PUBLICATION

HHS-OIG Enforcement Updates: Trends Relating to Telehealth Fraud Schemes and Tips to Avoid Them

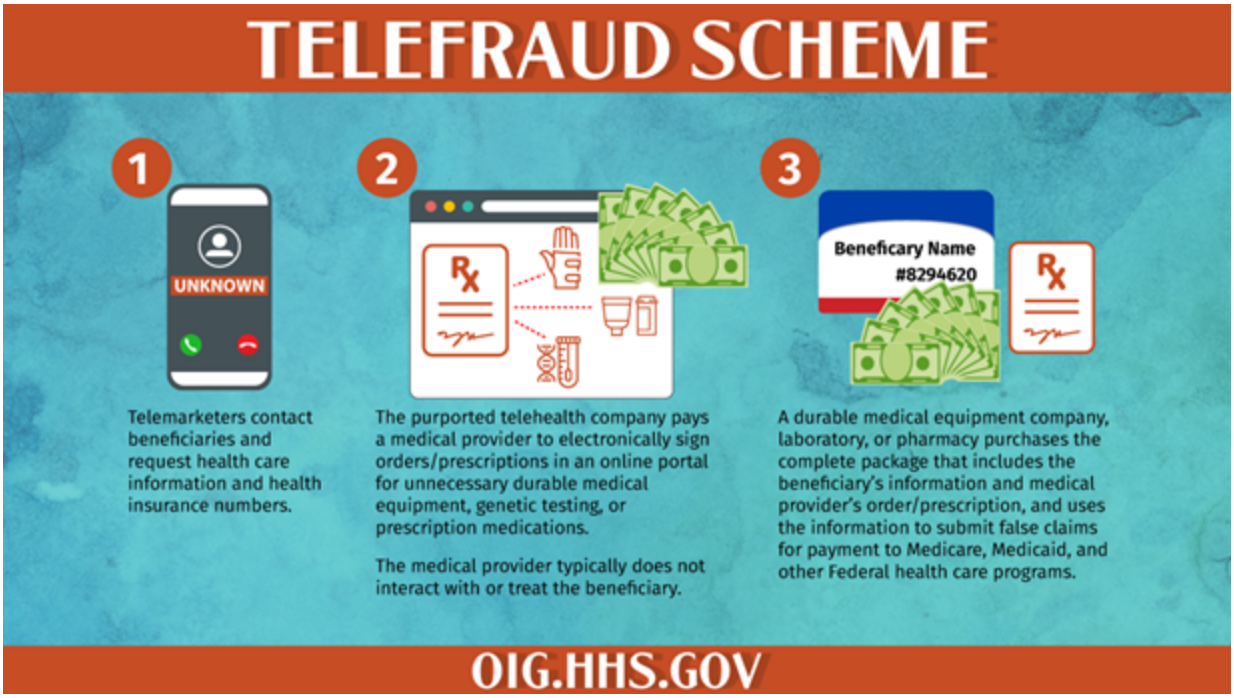
Authors: Thomas H. Barnard, Annie M. Kenville
July 26, 2022

On July 20, 2022, the Department of Health and Human Services (HHS), Office of Inspector General (OIG), released a Special Fraud Alert (the Alert) regarding fraudulent arrangements between practitioners and telemedicine companies, and a publication with tips for beneficiaries and providers to avoid being part of these schemes, emphasizing the protection of health information. This guidance was released alongside the Department of Justice's announcement of criminal charges against 36 defendants and the Centers for Medicare & Medicaid Services (CMS) Center for Program Integrity's announcement of administrative actions against 52 providers for fraudulent telehealth schemes.

The Alert and Publication Overview

In the Alert, OIG details the numerous ways companies providing telehealth, telemedicine, and telemarketing services have engaged in fraudulent schemes with physician and nonphysician practitioners. In almost all the fraudulent schemes, OIG determined that the companies were using kickbacks to recruit and reward practitioners by paying them in exchange for ordering or prescribing items of services without regard to medical necessity, or for purported patients with whom the practitioners had little or no contact. These schemes implicate federal health care programs and their beneficiaries by potentially increasing costs to those programs (charging these programs for medically unnecessary items or services), harming the beneficiaries (providing unnecessary items or services), and corrupting the physician's role as the medical decision-maker. Accordingly, they lead to potential criminal, civil, and administrative liability for both companies and practitioners.

In an associated "Featured Topic" publication on telehealth, the HHS OIG noted that telehealth services have had a recent expansion in benefits and flexibility by Congress, HHS, and CMS, which has been "critical to maintaining beneficiaries' access to care." In this publication, the OIG explained and diagrammed a typical "Telefraud Scheme," providing the graphic below:



The Alert and publication also provide a list of several "suspect characteristics" that OIG warns could indicate a fraudulent arrangement, and tips for both beneficiaries and providers to avoid being part of these schemes. The suspect characteristics include:

- When the company, or a sales agent, recruiter, call center, health fair, or advertising firm identifies or recruits the practitioner's patients;
- When the practitioner did not have the necessary information to meaningfully assess the medical necessity of the items or services, or follow up with the patient after the recommendation;
- When the company compensates the practitioner based on the volume of items or services ordered or prescribed;
- Factors relating to the company's acceptance of different health insurance; and
- Whether the company's product line is limited.

Tips for Avoiding Fraud Schemes

OIG noted in the publication that one of the common themes in these schemes is unlawful access to health information. Protecting and securing protected health information is a challenge for both beneficiaries and well-meaning health care providers who face constantly evolving threats to information security. Many of the tips provided by HHS focus on best practices for protecting information.

Historically, in fraud investigations, the old adage of "follow the money" was one of the most accepted practices. Future enforcement actions and the growth of cybersecurity threats put "follow the data" on similar status. Not only can data be stolen, but data can also be a form of "remuneration" as that term is defined by the Anti-Kickback Statute, and lack of compliance with cybersecurity and data protection requirements is a potential source of liability under the False Claims Act.

Takeaway

Providers should be carefully monitoring and updating their training and compliance material, and ensure it includes new and improved training on the proper handling of private information. The complete HHS and DOJ press release and reports can be found here. If you have questions on this topic or need assistance with

reviewing training and compliance materials, reach out to Tom Barnard, Annie Kenville, or any member of the Baker Donelson Government Enforcement and Investigations Team.