Telehealth: Potential Program Integrity Issues

OIG Technical Assistance as Requested
February 2021

Overview

This document provides technical assistance for policymakers considering program integrity as it relates to telehealth. It focuses on the Medicare program, but the principals articulated here may have broader application to other programs. This technical assistance focuses on three main areas:

- Quality of Care and Patient Safety
- Verification of Services and Patient Consent
- Infrastructure

For each area, OIG identifies potential risks and safeguards that should be considered by policymakers to protect patients and ensure that telehealth delivers on its promise to expand access to, and delivery of, quality health care.

Background

In response to the COVID-19 public health emergency, both Congress and the Department of Health and Human Services (HHS) acted to make telehealth more widely available. Based on those efforts and regulatory action taken by the Centers for Medicare & Medicaid Services (CMS), Medicare has seen significant, well-documented changes in telehealth utilization and service type.

The HHS Office of Inspector General (OIG) has conducted data analysis throughout the public health emergency on preliminary telehealth claims data in Medicare to monitor trends and aberrant patterns that may indicate potential program integrity concerns. These analyses have provided some early indications of vulnerabilities for fraud, waste, and abuse associated with expanded utilization of telehealth. OIG has a general understanding of many of these risks because they are common in a fee-for-service program (e.g., overutilization and upcoding). However, more work is needed to identify the magnitude of those risks and how differences in telehealth service delivery may lead to new program integrity concerns.

OIG's prior work recognizes telehealth can be used to improve access to care, increase patient convenience, and increase efficiency in the delivery of services.[1] While permanent changes and improvements are considered, program integrity vulnerabilities should be one factor among many others that are considered so that use of telehealth leads to more effective and efficient delivery of health care services. To better understand telehealth issues, OIG has ongoing work specifically assessing Medicare and Medicaid telehealth services during the public health emergency.[2] Once complete, OIG's reviews will provide in-depth, objective, and independent findings and recommendations that can further inform policymakers and other stakeholders.

Since the expansion of telehealth services due to the public health emergency, the **OIG Hotline** has reported an uptick in telehealth-related complaints. Examples of the types of complaints include:

- providers instructing staff to "cold call" Medicare beneficiaries via telephone and bill each for a telehealth visit;
- "upcoding" telehealth visits by billing for visits longer than they lasted;
- billing for services not rendered to the patient, or providing basic services and billing for more complex visits;
- billing for an impossible number of virtual visits in one day; and
- using overseas providers to provide telehealth services that do not appear to be licensed or credentialed in the United States

To date, OIG's data analysis on preliminary telehealth claims data in Medicare indicates some potential concerns related to fraud, waste, and abuse. For example, an analysis of claims from 3/1/2020 through 7/31/2020 shows that providers are billing telehealth office visits for new patients at a higher complexity level than those provided face to face. Twenty-two percent of telehealth visits for new patients were billed at the highest complexity level, versus 16 percent for non-telehealth visits. Additional analysis may explain the difference is appropriate, but this trend warrants further monitoring.

---

[1] *Provider Shortages and Limited Availability of Behavioral Health Services in New Mexico's Medicaid Managed Care*, OEI-02-17-00490, Sept. 2019.

[2] Audit of Home Health Services Provided as Telehealth During the COVID-19 Public Health Emergency; Audits of Medicare Part B Telehealth Services During the COVID-19 Public Health Emergency; Medicare Telehealth Services During the COVID-19 Pandemic: Program Integrity Risks; Use of Medicare Telehealth Services During the COVID-19 Pandemic; Medicaid—Telehealth Expansion During COVID-19 Emergency.

Telehealth: Potential Program Integrity Issues

OIG Technical Assistance as Requested
February 2021

The program integrity issues summarized below reflect both OIG Hotline complaint trends and OIG's data analyses.

Technical Assistance: Three Areas of Focus

OIG has identified the following potential program integrity risks and safeguards. The information provided in this section is based on OIG experience and work completed to date. This document is intended to provide preliminary context, and issues identified may not warrant specific action at this time. New issues may emerge or our understandings of existing issues may change as we continue our oversight work. The risks noted below derive from OIG work and are not exhaustive of all telehealth program integrity risks that may arise. OIG will share updated information as telehealth oversight and enforcement work provides additional insights on potential program integrity vulnerabilities.

Quality of Care and Patient Safety

OIG suggests considering the following risks and safeguards related to potential quality of care and safety concerns in connection with telehealth flexibilities. Telehealth waivers have expanded potential service areas for many providers. For example, OIG has identified more than 100 providers who served beneficiaries via telehealth in at least 10 States during the pandemic, whereas in prior years the same providers mostly treated beneficiaries in one or two states. While not directly indicative of fraud or abuse related to quality of care, it demonstrates that telehealth waivers may create challenges with existing safeguards such as requirements for provider enrollment and screening. Analyses also demonstrate that the types of providers engaging in services are changing. For example, office-based opioid treatment was much more likely to be provided by physician assistants and nurses when delivered via telehealth (37 percent of claims) than face to face (10 percent of claims). Again, this is not a direct indication of fraud or abuse but provides data that stakeholders should consider when assessing permanent changes to telehealth services.

