mercy care | mercy care advantage HMO SNP

COVID-19 provider webinar: Fraud, waste and abuse

June 16, 2020

Agenda

- **COVID-19 Fraud Schemes**
    - Phishing, counterfeit tests and supplies, ransomware/malware, etc.
- **Case Study**
- **Educating patients and staff**
- **How to report fraud**
- **Resources**

COVID-19 fraud schemes

Aggressive scams playing on public fears around COVID-19 that use tricks or threats to:

- Outright defraud you or your company of money
- Gain access to your sensitive information (to defraud Medicare, Medicaid or your patients of money)
- Install malware/ransomware on your computer (to defraud you, your company or patients of money)

COVID-19 fraud schemes vary

- Phishing emails with links and attachments
- Cold calls or robocalls
- Online, social media scams
- On-site, in-person visits

COVID-19 fraud scheme: Phishing

- You get an unsolicited **phone call** from someone who says they're a lab representative. They promise overnight delivery of COVID-19 viral and antibody test kits. Before they can process the order, they need to verify your name, address, National Provider Identifier (NPI) and Tax Identification Number (TIN).
- They can now file fraudulent claims through Medicaid or Medicare that appear as though they are coming from a legitimate source – your company.

COVID-19 fraud scheme: Counterfeit tests, supplies

- You want to expand your services by offering coronavirus testing, but tests are in short supply. A robocall from a lab you've never worked with promises overnight delivery of a significant batch of inexpensive COVID-19 test kits and N-95 masks with a low, upfront down payment.
- The supplies either never arrive or are unauthorized or counterfeit.

Fraud scheme: False cures, treatment offers

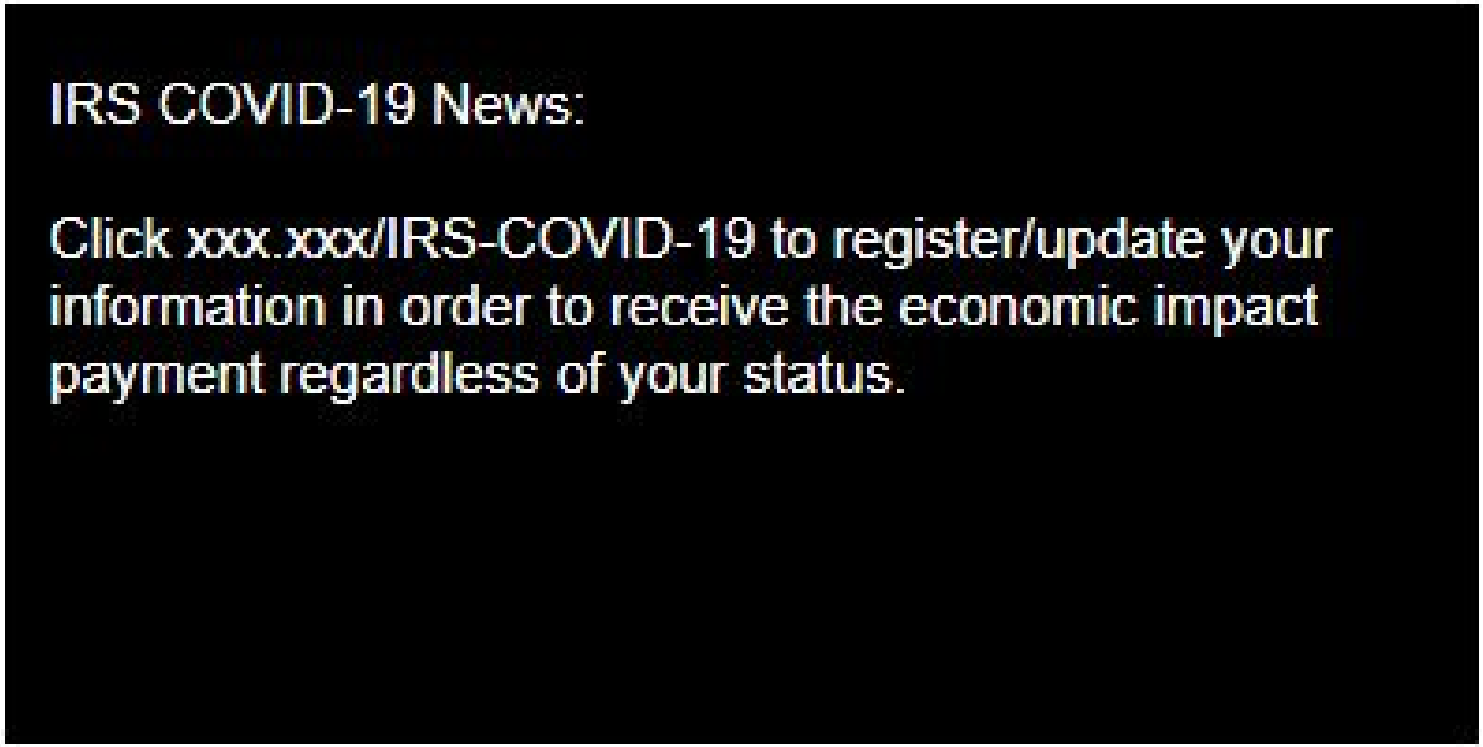
The Arizona AG's office shut down claims by YiLo, a local company, that their tincture helped the immune system resist and combat COVID-19.

