Social Engineering and Medicare Fraud

Social engineering is a tactic a scammer uses to trick you into giving them your personal information so they can commit fraud.



How does the scam work?

The scammer may use information they already know about you, like your name and address, to gain your trust. Once they have your trust, they try to get you to reveal more information, like your Medicare number. They can use that information to make money by billing Medicare for services you did not receive.

How do scammers get in contact?

Scammers may contact you over the phone, through text message, or via email. They often look at existing identity theft lists, social media, and other sources to learn about you before they get in touch.



Examples of Medicare fraud schemes using social engineering



A beneficiary received a free genetic testing kit in the mail. The form was pre-filled with some personal information and asked the beneficiary to provide their personal and insurance information to get their test results.



A beneficiary received a call from someone who already knew their name and address. The caller offered them a free back brace and followed up with a welcome letter that said they could get free orthotics.

Social Engineering and Medicare Fraud

Tips for avoiding scams

- Do not answer calls from unknown numbers.
- Be comfortable hanging up on a scammer. Consider having an exit line, like "My family member is on the other line. I need to hang up now."
- Know that Medicare will never call you to ask for your Medicare number, address, or other personal information. They already have it.
- Be wary of clicking on links in emails. If you get a strange email from your provider, a friend, or a family member, contact them directly to confirm whether they sent the email.
- Be suspicious of offers for free items or services and of people who use scare tactics or urgency to try and get you to provide your personal information.



Contact your Senior Medicare Patrol (SMP) to report potential Medicare fraud, abuse, or errors, or if you think you may have experienced fraud.

Who to Contact for Help

Senior Medicare Patrol (SMP): Contact your SMP if you think you have experienced potential Medicare fraud, errors, or abuse. An SMP representative will be able to help you identify what has happened and report any incidents to the proper authorities.

State Health Insurance Assistance Program (SHIP): Contact your State Health Insurance Assistance Program (SHIP) if you have questions about anything you read about Medicare online or hear about Medicare from unknown callers.

1-800-MEDICARE (633-4227): Contact Medicare to confirm what is covered and ask questions about anything you read online or hear about over the phone.

Local SHIP contact information	Local SMP contact information
SHIP telephone: 334-793-6843	**SMP telephone: 334-793-6843**
SHIP email: joy.riddle@sarcoa.org	**SMP email: joy.riddle@sarcoa.org**
SHIP website: www.sarcoa.org	**SMP website: www.sarcoa.org**
To find a SHIP in another state: Call 877-839-2675 (and say "Medicare" when prompted) or visit www.shiphelp.org	**To find an SMP in another state:** Call 877-808-2468 or visit www.smpresource.org

SHIP Technical Assistance Center: 877-839-2675 | www.shiphelp.org | info@shiphelp.org
SMP Resource Center: 877-808-2468 | www.smpresource.org | info@smpresource.org
© 2026 Medicare Rights Center | www.medicareinteractive.org

The Medicare Rights Center is the author of portions of the content in these materials but is not responsible for any content not authored by the Medicare Rights Center. This document is supported by the Administration for Community Living (ACL), U.S. Department of Health and Human Services (HHS) as part of a financial assistance award totaling $5,726,000 with 100% funding by ACL/HHS. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by ACL/HHS, or the U.S. government.