Telehealth Fraud, Waste and Abuse: How to Develop a Prevention and Detection Program

With telehealth utilization at 38x what it was pre-pandemic, plan sponsors should address telehealth fraud as part of overall anti-fraud, waste and abuse plans

> ***More than 28 million Medicare beneficiaries—about 2 in 5—used telehealth services the first year of the pandemic. In total, beneficiaries used 88 times more telehealth services during the first year of the pandemic than they did in the prior year*.**
>
> *OIG Data Brief-OEI-02-20-00720 Sept. 2022*

The pandemic had a tremendous impact on healthcare delivery. Fee-for-service Medicare previously offered telehealth services on a limited basis—mostly to beneficiaries in rural and medical staff- shortage areas. And while Medicare Advantage (MA) plans have always been able to offer broader supplemental telehealth benefits, usage prior to the pandemic was relatively low. CMS relaxed certain telehealth prohibitions, such as geographic area restrictions, and expanded the list of eligible services and the types of providers permitted to use telehealth. CMS also allowed the use of audio-only for certain telehealth services, such as office visits and behavioral health services. As a result of these flexibilities and patient support for telehealth services, its use increased dramatically during and following the pandemic. According to McKinsey & Company, in 2021 telehealth utilization leveled off at about 38-times higher than before the pandemic.

Anatomy of a Telehealth-Related Crime

- ***Clinical laboratories enlisted an array of co-conspirators to order and fulfill unneeded tests, durable medical equipment (DME) and/or prescription drugs for cardiovascular and cancer patients through telehealth appointments.***
- ***They paid more than $16 million in kickbacks to marketers who then paid telemedicine companies and call centers in exchange for doctors' orders.***
- ***Marketers and call centers coaxed patients to agree to tests and DME through telehealth visits.***
- ***Practitioners wrote orders without appropriate review of medical records to establish medical necessity—or without medical record review at all.***
- ***DME companies, genetic testing labs and pharmacies purchased the orders in exchange for kickbacks/bribes and submitted fraudulent claims to Medicare and other government insurers.***
- ***36 individuals charged, including more than 100 licensed medical professionals representing more than $174 million in claims.***

Some of the areas of highest telehealth usage include psychiatry and substance abuse, prescription/pain management, urgent care, dermatology, chronic disease management and endocrinology. Unfortunately, as a greater percentage of healthcare is delivered through remote technology, there is the potential for increased fraud, waste and abuse (FWA). Telehealth services are highly prone to abuses and some of the highest dollar recent cases in Department of Justice history are related to telehealth.

DOJ, OIG and CMS Enforcement

Since 2020, CMS program integrity investigations related to telehealth resulted in the revocation of billing privileges for hundreds of medical professionals involved in telemedicine schemes. In July of 2022, the DOJ announced the largest telehealth scheme in its history. This case and another highly publicized case announced this past July, represent more than a billion dollars in kickback and bribery schemes related to telehealth.

What Recent Data Reveals

The Office of Inspector General (OIG) released a report with results of an examination of fee-for-service (FFS) claims and MA encounter data related to telehealth usage. The study focused on the program integrity risks during the first year of the pandemic. The results telegraph the kinds of issues plan sponsors should watch for as telehealth continues to grow.

The OIG analyzed FFS claims data and MA encounter data for the first year of the pandemic (March 1, 2020 to February 28, 2021). Analysts looked at telehealth billing of 742,000 providers against seven measures deemed indicative of potential fraud, waste, or abuse. Issues were detected in the billing of 1,714 providers for approximately half a million beneficiaries. Payments against these claims represent more than $125 million.

It is important to note that these fraud indicators did not relate to services provided that were not medically necessary, or phantom billing for services that were never provided. However, enforcement actions clearly indicate how concerned we should be in those and other areas.

OIG Billing Fraud Indicators

- **Billing both a telehealth service and a facility fee for most visits**
- **Billing telehealth services at the highest, most expensive level every time**
- **Billing telehealth services for a high number of days in a year**
- **Billing both Medicare FFS and a MA plan for the same service for a high proportion of services**
- **Billing a high average number of hours of telehealth services per visit**
- **Billing telehealth services for a high number of beneficiaries**
- **Billing for a telehealth service/ordering medical equipment for a high number of beneficiaries**

From OIG Data Brief; September 2022. OEI-02-20-00720

How to Develop a Telehealth FWA Prevention and Detection Program

Plan sponsors should address telehealth fraud as part of their overall anti-fraud, waste and abuse plans. Supported by a robust compliance plan, a telehealth fraud program should be integrated into prevention and detection efforts, including raising awareness of vulnerabilities in the administration of these services and the rapidly evolving billing and coding requirements.

Fraud Prevention Activities

1. Compliance should take the lead in training relevant staff, applying CMS and OIG guidance and sharing the analysis of claims and encounter data. One visit to Telehealth.HHS.gov will remind you how much the regulatory environment is changing and how much more is yet to be addressed.
2. Special investigative units and claims departments should monitor evolving billing and coding requirements to ensure outdated policies and regulations are no longer applied.
3. Staff and network providers should be trained on evolving state and federal telehealth laws/rules and exceptions. For example:
    - State laws can differ and/or exceed federal standards and requirements, including the types of providers allowed to use telehealth, or the technology permitted.

The OIG Data Brief found that more than 670 of the providers analyzed billed inappropriately for both a telehealth service and a facility fee for most of their visits.

    - Providers should ensure they understand associated HIPAA rules and storage requirements for telehealth documentation.
    - Be on the lookout for common mistakes, such as billing time a patient spends with clinical staff and forgetting to note patient consent for the visit in the medical record.

4. Communicate to your members questionable telehealth-related practices:

    - Watch for companies that market telehealth visits to potential patients touting free or low-cost health items or services.
    - Understand how personal health and financial information shared during a virtual appointment can be used for marketing purposes without the patient's consent and identity theft.
    - Avoid making appointments with providers or companies that the patient has never seen.

Detection Activities

1. Train claims and audit staff on vulnerabilities:
    - Train audit staff to review medical records to ensure appropriate documentation including location, purpose, and type of equipment used for telehealth visits.
    - Training should include billing practices and red flags related to specific types of remote technologies including secure email, web-based applications and remote patient monitoring.

2. Monitor telehealth services on an ongoing basis to identify providers who pose a risk to the program, including:

    - Providers who chronically bill for the highest, most expensive levels of certain telehealth services as an indicator for potential problems.
    - Practices that have multiple providers consistently billing for maximum timeframes for telehealth visits.
    - Providers who fail to meet appropriate medical record documentation standards, including support of medical necessity for prescriptions, DME and testing ordered during a telehealth appointment, and location and duration of visit.

3. Alert network providers to red flags in written agreements with telehealth companies identified by the OIG, for example:
    - Arrangements that compensate providers based on the volume of items/services ordered or prescribed during telehealth care.
    - Arrangements that allow providers to prescribe/order services to patients without an established relationship, or without complete and/or recent medical records.

There are many other aspects to telehealth FWA, including the area of incident-to billing and cybersecurity threats. ATTAC Consulting Group can help your organization identify telehealth-related vulnerabilities, interpret recent data and make recommendations for augmenting your current FWA program.