MEDICARE TELEHEALTH

Actions Needed to Strengthen Oversight and Help Providers Educate Patients on Privacy and Security Risks

What GAO Found

In response to the COVID-19 pandemic, the Department of Health and Human Services (HHS) temporarily waived certain Medicare restrictions on telehealth—the delivery of some services via audio-only or video technology. Use of telehealth services increased from about 5 million services pre-waiver (April to December 2019) to more than 53 million services post-waiver (April to December 2020). Total utilization of all Medicare services declined by about 14 percent post-waiver due to a 25 percent drop in in-person service use. GAO also found that, post-waiver, telehealth services increased across all provider specialties, and 5 percent of providers delivered over 40 percent of services. Urban providers delivered a greater percentage of their services via telehealth compared to rural providers; office visits and psychotherapy were the most common services.

The Centers for Medicare & Medicaid Services (CMS) within HHS took actions to monitor some program integrity risks related to the telehealth waivers. However, CMS lacks complete data on the use of audio-only technology and telehealth visits furnished in beneficiaries’ homes. This is because there is no billing mechanism for providers to identify all instances of audio-only visits. Moreover, providers are not required to use available codes to identify visits furnished in beneficiaries’ homes. Complete data are important, as the quality of these services may not be equivalent to that of in-person services. Also, CMS has not comprehensively assessed the quality of telehealth services delivered under the waivers and has no plans to do so, which is inconsistent with CMS’ quality strategy. Without an assessment of the quality of telehealth services, CMS may not be able to fully ensure that services lead to improved health outcomes.

In March 2020, HHS’s Office for Civil Rights (OCR) announced that it would not impose penalties against providers for noncompliance with privacy and security requirements in connection with the good faith provision of telehealth during the COVID-19 public health emergency. OCR encouraged covered providers to notify patients of potential privacy and security risks. However, it did not advise providers of specific language to use or give direction to help them explain these risks to their patients. Providing such information to providers could help ensure that patients understand potential effects on their protected health information in light of the privacy and security risks associated with telehealth technology.