ALLIANCE for CONNECTED CARE

February 9, 2021

Ms. Christi Grimm
Principal Deputy Inspector General
U.S. Department of Health and Human Services
Office of Inspector General
330 Independence
Washington, DC 20201

Dear Ms. Grimm:

The declaration of the Public Health Emergency (PHE) and the subsequent action by Congress and the Executive branch to lift Medicare restrictions on telehealth has given us a unique opportunity to examine the impact of allowing seniors to access to telehealth services beyond institutions in rural areas.

The Alliance for Connected Care, a not-for-profit dedicated to facilitating the delivery of high-quality care using connected care technology, was pleased to see that as part of your 2021 workplan, you will conduct audits of Medicare Part B telehealth services during the PHE. This is exactly the kind of audit that is necessary to understand how Medicare reimbursement without restrictions is impacting the Medicare program. As you know, many policymakers are looking into long-term expansion of telehealth in Medicare, and meaningful data around these services during COVID-19 is crucial.

We writing today because previous OIG and DOJ investigations that are identified as "telehealth" were not actually related to telehealth. They were investigations of traditional fraud masquerading as telehealth. These schemes focused on durable medical equipment (DME), compounding pharmacy, opioids, diagnostic tests and other areas – rather than false claims related to virtual treatment of a patient. These schemes also took place before the Medicare restrictions on telehealth were lifted, and to the extent these criminals used real telehealth tools, the telehealth was the means to the end, not the source of the fraud itself.

As we work to educate lawmakers on the impact of the PHE Medicare telehealth changes, we are continually encountering a conventional wisdom that telehealth services are uniquely susceptible to fraud. After review of the HHS OIG/DOJ Health Care Fraud and Abuse Control Program's (HCFAC) prior year annual reports (FY2010-FY2018), we believe the more appropriate conclusion is that there is simply limited evidence of fraud in Medicare Part B Telehealth Services.

Additionally, some research on inappropriate telehealth billing has been the result of confusion and complexity, rather than fraudulent behavior. In the February 20, 2020 edition of the CMS MLN Connects newsletter, CMS acknowledged that the primary issue with Medicare telehealth compliance is due to

challenges related to billing and provided training videos and related content to help providers better understand how to bill appropriately.

When we looked back at the OIG reports, we found only one recent report that identified improper telehealth payments, and those payments were primarily due to administrative mistakes:

- 24 claims were unallowable because the beneficiaries received services at nonrural originating sites that did not fall under the demonstration program exception,
- 7 claims were billed by ineligible institutional providers,
- 3 claims were for services provided to beneficiaries at unauthorized originating sites,
- 2 claims were for services provided by an unallowable means of communication,
- 1 claim was for a noncovered service, and
- 1 claim was for services provided by a physician located outside the United States

Your office found that the causes of improper payments for Telehealth Services were the result of:

1. Medicare Contractors Were Unable to Implement Edits for Some Errors
   - The MACs could not implement edits for these types of errors because the claim form did not have a designated field for the originating-site location.
2. Contractor Claim Processing Edits Were Not Implemented
   - Some edits outlined in the Manual (chapter 12, § 190.7) were not implemented by the MACs.
3. Several Practitioners Were Not Aware of Requirements
   - Practitioner awareness can be accomplished through training practitioners on telehealth requirements and related online resources. Although CMS issues telehealth guidance, CMS currently does not offer telehealth training to practitioners.

In response, your office issued a series of recommendations, with CMS concurrence, to address improver telehealth payments. The Alliance for Connected Care supports these recommendations, many of which CMS has already taken.

1. Conduct periodic post-payment reviews to disallow payments for errors for which telehealth claim edits cannot be implemented (for example, unallowable originating sites or unallowable means of communication
2. Work with MACs to implement all telehealth claim edits listed in the *Medicare Claims Processing Manual*;
3. Offer education and training sessions to practitioners on Medicare telehealth requirements and related resources.