Risks

- New service with limited accepted standards of care when provided via telehealth
- Expanded scope of services that may be more appropriate for in-person care or require in-depth assessment via physical exam
- Lack of infrastructure and/or programs for quality oversight
- Supervision via telehealth (e.g., the provider is not present and accountable for service if another professional provides the care)

Safeguards

- Incentivize quality by linking telehealth reimbursement with quality-of-care measurements
- Create a standard that requires CMS to consider clinical appropriateness as part of the process of approving new services for telehealth reimbursement
- Document consent to ensure patient understands services being provided and is capable of carrying out provider instructions at home
- Develop oversight mechanisms that help ensure telehealth delivery is safe and effective for patients
- Ensure telehealth services have standard-of-care and medical-necessity parity with in-person visits (e.g., in-person service quality requirements should apply to telehealth)

Telehealth: Potential Program Integrity Issues

OIG Technical Assistance as Requested
February 2021

Verification of Services and Patient Consent

OIG enforcement and oversight work indicates that bad actors and unscrupulous providers may take advantage of telehealth services to expand well-known fraud schemes. Recent fraud schemes used "telefraud" or telemarketing to reach beneficiaries at home and used that interaction to bill for medically unnecessary items and services, such as durable medical equipment (DME). These schemes have not regularly included billing for fraudulent telehealth services but have involved sham "telemedicine companies." With additional telehealth flexibilities, bad actors may double dip by billing for fraudulent telehealth services and order other unnecessary items or services.

To provide context, the following data is about audio-only telehealth. Since 3/1/2020, Medicare has paid more than $440 million for audio-only phone call codes involving more than 300,000 providers and 5.2 million beneficiaries. Most of these calls were between patients and providers with prior relationships, but approximately 5 percent were between providers and patients with no prior relationships. Collectively, approximately 90,000 beneficiaries received approximately $43 million worth of DME supplies ordered by providers with whom they had a phone call billed. These data are not indictive of any particular fraud and abuse trends. Instead, it may reflect other issues, such as lack of Medicare beneficiary access to video technology or broadband access.

Risks

- Gaps in requirements for validating that a given telehealth event took place and was appropriate for the patient
- Different modalities may present verification challenges (e.g., audio-only services are harder than video calls to verify from an oversight perspective)
- Patient verification of the provider can be harder than over telehealth, particularly for audio-only
- Current coding and modifiers are limited and do not provide granular data that enable specific analysis of telehealth services and modality
- Challenges with verifying that provider is appropriately licensed and credentialed in the United States
- Difficulties with consent verification that service was needed if patient receives unsolicited calls and does not need to leave the home, and special concern for vulnerable populations with cognitive issues that may have limited protections and/or understanding of consent

Safeguards

- Use technology to document service (e.g., screenshot of video)
- Condition payment on a patient attestation or consent to ensure patient agreed to service
- Limit reimbursement for audio-only to patient-initiated or scheduled services, or for patients with a documented lack of video technology access
- Improve CPT and modifiers to track modality of technology
- Capture additional data to support verification similar to mobile phone call metadata (e.g., call detail records).
- Verification that a doctor who signed up to provide services is the one providing services (could augment use of screenshots)
- Require or provide guidelines for vulnerable individuals with cognitive issues or impaired decision-making abilities to authorize another designated individual for dual consent of services on their behalf

Telehealth: Potential Program Integrity Issues

OIG Technical Assistance as Requested
February 2021

Infrastructure

The increased demand for services may lead to privacy and security concerns as providers and patients adopt new technology for telehealth and other virtual care. Expanded access to telehealth services should consider how best to ensure that the technology remains safe and secure for use and protects patient health information.

Risks

- Early concerns regarding cybersecurity that expanded technology for telehealth has the potential to expose patients' protected electronic health information or other personal information to data breaches and/or phishing attempts
- Evolving cybersecurity threats specifically configured to target telehealth IT infrastructure through malware toolkits and unique strains of ransomware
- More of the onus is put on patients to ensure cybersecurity (e.g., installing smartphone operating system updates)
- Different tiers of permitted technology or security requirements may pose risks (e.g., public-facing video technology is acceptable for some services, but not all)
- Security issue that the provider on the other end is the provider who is supposed to be seen (e.g., identify theft)
- Patients with limited access to reliable internet connections may not have the capabilities to regularly engage in telehealth or other virtual care, and may need to utilize secure communication methods to virtually interact with providers (e.g., text messages)

Safeguards

- Require expanded technology for telehealth should be to meet a consistent level of security expectation
- Ensure security requirements take into account the patient role and potential vulnerabilities
- Harmonize security requirements as much as possible across service types.
- Create a system between provider and patient to verify the provider (e.g., technology verification "handshake" or something similar to the electronic visit verification system for home health and personal care services)
- Continue addressing patient access to reliable internet connection to ensure patients can securely communicate with their providers
- Ensure training on telehealth-specific health care privacy and security training for providers and staff who provide telehealth services

For questions, please contact Britanny Vanderhoof in OIG's Office of Congressional Affairs at 202-893-4969 or by email at Britanny.Vanderhoof@oig.hhs.gov.