www.medscape.com

Docs Faked Patient Visits and Orders; Caught in Telehealth Crime

Harris Meyer

March 09, 2022

Hugh G. Deery II, MD, an infectious disease specialist in Petoskey, Michigan, received batches of prewritten physician orders for knee braces, along with patient "exam" notes and letters of medical necessity, from a marketing company that asked him to sign the orders. That company had obtained the detailed patient information from telemarketers who targeted seniors.

The marketing firm allegedly paid Deery, two other Michigan physicians, and a nurse practitioner to review and sign the orders and other documents for braces and cancer genetic tests. It gave the providers access to recorded phone calls between the telemarketers and Medicare beneficiaries, but didn't require them to listen to the calls or contact the beneficiaries, according to the US Department of Justice.

Deery and the other providers signed the documents. The marketing firm then sold the signed orders to durable medical equipment (DME) companies and genetic testing labs. Those companies billed Medicare for the braces and tests, listing Deery and the other clinicians as the referring provider.

Medicare paid out more than $7.3 million on those false claims. The three physicians settled civil False Claims Act charges and were fined, while the nurse practitioner pleaded guilty to a criminal charge of making a false statement, the Justice Department reported last August.

That investigation, dubbed Operation Happy Clickers, and other, larger enforcement actions over the past 3 years are part of the federal government's crackdown on telehealth fraud. It's a preemptive response to the skyrocketing use of telehealth during the COVID-19 pandemic, which the government has encouraged by easing Medicare payment rules for services provided through video and phone exams.

"Telehealth can foster efficient, high-quality care when practiced appropriately and lawfully," said US Department of Health and Human Services Agency (HHS) Deputy Inspector General Gary Cantrell in a September 2020 written statement. "Unfortunately, bad actors attempt to abuse telemedicine services and leverage aggressive marketing techniques."

Should doctors who use telehealth worry about being investigated?

The vast majority of physicians would never sign up for fraud schemes. But because telehealth delivery is new and potentially confusing, many doctors may be lulled into doing things they wouldn't previously have done. This could lead to legal problems. For instance, under the COVID-19 pandemic emergency rule waivers, physicians are allowed to bill Medicare for telehealth visits with patients they hadn't previously seen in person. So they should take common-sense precautions.

"Use your doctor brain: 'Can I properly evaluate this patient for whatever the clinical issue is via telehealth?' " advised Ty Howard, a former federal prosecutor who is with Bradley Arant Boult Cummings. He defends physicians in regulatory actions. "If you have questions about that, that's a big red flag."

Despite the crackdown, legal experts and telehealth industry leaders say physicians and other providers shouldn't worry about participating in telehealth delivery as long as they take the usual precautions to comply with the rules of Medicare and other public and private insurance programs. They express concern, however, that overzealous enforcement and new regulations could discourage physicians from offering telehealth services that benefit patients.

"Everyday medical providers doing their best have no reason to fear getting caught in fraud, waste, and abuse stories that involve criminals," said Kyle Zebley, the American Telemedicine Association's vice president of public policy. "Telehealth is no more prone to fraud than in-person care."

Still, some legal experts expect the Department of Justice, the HHS' Office of the Inspector General (OIG), and Centers for Medicare & Medicaid Services (CMS) to go further than attacking traditional fraud in their telehealth crackdown. The feds may start examining illegal telehealth practices, such as billing for more services than were actually provided, billing for services that were not provided, or inappropriately upcoding services.

"If you do a general video consult but bill for something more complex, that's classic upcoding, and that's where we're most likely to see fraud claims in the future," said Miranda Hooker, a former federal prosecutor at Troutman Pepper in Boston who defends clients accused of healthcare fraud. "Also, if you bill for a video consult when it's actually a phone consult, that's technically a false claim."

Demand for telehealth services soared as physicians and patients avoided in-person visits during the pandemic. During the first 6 months of 2020, 10.3 million traditional Medicare beneficiaries received at least one telehealth service, compared with 134,000 during the same period the year before, according to the Medicare Payment Advisory Commission.

That was made possible by public health emergency rule waivers that, for the first time, allowed all Medicare beneficiaries to receive coverage for at-home telehealth visits, as well as for audio-only phone visits.

The rules also let patients conduct telehealth visits with providers they had never seen in person. Under those rules, Medicare pays the same rates for telehealth visits as it does for in-person visits. And the program allows providers to reduce or waive deductibles and copayments.

These policies have heightened anxieties about potential increased spending due to telehealth overutilization and fraud. Federal officials fear that telehealth schemes could hit Medicare harder than in-person schemes because they can quickly achieve high volumes through physician-patient phone interactions.

For instance, the Department of Justice in 2019 charged 35 people, including nine physicians, with bilking Medicare out of more than $2.1 billion for medically unnecessary cancer genetic tests for hundreds of thousands of patients who were contacted by telemarketing firms.

