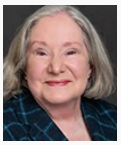
COSMOS
Navigate the Compliance Universe

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.

Privacy and security

When the COVID-19 pandemic began, it wreaked havoc on the healthcare system. In areas where COVID-19 exposure was high, hospitals initially had to discontinue surgeries other than emergency care. Physicians and other practitioners limited their office practices to minimize exposure. Even with COVID-19 consuming healthcare resources, people still needed to "see" their healthcare providers to monitor chronic conditions and evaluate their health problems; however, sometimes, a virtual visit was a good substitute for risking exposure to going to the doctor's office.

Many factors had limited the utilization of telehealth prior to the pandemic—especially limitations on Medicare and insurance coverage. An additional contributing factor was uncertainty about how healthcare providers could offer telemedicine while complying with HIPAA Privacy and Security rules. In 2020 and 2021, the HHS Office for Civil Rights (OCR) published four Notifications of Enforcement Discretion notices, extending flexibility in how the Privacy, Security, Breach Notification, and Enforcement rules would be applied during the pandemic. The most wide-reaching notice of enforcement discretion permitted healthcare providers to use nonpublic facing remote communication products to communicate with patients.[8] This included applications such as Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype. OCR stated it would not impose penalties against a healthcare provider for lacking a business associate agreement (BAA) with video communication companies relating to the good faith provision of telehealth services during the pandemic. The four Notifications of Enforcement Discretion notices expired May 11, 2023.[9] However, with regard to telehealth remote communications, OCR allowed a 90-day transition period, up to August 9, 2023, for healthcare providers to come into compliance by choosing a telehealth technology vendor that will enter into a BAA and comply with

HIPAA rules. Compliance teams should verify that their telehealth programs now have a BAA in place for the technology used to communicate with patients.

In 2022, the Government Accountability Office (GAO) reviewed telehealth services under the waivers introduced by the Medicare program during the pandemic and the OCR enforcement discretion.[10] The GAO noted that while OCR encouraged healthcare providers to notify patients of potential privacy and security risks of remote communications technologies, it did not provide direction to help providers explain these risks. OCR concurred with the recommendation and has published a resource providing guidance for healthcare providers on how to educate patients about privacy and security risks.[11] While noting that HIPAA Privacy, Security, and Breach Notification rules do not require providers to educate patients about these risks, OCR comments that ensuring privacy and security of protected health information is important for quality care.

Controlled substances

In 2008, Congress passed a statute in response to the death of a young man who overdosed on Vicodin prescribed by a physician he had never met and obtained through an online pharmacy. The Ryan Haight Online Pharmacy Consumer Protection Act provides that, with certain exceptions, a prescribing practitioner may prescribe controlled substances to a patient only after conducting an in-person examination.[12]

During the pandemic, the Drug Enforcement Administration (DEA) granted temporary exceptions to the restrictions imposed under the Ryan Haight Act to prevent lapses in care. These telemedicine flexibilities permitted a DEA-registered practitioner to prescribe Schedule II–V controlled substances via telemedicine without an in-person medical evaluation if the following conditions were met:

1. "The prescription is issued for a legitimate medical purpose by a practitioner acting in the usual course of professional practice;
2. "The prescription is issued pursuant to a communication between a practitioner and a patient using an interactive telecommunications system";
3. The practitioner is authorized under their DEA registration "to prescribe the basic class of controlled substance" or is exempt from registration; and
4. The prescription is consistent with all other DEA requirements for controlled substance prescriptions.[13]

The DEA has extended the telehealth flexibilities until December 31, 2024.[14] Meanwhile, the DEA published proposed rules on March 1, 2023, regarding telemedicine prescribing of controlled substances when the practitioner and patient have not had a prior in-person medical evaluation.[15] Under the proposed rules, there will be two options for prescribing controlled substances to patients whom the practitioner has not seen in person. The first option would permit a practitioner to issue a prescription for a non-narcotic Schedule III–V drug if the quantity is limited to a 30-day supply. The second option applies if the patient has had an in-person exam with a DEA-registered practitioner who refers the patient to the prescribing practitioner. In that case, the practitioner can issue a prescription for a Schedule II–V drug, including narcotics, limited to a 30-day supply.

Licensure issues

One good thing about brick-and-mortar healthcare is that you always know what state regulators you're dealing with. Even if patients come to you from a neighboring state, you would rarely find regulatory agencies from that state knocking on your door. However, state medical boards care very much about who provides care to residents

of their state via telehealth. Your telehealth patients could be anywhere unless you have processes to control which patients can access your services.

Laws regarding telehealth vary greatly among the states; however, typically, state laws require that a healthcare professional providing services to residents of the state via telehealth must be licensed in that state. For example, the Illinois Medical Practice Act recognizes that "the practice of medicine is a privilege and that the licensure by this State of practitioners outside this State engaging in medical practice within this State and the ability to discipline those practitioners is necessary for the protection of the public health, welfare, and safety."[16] Illinois, like some other states, recognizes limited exceptions in the interest of continuity of care (such as follow-up services aftercare was provided to the patient in the state in which the physician is licensed, or healthcare services provided to an existing patient while the physician or patient is traveling).[17]

A few states have a special permitting system for telehealth providers who are not licensed in the state. For example, Florida permits healthcare practitioners with a valid out-of-state license to obtain a telehealth provider registration number if they do not open an office in Florida or provide in-person care to Florida residents and meet certain other requirements.[18]

Like the OCR enforcement discretion previously discussed, licensure requirements are another area where state enforcement was deferred or modified during the pandemic, usually by executive order of the state governor. This allowed for interstate expansion of telehealth practices during the COVID-19 public health emergency. With the pandemic now thankfully in the rearview mirror, these flexibilities have generally expired. Compliance teams should confirm that their telehealth programs have adapted to this new regulatory environment and implemented safeguards to ensure that providers are appropriately licensed based on the patient's state of residence. It is also essential to remember that if certain providers must be licensed in another state, they will be subject to all requirements under that state's licensure laws, including restrictions on fee-splitting and the corporate practice of medicine.

