Medicare Phone Scams and How to Protect Yourself

Medicare beneficiaries are targeted by scammers all year long, but fraudulent activity tends to increase around the Medicare Open Enrollment (MOE) period each year. Protect yourself by learning about the most common Medicare scams and how to determine whether communication from the Centers for Medicare & Medicaid Services (CMS) is legitimate.

Common Medicare Scams

Most of these scams take place over the telephone, but some do occur via email, U.S. mail and door-to-door visits. Fraudulent callers typically steal a person's identity by making up stories to try to obtain their name, Social Security number (SSN) or financial information. Medicare beneficiaries should be wary of the following schemes:

1. **Attempts to "verify your identity."**
   Someone calls to tell you that you must provide identifying information to receive a new or updated Medicare card. They may even tell you there's a charge for the new card and request a credit card number as well.
2. **Bogus offers for "free medical supplies."**
   A caller will pretend to offer durable medical equipment or a medical checkup at no cost to you because "Medicare will cover it." The only catch is that the caller needs your SSN or Medicare number to verify coverage and/or a credit card number to cover shipping costs for the free supplies.
3. **False claims that you're entitled to a "refund."**
   Another devious variation involves a caller who explains that, due to a vague change in Medicare coverage, you're owed a refund. They will typically ask for your Medicare number and bank account information so they can direct deposit the funds.

Scammers often gather some basic personal information on their targets like full names, birthdates, and mailing addresses before they even call. This data is used to convince you of their legitimacy and make you feel comfortable with sharing additional sensitive information. While evaluating your Medicare options for 2023, watch out for scammers targeting your money and personal information.

What Is Spoofing?

Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Scammers often use 'neighbor spoofing' so it appears that an incoming call is coming from a local number or spoof a number from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity.

How to Avoid Spoofing

You may not be able to tell right away if an incoming call is spoofed. Be extremely careful about responding to any request for personal identifying information.

- Don't answer calls from unknown numbers. If you answer such a call, hang up immediately.
- If you answer the phone and the caller or a recording asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.
- Do not respond to any questions, especially those that can be answered with "Yes" or "No."
- Never give out personal information such as account numbers, Social Security numbers, mother's maiden name, passwords, insurance information, or other identifying information in response to unexpected calls or if you are at all suspicious.

- If you get an inquiry from someone who says they represent a company or a government agency, hang up and call the phone number on your account statement or on the company's or government agency's website to verify the authenticity of the request. You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.
- Use caution if you are being pressured for information immediately.
- If you have a voicemail account with your phone service, be sure to set a password for it. Some voicemail services are preset to allow access if you call from your own phone number. A hacker could spoof your phone number and gain access to your voicemail if a password is not set.
- Talk to your phone company about call blocking options. The Federal Communications Commission (FCC) allows phone companies to block robocalls by default based on reasonable analytics. More information about robocall blocking is available at fcc.gov/robocalls.
- If a telephone number is blocked or labeled as a "potential scam" or "spam" on your caller ID, it is possible the number has been spoofed. Several phone companies and application developers offer call-blocking and labeling services that detect whether a call is likely to be fraudulent based on call patterns, consumer complaints or other means.

Tips to Help Prevent Medicare Fraud

DOs

- Protect your Medicare number and your Social Security number. Treat your Medicare card like it's a credit card. Don't ever give it out except to your doctor or other Medicare provider.
- Remember that nothing is ever "free." Don't accept offers of money or gifts for free medical care.
- Ask questions. You have a right to know everything about your medical care including the costs billed to Medicare.
- Know your rights and know what a provider can and can't bill to Medicare. Read your "Medicare & You" handbook or visit Medicare.gov to learn more about your rights
- Use a calendar to record all your doctor's appointments and what tests or x-rays you got. Then check your Medicare statements carefully to make sure all the details are correct.
- Be wary of providers who tell you that the item or service isn't usually covered, but they "know how to bill Medicare" so Medicare will pay.
- Make sure you understand how a plan works before you join.
- Report suspected instances of fraud.
- Review your "Medicare Summary Notices" or other statements from your plan for errors.

DON'Ts

DON'T allow anyone, except your doctor or other Medicare providers, to review your medical records or recommend services.

DON'T let anyone persuade you to see a doctor for care or services you don't need.

DON'T accept medical supplies from a door-to-door salesperson. If someone comes to your door claiming to be from Medicare or Medicaid, remember that Medicare and Medicaid don't send representatives to your home to sell products or services.

How to Report Suspected Fraud

Report suspected fraud to the Department of Health and Human Services (HHS) Inspector General by calling **1-800-447-8477** or emailing **HHSTips@oig.hhs.gov**. For more information on preventing Medicare fraud, visit the **http://www.stopmedicarefraud.gov/** website.