Given the tens of thousands of practitioners who never billed telehealth services in Medicare before last spring, our speculation is that when you conduct your study on telehealth billing this year there will be

some mis-billing similar to what you found in your 2018 report. However, we ask you to take care in differentiating deliberate actions to defraud American taxpayers from mistakes due to the complexity of billing the Medicare program.

When we looked into what could be causing lawmakers to believe that telehealth needed extra guardrails to protect against fraud, we realized that the reports and press releases on your website, Facebook and other places on the internet highlighted telehealth as parts of other fraudulent activity.

As an example, the $4.5 billion false and fraudulent claims DOJ lawsuit was against 86 criminal defendants who, according to the filing, were "*purporting to be telemedicine companies*" to commit Durable Medical Equipment (DME), diagnostic testing and pain medication fraud. The DOJ filings on "telemedicine" fraud, linked here and here, did not charge the defendants with submitting false telehealth claims, but with DME fraud. Further, this fraud was committed from 2016-2019 when the site restrictions were in place in Medicare. We are not aware of any evidence indicating a correlation between this kind fraud and the policies being discussed by lawmakers that would make permanent the PHE flexibilities to treat patients in their homes via telehealth.

On page 2 of the first filing, DOJ describes the accomplices as "*purporting themselves to be telehealth companies."* The DOJ described the criminal act this way: *"[they] gained access to Medicare beneficiary information for thousands of vulnerable Medicare beneficiaries from Company-1 and others, in order for [defendant] to sign DME orders for those beneficiaries*." The entire purpose of masquerading as "telehealth companies" was to submit false DME orders. We note that fraud actors masquerading as telehealth providers is a shared interest – both the federal government and legitimate telehealth providers are harmed by this activity.

The second filing describes the crime this way: *"During the relevant time period, De Lanoy worked for a company ("Company 1") at the center of the nationwide "telemedicine" scheme. Individuals known and unknown to De Lanoy developed a scheme that targeted the Medicare program to obtain millions of dollars in reimbursement for durable medical equipment, prescription creams and ultraviolet wands, among other items."* This was not a scheme to bill Medicare for telemedicine, they set up improper means of communicating with patients to get to the more traditional fraud.

We do not intend to suggest that lifting telehealth restrictions is not without risk, but calling DME and other traditional fraud "telehealth fraud" is comparing apples and oranges. A more apt comparison is in-person Medicare provider fraud and telehealth fraud.

We respectfully request that you update posts on your website, Facebook, in press releases and elsewhere related to what you call the "national telefraud takedown." In these materials you describe "telehealth executives" as masterminds of a fraud scheme. This kind of rhetoric is misleading and disrespects the dedication of people in health systems, tech platforms and employer HR departments trying to ensure that people have access to care. It is also likely to lead to millions of seniors – that may be homebound, or have limited access to providers—being deprived of access to legitimate telehealth services.

ALLIANCE for CONNECTED CARE

Real telehealth executives are the dedicated people who stepped up and managed a 13,000% increase in Medicare beneficiaries seeking health care services during the single month of April 2020. They are the people who went from providing telehealth software to 5,000 physicians, nurses and behavioral health providers to 40,000 in the first three months of the pandemic. Telehealth executives have been working tirelessly to ensure access to all kinds of care for their patients. Telehealth executives at some of our member companies have prioritized recruiting and retaining women practitioners on their platforms understanding the importance of keeping them in the workforce by providing the flexibility to manage the personal obligations that disproportionately fall on them. These telehealth executives must be differentiated from those who are "purporting to be telehealth executives."

We would be happy to work with you on designing and recommending tools to address the real fraud that is happening in the Medicare program. By better controlling inappropriate Medicare enrollment, solicitation, and prescribing while instituting stronger monitoring and audits to ensure fraudulent providers are caught sooner and weeded out of the system we can protect the program while ensuring access to needed services for Medicare beneficiaries.

Thank you for your consideration. We respectfully request that you consider meeting with experts among our member organizations to learn about the tools and tactics that can best differentiate legitimate telehealth providers from fraud actors pretending to offer telehealth.

Sincerely,

Krista Drobac
Executive Director
202-415-3260