Takeaways

- Many providers expanded interstate telehealth practice during the pandemic when licensure and other requirements were temporarily waived. Patient registration procedures for telehealth should be reviewed to determine whether access is limited to residents of states where healthcare practitioners are licensed.
- The U.S. Department of Health and Human Services Office of Inspector General (OIG) fraud alert identifies several characteristics of suspect telemedicine arrangements. Review any contractual arrangements with durable medical equipment companies or other suppliers for potential kickback violations.
- Telehealth practices can present the same risk of upcoding as seen with evaluation and management coding. Consider adding some areas identified in OIG's toolkit to claims audits.
- The HIPAA enforcement flexibilities in effect during the pandemic have expired, and it is important to review HIPAA compliance and cybersecurity practices. Verify that a HIPAA business associate agreement was signed for telehealth communication technology and that patients are informed of privacy and security risks.
- The Drug Enforcement Administration's telemedicine flexibilities for prescribing without an in-person exam will run out at the end of 2024. Compliance teams should use the intervening year to educate telehealth teams about the upcoming need for in-person examinations.

1 Telehealth.HHS.gov, "Legal considerations," last updated November 7, 2023, https://telehealth.hhs.gov/providers/legal-considerations.
2 U.S. Department of Justice, Office of Public Affairs, "Federal Indictments & Law Enforcement Actions in One of the Largest Health Care Fraud Schemes Involving Telemedicine and Durable Medical Equipment Marketing Executives Results in Charges Against 24 Individuals Responsible for Over $1.2 Billion in Losses," news release, April 9, 2019, https://www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes.
3 U.S. Department of Justice, Office of Public Affairs, "Federal Law Enforcement Action Involving Fraudulent Genetic Testing Results in Charges Against 35 Individuals Responsible for Over $2.1 Billion in Losses in One of the Largest Health Care Fraud Schemes Ever Charged," news release, September 27, 2019, https://www.justice.gov/opa/pr/federal-law-enforcement-action-involving-fraudulent-genetic-testing-results-charges-against.
4 U.S. Department of Justice, Office of Public Affairs, "National Health Care Fraud Enforcement Action Results in Charges Involving over $1.4 Billion in Alleged Losses," news release, September 17, 2021, https://www.justice.gov/opa/pr/national-health-care-fraud-enforcement-action-results-charges-involving-over-14-billion.
5 U.S. Department of Health and Human Services, Office of Inspector General, "Special Fraud Alert: OIG Alerts Practitioners To Exercise Caution When Entering Into Arrangements With Purported Telemedicine Companies," July 20, 2022, https://oig.hhs.gov/documents/root/1045/sfa-telefraud.pdf.
6 Ann Maxwell, "Toolkit: Analyzing Telehealth Claims to Assess Program Integrity Risks," OEI-02-20-00723, U.S. Department of Health and Human Services, Office of Inspector General, April 2023, https://www.oig.hhs.gov/oei/reports/OEI-02-20-00723.pdf.
7 U.S. Department of Health and Human Services, Office of Inspector General, "Toolkit: Analyzing Telehealth Claims to Assess Program Integrity Risks," 14.
8 Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, 85 Fed. Reg. 22,024 (April 21, 2020), https://www.federalregister.gov/documents/2020/04/21/2020-08416/notification-of-enforcement-discretion-for-telehealth-remote-communications-during-the-covid-19.
9 Notice of Expiration of Certain Notifications of Enforcement Discretion Issued in Response to the COVID-19 Nationwide Public Health Emergency, 88 Fed. Reg. 22,380 (April 13, 2023), https://www.federalregister.gov/documents/2023/04/13/2023-07824/notice-of-expiration-of-certain-notifications-of-enforcement-discretion-issued-in-response-to-the.
10 Government Accountability Office, *Medicare Telehealth: Actions Needed to Strengthen Oversight and Help Providers Educate Patients on Privacy and Security Risks*, GAO-22-104454, September 2022, https://www.gao.gov/assets/gao-22-104454.pdf.
11 U.S. Department of Health and Human Services, Office for Civil Rights, "Resource for Health Care Providers on Educating Patients about Privacy and Security Risks to Protected Health Information when Using Remote Communication Technologies for Telehealth," content last reviewed October 17, 2023, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/resource-health-care-providers-educating-patients/index.html.
12 Pub. L. No. 110-425, 122 Stat. 4820 (2008).
13 21 C.F.R. § 1307.41(e).
14 Second Temporary Extension of COViD-19 Telemedicine Flexibilities for Prescription of Controlled Medications, 88 Fed. Reg. 69,879 (Oct. 10, 2023), https://www.federalregister.gov/documents/2023/10/10/2023-22406/second-temporary-extension-of-covid-19-telemedicine-flexibilities-for-prescription-of-controlled.
15 Telemedicine Prescribing of Controlled Substances When the Practitioner and the Patient Have Not Had a Prior In-Person Medical Evaluation, 88 Fed. Reg. 12,875 (March 1, 2023), https://www.govinfo.gov/content/pkg/FR-

2023-03-01/pdf/2023-04248.pdf.
16 225 ILCS 60/49.5(a).
17 225 ILCS 60/49.5(c).
18 Fla. Stat. 456.47; Florida Board of Medicine, "Out-of-State Telehealth Provider Registration," accessed December 6, 2023, https://flboardofmedicine.gov/licensing/out-of-state-telehealth-provider-registration/.