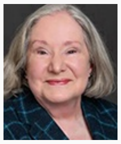
COSMOS
Navigate the Compliance Universe

Compliance Today - February 2024



Patricia D. King (pking@mbhealthlaw.com, linkedin.com/in/patriciadking/) is an Attorney with Malecki Brooks Law Group LLC in Des Plaines, IL.

Telehealth challenges for compliance teams

by Patricia D. King, JD, MBA

Telehealth presents no shortage of challenges for compliance professionals. These include familiar issues in a new setting and completely new concerns. Potential vulnerabilities include not only variants of fraud, kickback breaches, and incorrect billing concerns that have haunted compliance teams for decades but also limitations on prescribing controlled substances and state licensure issues. Compliance teams should be aware that some acceptable practices for 2020 through 2022 are now vulnerable. The rapid expansion of telehealth during the COVID-19 pandemic—born out of necessity—was accompanied by waivers of regulatory requirements and enforcement discretion in several key areas. Most of these special considerations are gone, but some practitioners who got too comfortable with the eased restrictions may have never adapted to a new environment of increased regulatory scrutiny.

Telehealth is a rapidly evolving area that is the focus of attention for state and federal regulators. The U.S. Department of Health and Human Services (HHS) has created a hub for telehealth updates, including legal considerations and best practices.[1]

Fraud and billing concerns

Compliance professionals know that both governmental programs and private insurance plans have long been vulnerable to fraud, false claims, and kickback violations. Fraudsters exploited telehealth even prior to the pandemic. Early examples of the U.S. Department of Justice (DOJ) enforcement actions in the telehealth space included “Operation Brace Yourself,” a scheme in which durable medical equipment (DME) companies paid kickbacks to telemedicine companies which contracted with physicians to order medically unnecessary braces with little or no patient contact,[2] and “Operation Double Helix,” which resulted in charges against 35 defendants (including nine doctors) associated with telemedicine companies who billed Medicare for over $2.1 billion in false charges for medically unnecessary cancer genetic tests.[3] As telehealth utilization exploded during the pandemic, telefraud continued. In September 2021, 138 defendants—including 42 physicians, nurses, and other clinicians—were indicted for involvement in fraudulent claims for telehealth services totaling $1.1 billion.[4] The indictment alleged that telemedicine executives paid doctors and nurse practitioners to order medically unnecessary DME, genetic and other lab tests, and pain medications; in some instances, physicians and nurse practitioners billed for telehealth consultations that did not occur.

The HHS Office of Inspector General (OIG) has been active in monitoring telehealth utilization, and some activities examining telehealth services have been included in the OIG annual work plan since 2017. On July 20, 2022, OIG issued a special fraud alert identifying characteristics of suspect arrangements between practitioners and telemedicine companies:

- “The purported patients for whom the Practitioner orders or prescribes items or services were identified or recruited by the Telemedicine Company, telemarketing company, sales agent, recruiter, call center, health fair, and/or through internet, television, or social media advertising for free or low out-of-pocket cost items or services.
- “The Practitioner does not have sufficient contact with or information from the purported patient to meaningfully assess the medical necessity of the items or services ordered or prescribed.
- “The Telemedicine Company compensates the Practitioner based on the volume of items or services ordered or prescribed, which may be characterized to the Practitioner as compensation based on the number of purported medical records that the Practitioner reviewed.
- “The Telemedicine Company only furnishes items and services to Federal health care program beneficiaries and does not accept insurance from any other payor.
- “The Telemedicine Company claims to only furnish items and services to individuals who are not Federal health care program beneficiaries but may in fact bill Federal health care programs.
- “The Telemedicine Company only furnishes one product or a single class of products (e.g., durable medical equipment, genetic testing, diabetic supplies, or various prescription creams), potentially restricting a Practitioner’s treating options to a predetermined course of treatment.
- “The Telemedicine Company does not expect Practitioners (or another Practitioner) to follow up with purported patients [. . .]”[5]

OIG stressed that this list was not exhaustive but illustrative and encouraged practitioners to use heightened scrutiny before entering an arrangement containing one or more suspect criteria.

In addition to these blatant types of fraud, telehealth can present risks of upcoding and overutilization similar to traditional delivery methods. In April 2023, OIG published a toolkit for identifying program integrity risks associated with telehealth claims. “This toolkit is intended to assist public and private sector partners—such as Medicare Advantage plan sponsors, private health plans, State Medicaid Fraud Control Units, and other Federal health care agencies—in analyzing their own telehealth claims data to assess program integrity risks in their programs.”[6]

[*Practice note*: Compliance teams may wish to consider using the toolkit proactively to assess billing compliance within their telehealth programs.]

OIG’s toolkit suggests that users identify claims for telehealth services and conduct data analysis to identify program integrity risks. Some factors may complicate the analysis. For example, where “incident-to“ billing occurs, multiple individuals may provide telehealth services under the National Provider Identifier (NPI) number of the supervising physician or practitioner, which can complicate some of the measures (e.g., the number of telehealth services provided per visit). OIG describes seven measures focusing on different types of billing that may indicate potential for fraud, waste, or abuse:

1. “Billing telehealth services at the highest, most expensive level for a high proportion of services”
2. “Billing a high average number of hours of telehealth services per visit”
3. “Billing telehealth services for a high number of days in a year”

4. "Billing telehealth services for a high number of patients"
5. "Billing multiple plans or programs for the same telehealth service for a high proportion of services"
6. "Billing for a telehealth service and then ordering medical equipment for a high percentage of patients"
7. "Billing for both a telehealth service and a facility fee for most visits"

For some factors, OIG also identified related areas that may be appropriate for additional analysis. For example, related to No. 2, OIG suggests an "impossible day" analysis:

> A common program integrity measure identifies providers who bill for an improbable or impossible number of hours in a single day. For example, a provider could not provide, and therefore should not bill for, 25 hours of services in a single day. This is known as an 'impossible day' analysis.
>
> However, an impossible day analysis is not a good fit for programs that allow for 'incident to' billing. Under 'incident to' billing, services provided by clinical staff who are directly supervised by a physician or non-physician practitioner may be billed under the supervising practitioner's identification number. Consequently, multiple individuals can provide telehealth services under a single identification number.[7]

OIG also suggests that providers who pose a risk to the program may be identified through other characteristics, such as identifying providers with similar problematic patterns who are part of the same medical practice and providers who appear to be associated with telehealth companies.