YiLo * COVID-19 cautions cont.
Coronav Immunization
Stabilizer Tincture Now
Available WSL, 10% OFF Online
Leafly Orders Continues
http://yeatic.com/reMGBDR

Fraud scheme: Ransomware, malware

- Your employee gets an email from **CDC.com**, marked urgent**,** inviting them to click on “this link” to learn about a breakthrough COVID-19 cure or prevention treatment.
- With one click on a link, or one download of an attachment, everyone is locked out of your network.
- That link or attachment downloaded software that holds hostage sensitive details about your customers, employees and company.
- The attackers ask for money or cryptocurrency in exchange for release of the information.
- This is a ransomware attack.

Social media: Ransomware bait



Fraud scheme: Job hunting, recruiting

- Healthcare professional being recruited online for lucrative jobs related to COVID-19. Offers are rescinded after the individual provides their personal, enrollment and billing information.
- Forbes published an article on May 11, 2020 with some warning signs of jobs hunting scams.
    - For example, a scam job offer will have a sense of urgency. No phone or video communication. May request payment for an application, uniforms, a background check or an employee processing fee. A false offer may also request personal identification information prior to completing the hiring process.

Fraud scheme: Medically unnecessary tests, services and products

- Providers going into skilled nursing facilities (SNF), assisted living centers (ALC) and hospice facilities to conduct medically unnecessary COVID-19-related tests and services without regard to patient symptoms
- Telemarketing companies engaging in illegal kickbacks with international calls centers, medical providers and durable medical equipment (DME) companies to get personal information and submit fraudulent claims
- Fraudsters soliciting sensitive information from individuals to bill for medication(s) for which they were never appropriately evaluated

A case study: Harmony Medical Care

TAKE CONTROL OF YOUR HEALTH DURING THESE UNCERTAIN TIMES.

mercy care | mercy care advantage

A case study

On May 25, 2020, the U.S. Attorney's Office for the District of Arizona filed a criminal complaint charging Jeremiah Faber, the CEO of Harmony Medical Care, with health care fraud and money laundering.

The complaint alleges that Faber used Harmony's Facebook and other social media sources to offer free COVID-19 testing in order to induce patients to also complete Harmony's Comprehensive Whole-Body Assessment.

The complaint documents the case of one patient who visited Harmony for the free COVID-19 test. This patient was then given additional services that were medically unnecessary. The complaint further alleges that Harmony subsequently submitted false claims to Mercy Care by billing for these medically unnecessary services under the names of physicians who had no involvement with the patient's testing.

Protect your community through education

Scammers are also targeting your patients. Often the goal is to obtain their Medicare or Medicaid information to file fraudulent claims. You've probably heard some of these:

1. Home delivery of home supplies
2. Free diabetes monitor and COVID-19 test
3. Free coronavirus test kit delivered immediately

**Click each link above to hear the recording of each example

A COVID-19 FWA community forum

Mercy Care is hosting a similar forum for your patients, our members and the community. They can learn more about ways that scammers target them with fraudulent scheme and how they can protect themselves.

Once we schedule that event, “COVID-19 Fraud, Waste and Abuse: A Community Forum,” we’ll send out a provider notice with the details. Then, you can help us get the word out and encourage your patients and others in the community to attend.

Protect your company: Educate your staff

- Do not open attachments or click links within emails from senders you don't recognize.
- Do not provide your username, password, date of birth, social security number, financial data, or other personal information in response to an email or robocall.
- Check for misspellings or wrong domains within a link (for example, an address that should end in a ".gov" ends in .com" instead).
- Ignore offers for a COVID-19 vaccine, cure or treatment.
- Be cautious of purchasing personal protective equipment (PPE) from unknown third-party vendors. Verify the company is legitimate before ordering or sending money.

Sources:
https://azahcccs.gov/AHCCCS/AboutUs/covid19.html;
https://www.ic3.gov/media/2020/200320.aspx

Report COVID-19 schemes, fraud

If you believe you have been a target of a coronavirus-related scam, or know someone else who has been, you should report the fraud. You can report fraud in several ways:

- National Center for Disaster Fraud Hotline: **1-800-720-5721** or **https://www.justice.gov/disaster-fraud/ncdf-disaster-complaint-form**
- Medicare fraud: **1-800-633-4227**
- Mercy Care Fraud Hotline: **1-800-810-6544**
- Arizona Attorney General's Office: **www.AZAG.gov/complaints/consumer**
- FBI's IC3 (for internet-related scams): **www.IC3.gov**

Resources

Fraudsters and scammers are constantly changing their approach and developing new ways to use COVID-19 to trick and threaten companies and individuals out of sensitive information or money.

Get the latest alerts about COVID-19-related schemes and fraudulent activity:

- AZ Attorney General's COVID-19 Consumer Protection
- Office of Inspector General
- FBI Internet Crime Complaint Center (IC3): Fraud Alerts
- Federal Trade Commission Coronavirus Consumer Advice

Additional Resources

Go to www.MercyCareAZ.org

- Mercy Care Advantage Provider Manual
- All other programs Provider Manual
- Fraud, Waste, and Abuse reporting form
- Network Management Department
  - Select “Network Management Department”
  - Select the applicable contact list

Questions?

If you have questions about the information shared today, email your questions to:

MercyCareNetworkManagement@MercyCareAZ.org

You may also contact your Network Management Representative directly.

Thank You