MedPAC recommended last year that CMS do the following:

• Apply heightened scrutiny to clinicians who bill for many more telehealth services per beneficiary than other clinicians or who bill for a high volume in a week or month;

• Require clinicians to provide an in-person visit with a beneficiary before ordering expensive DME or lab tests;

• Prohibit "incident-to" billing for telehealth services not provided by clinicians who can bill Medicare directly.

While there are no specific criteria for telehealth overbilling, then-CMS Administrator Seema Verma wrote in 2020 that her agency would watch out for providers who bill for longer telehealth visits than they actually provide or who bill for more telehealth visits than are possible in a day.

So far, it's not clear whether telehealth has boosted spending by causing patients to see physicians more often than they would if they had to see them in person, researchers say.

Despite the lack of data, there is bipartisan support in Congress for extending or making permanent expanded Medicare access to telehealth after the public health emergency ends — but with new guardrails to prevent fraud and abuse. House and Senate bills would implement some of MedPAC's antifraud recommendations, such as requiring an in-person visit for ordering DME and lab tests.

Telehealth industry leaders argue that the newly proposed restrictions are unnecessary because it's easier to detect fraud in telehealth than for in-person care, owing to telehealth's digital trail. In addition, insurers and law enforcement agencies have adequate tools for ferreting out fraud, they say.

"We aren't happy with the idea of too many guardrails," said Joseph Kvedar, MD, board chairman of the American Telemedicine Association. "Having to see the provider in person every six months doesn't make sense to me. I worry about the chilling effect on providers."

The Department of Justice and the OIG have loudly trumpeted their campaign against telehealth fraud. But so far, they have focused on classic illegal kickback schemes. For example, Operation Happy Clickers targeted physicians and other providers who allegedly took payments for ordering medically unnecessary services.

Last September, the Department of Justice announced a nationwide criminal prosecution against 138 defendants, including 42 physicians and other medical professionals, for submitting $1.1 billion in false and fraudulent telehealth-related claims.

Telemedicine executives allegedly paid physicians and nurse practitioners to order unnecessary DME, diagnostic tests, and pain medications with limited or no patient interaction. In some cases, the medical professionals allegedly billed Medicare for sham telehealth consultations.

That same day, the CMS Center for Program Integrity announced it was revoking the Medicare billing privileges of 256 medical professionals for their involvement in telemedicine schemes.

Beyond targeting traditional fraud, the OIG and CMS are likely to start scrutinizing criteria for valid telemedicine visits, such as the site of the visit and the CPT codes that are used, said Howard. Those criteria could vary by state, since each state has different rules about telemedicine and establishing a physician-patient relationship.

"This will be murky because so much is in flux with COVID-19," Howard said.

Other legal experts, however, downplay the odds that antifraud enforcers will target providers for relatively minor issues, like billing for a video visit when only an audio visit occurred, particularly if that was due to technical difficulties. "Billing for the higher video code could be fraud if it's a knowing submission, but the government isn't spending time on one-offs," said attorney Colette Matzzie, a partner at Phillips & Cohen who represents whistleblowers in False Claims Act cases.

Other possible enforcement targets are physicians who use electronic health record systems or other technology platforms that promote upcoding and overbilling for telehealth services, Matzzie said.

"Providers have to be mindful that some health IT companies are advertising that they can dramatically increase your reimbursement," she said. "Algorithms can be built in that could lead to upcoding, and telehealth would be one of those situations. Be wary of those promises."

Telehealth violations like these may be harder to detect than fraud and abuse tied to in-person care because providers and patients may be sitting at home in front of a computer, and there are no nurses or other potential whistleblowers to witness these interactions, Matzzie warned.

Physicians should seek legal counsel before signing contracts to provide services for telehealth companies, Howard added. They need to consider what they're being asked to provide and what they're being paid for, especially if the contract involves a consult fee tied to ordering specific products or services.

"It's mostly relatively unsophisticated doctors who think, 'Great, I can do that between things and on weekends,' " Howard said. "They think they're insulated because they're receiving a consult fee from the company and they aren't directly billing Medicare. But that's a classic kickback violation."

On the other hand, the American Telemedicine Association's Zebley said the OIG has assured his organization that it's not going to target providers for honest mistakes, and it doesn't believe that telehealth is more likely than in-person care to generate fraud.

The OIG declined to provide an interview or written comment for this article.

"If you're doing all the right things consistent with in-person care — and it's not easy — you have nothing to fear from telehealth," Zebley said. "But if you think you can make a quick buck from virtual care, you'll be held to account at the end of the day."

For more news, follow Medscape on Facebook, Twitter, Instagram, and YouTube.

Credits:

Images: Maxkabakov/Dreamstime

Cite this: Harris Meyer. Docs Faked Patient Visits and Orders; Caught in Telehealth Crime - *Medscape* - Mar 09, 2022.