OIG looking closely at telehealth as it weighs future enforcement

In a HIMSS21 session with updates on the HHS inspector general's oversight and compliance efforts, officials said they plan to ensure virtual care is provided with integrity, and will take aim at telehealth fraud schemes.

By Mike Miliard | August 11, 2021 | 09:40 AM

Lisa Re, RN, and Andrew Vanlandingham

LAS VEGAS – The Office of Inspector General for the U.S. Department of Health and Human Services works to ensure the integrity of federal healthcare programs and to safeguard the health and welfare of those programs' beneficiaries.

In a session at HIMSS21 on Tuesday, two HHS OIG leaders offered a look at the enforcement priorities the agency has in mind these days, and some hints about the compliance responsibilities healthcare organizations should be prioritizing in the coming months.

OIG claims to recover three taxpayer dollars for every dollar it spends, and recoups billions in misspent money every year.

Speaking via webcam, Lisa Re, assistant inspector general of legal affairs at OIG, offered an update on some of the legal liabilities and risk areas in the health IT space, related to the False Claims Act, the Anti-Kickback Statute and the Civil Monetary Penalties Law.

She recounted some of the agency's enforcement actions in recent years, with companies such as athenahealth, CareCloud, eClinicalWorks and Practice Fusion required to pay millions to settle cases.

Andrew Vanlandingham, senior counselor for Medicaid Policy and acting health IT lead at OIG, called attention to recent revisions to safe harbors under the Anti-Kickback Statute and Civil Monetary Penalty Rules around coordinated care.

He also highlighted a major new priority at OIG: telehealth.

"As policymakers, we want to look at what telehealth might look like after the pandemic," said Vanlandingham. "All of those questions are centered around where do they plan on taking this? How will this impact their expenditures for healthcare programs? How to make sure that patients are getting good quality care from telehealth? And I think it's important for us to recognize that we don't know a whole lot right now."

He said the OIG is guided by a philosophy summed up in a quote from HHS Principal Deputy Inspector General Christi A. Grimm: "It is important that new policies and technologies with potential to improve care and enhance convenience achieve these goals and are not compromised by fraud, abuse or misuse."

When new technologies such as telehealth – with huge upside, but also potential risks – become more commonplace, "it's up to OIG and other healthcare stakeholders to make sure they do live up to that promise and aren't compromised by fraud, abuse or misuse," said Vanlandingham.

"And we recognize that a lot of folks in the audience are doing just that: implementing telehealth so it works for patients, for the providers, and is a good tool to enhance care."

He said OIG is "working hard to assess how telehealth utilization changed during the pandemic – what that means for corporate integrity, what that means for access, what that means for health equity. We have roughly eight audits and studies ongoing right now that we hope will really be the first down payment for OIG to be part of the broader conversation about what telehealth will look like after the pandemic."

The goal is to "help the health technology community and providers as they continue to refine their development of telehealth and enhance virtual care," he said.

"This is going to be a whole-of-government and whole-of-industry approach," he added. "It's really up to us to make sure that, since we are at this early stage of implementation of telehealth, that we can avoid issues to make sure that this works as intended, and really ensure that it drives the efficiency

and effectiveness and really improves healthcare for all Americans."

There have already been some ripe areas for enforcement, said Vanlandingham.

"We've had several large-scale national takedown actions involving telefraud schemes with sham or fake telehealth companies," he said. (One of them occurred just this week.)

"No one is billing for those telehealth visits fraudulently. They're not submitting a telehealth claim to Medicare. Instead, sophisticated criminal organizations are partnering with telemarketing companies and sometimes unscrupulous doctors to essentially cold call Medicare beneficiaries, get them online with a doctor. And the doctor [asks] a few questions, and then will forge or prescribe expensive equipment that Medicare will pay for durable medical equipment like back braces, or even genetic testing that beneficiaries don't need."

DME fraud has been around since Medicare started reimbursing for it, of course.

"But for these schemes, what used to be, let's say, $30 or $40 million dollars, maybe $100 million dollars, you've really seen an explosion of exploiting this virtual care model to really bill for a large amount of fraud," said Vanlandingham. "One scheme went for $1.6 billion, with a B, of alleged fraud. So that's obviously very alarming."

No one quite knows yet what "telehealth 2.0" will look like, he said.

"But I think it is a good example that, as we expand telehealth, there are likely to be instances of large-scale criminal activity that takes advantage of this. And it's up to OIG to assess those risks, and inform policymakers and stakeholders of those risks, and then from those policymakers and stakeholders to adjust."

OIG's job now, he said, is to decide "how we can better increase oversight and enforcement to make sure that whatever Congress, CMS and others should decide about how telehealth should be used as providers continue to adopt it, that we've got safeguards to maximize the benefit of telehealth for patients and providers."

Twitter: @MikeMiliardHITN
Email the writer: mike.miliard@himssmedia.com
Healthcare IT News is a HIMSS publication.