Health Information Compliance Alert

Case Study: Feds Indict 24 Individuals for Telemedicine Fraud

Prescribing DME or drugs via telemedicine? Document it - thoroughly.

If your practice is one of many jumping on the telemedicine train, your patients are lucky to have the electronic option of a clinician's care. However, the convenience of offering clinical services to electronically has its drawbacks. In fact, a recent case suggests the feds aren't playing any games when it comes to proving medical necessity for telemedicine claims.

Context: Last month, the **Department of Justice** (DOJ), in collaboration with the **Department of Health and Human Services** (HHS), and the **Federal Bureau of Investigation** (FBI), charged 24 defendants, including three licensed clinicians, for Medicare abuse and fraud. Five telemedicine firms, 130 durable medical equipment (DME) companies, and medical professionals concocted a scheme using telemedicine to defraud Medicare upwards of $1.2 billion.

The involved parties employed a plethora of tactics to trick patients and commit Medicare fraud, the DOJ report reveals. These included:

- Using international call centers to mine for vulnerable Medicare beneficiaries to sell free or low-cost DME products to.
- Bribing and giving kickbacks to telemedicine firms to arrange the DME orders.
- Paying physicians to write up medically unnecessary DME claims after conducting short visits via telemedicine, or even worse, write up claims without speaking with beneficiaries at all.
- Selling the DME orders garnered from the telemedicine firms to DME companies, who then fraudulently billed Medicare.

"These defendants - who range from corporate executives to medical professionals - allegedly participated in an expansive and sophisticated fraud to exploit telemedicine technology meant for patients otherwise unable to access health care," explains **Brian A. Benczkowski,** DOJ Criminal Division assistant attorney general, in a brief on the case.

DOJ in conjunction with the **Medicare Fraud Strike Force** are taking the lead on these enforcement activities and working closely with officials in New Jersey, the middle district of Florida, and South Carolina as well as the **Internal Revenue Service** (IRS) to settle the case. However, individuals charged in the case reside or practice in other areas of the United States, too, and impact the following states: California, Florida, Missouri, Nebraska, New Jersey, North Carolina, Pennsylvania, South Carolina, Texas, and Washington.

Note to providers: The DOJ appears to still be investigating other avenues related to the case. "Any doctors or medical professionals who have been involved with alleged fraudulent telemedicine and DME marketing schemes - including **Video Doctor USA, AffordADoc, Web Doctors Plus, Integrated Support Plus,** and **First Care MD** - should call to report this conduct to the FBI hotline at 1-800-CALL-FBI," offers the release.

Seek Guidance Before You Enter Into a Telehealth Arrangement

Before you embark on a business partnership with a telehealth vendor, you may want to seek legal assistance to determine the logistics of how you're going to conduct telemedicine at your office. "Telehealth arrangements can be quite complex and require a review by competent healthcare counsel," advises attorney **John E. Morrone,** a partner at **Frier Levitt Attorneys at Law** in New York City.

"Two critical elements of any telehealth analysis are, (i) does the communication between the physician and the patient comport with applicable state law; and (ii) how is the physician being compensated," Morrone says.

Caution: Not all telehealth and telemedicine companies are the same, as evidenced by the DOJ case. That's why it's essential to investigate your business associates before you enter into a contract. "If the physician is not billing the patient or the patient's insurance the arrangement is likely suspect," Morrone warns.

"Another red flag occurs if the undue pressure is placed on the physician to approve prescriptions or write orders for other ancillary services," he adds. "No arrangement should be structured to inappropriately influence the independent clinical judgement of the physician."

Tip: Before you sign on the dotted line with a telehealth company, consider your dealings with your other business associates like your EHR vendor. "Providers that would like to engage in telehealth need to evaluate the experience of the EHR vendor especially as it relates to their compliance programs. Special attention must be paid to HIPAA and patient privacy issues," indicates Morrone. "Many vendors inappropriately collect and sell patient data."

Resource: Read all the DOJ details about this billion-dollar case at www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes.

Don't Forget About Malpractice, Too

Being able to assist patients through telemedicine is a wondrous device for providers, but the rules are complicated. Practices must consider things as varied as state liability, procedure, and pharmacy laws as well as medical licensing rules and Medicare Administrative Contractor (MAC) jurisdictions.

Reasoning: The majority of telemedicine-related malpractice suits concern medication prescriptions across state lines without a face-to-face visit, explains attorney **Bonnie G. Ackerman,** of the national law firm **Wilson Elser,** in the Professional Liability Advocate blog. "Telemedicine poses unique medical malpractice risks and complicates traditional medical malpractice claims due to distinct issues regarding jurisdiction, procedure and duty of care," writes Ackerman.

Consider these five liability worries that Ackerman points to before you engage in telemedicine:

1. Liability laws of the state where you practice.
2. State licensing provisions of your state and other states.
3. Statutes of limitations for your state and other states.
4. The intersection of federal and state pharmacy laws and telemedicine.
5. Privacy and security rules and unauthorized medical personnel.