners to combat healthcare fraud related to telehealth services.[2] In this most recent takedown, 36 defendants in 13 U.S. federal districts were charged with participating in fraudulent schemes involving telehealth-related technology. Defendants included telemedicine executives who allegedly paid practitioners to order medically unnecessary items and services, including laboratory testing and durable medical equipment (DME). The charges against the defendants were for more than $1.2 billion in fraudulent telemedicine, cardiovascular and cancer genetic testing, and DME schemes.[3] Additionally, the Centers for Medicare & Medicaid Services Center for Program Integrity (CPI) concurrently announced that it took administrative actions against 52 providers involved in similar schemes.[4]

Among the 2022 National Health Care Fraud Enforcement Action allegations were that laboratory owners and operators paid illegal kickbacks and bribes in exchange for referrals by medical professionals working with fraudulent telemedicine and digital health companies.[5] Cardiovascular genetic testing schemes have emerged as arrangements that will be subject to increased scrutiny after this recent prosecution.[6] Medicare had not approved cardiovascular testing for use as general screening tests proven to effectively indicate increased risk of

developing future cardiac conditions.[7] Nonetheless, over $174 million in false and fraudulent claims were allegedly submitted to Medicare based on orders for cardiovascular and genetic testing—the results of which were not used in the treatment of patients.[8] Similar to past telefraud schemes, some defendants were alleged to have controlled an international telemedicine network that used deceptive marketing techniques to target Medicare beneficiaries and induce them to agree to cardiovascular genetic testing, other genetic testing, and DME.[9]

These schemes involving purported telemedicine companies, telemarketers, and practitioners that were paid kickbacks in exchange for illegal referrals closely resemble the arrangements prosecuted in past telefraud takedowns. For example, "Operation Rubber Stamp" in the Southern District of Georgia targeted a similar criminal network involving individuals and companies that collected data from patients lured into the scheme by an international telemarketing network and sold it to DME suppliers, pharmacies, or labs.[10] Operation Rubber Stamp was part of a series of DOJ–HHS actions alleging telefraud, which also included Operations Double Helix and Brace Yourself.[11] The operations all involved enforcement of the AKS against illegal referral arrangements between telemedicine providers and manufacturers of DME (e.g., orthotic braces) and laboratory testing companies (e.g., cancer genetic tests).[12]

In both the recent and previous enforcement actions, the allegations do not suggest that the defendants' actions were good-faith efforts to provide telehealth services in which practitioners misunderstood billing requirements. Instead, there was often a complete failure to engage in any interaction that would qualify as telehealth, establish the practitioner/patient relationship, or satisfy any of the standards for remote services that could lead to legitimate orders for medical items or services. The earlier takedowns raised awareness and led to further scrutiny of telehealth services and arrangements in which companies that purport to provide telehealth services profit from false or fraudulent claims for medically unnecessary services.