Medical Identity Theft

What is medical identity theft?

Medical identity theft is when someone fraudulently gets and uses your personal information, like your:

- Name
- Medicare number
- Social Security number
- Driver's license number
- Address



To then use this information to:

- Get medical treatment
- Buy medical equipment
- Get prescriptions
- Submit claims to your health insurance for items you don't need, request, or may have never received.

How to protect yourself from medical identity theft

- Be careful about who you give your personal information to.
- Never give out your Medicare number to anyone who contacts you through unexpected or unknown calls, texts, or emails. Remember that Medicare and Social Security will never reach out to you to ask for your personal information.
- Keep documents that contain your medical information somewhere safe.
- When getting rid of these documents, shred them or wait for a local shred day.
- Look out for common fraud schemes used to steal personal information.
    - This includes scams offering "free" COVID-19 tests, back or knee braces you didn't ask for, genetic testing, cancer screening kits, "new" Medicare cards, and telehealth.

Medical Identity Theft

Identify the signs of medical identity theft

If someone steals and then uses your medical information, be on the lookout for:

- Charges and providers on your Medicare statements that you don't recognize
- Shipments of back or knee braces, testing kits, or other medical supplies that you didn't ask for
- Contact from a debt collection company for a provider bill that you don't owe
- Medicare and/or your Medicare Advantage (MA) plan denies or limits your coverage or benefits because of a medical condition you do not have or says you already received a product or service when you did not

Report medical identity theft

If you believe someone has stolen your medical information, contact your local Senior Medicare Patrol (SMP). Your SMP will encourage you to:

- Review your Medicare statements for any additional concerns
- Get copies of your medical records from providers the scammer may have used
- Review your credit reports
- Report any errors on medical records or statements to your providers and your compromised number to Medicare, 1-800-Medicare (633-4227) or your MA plan
- If you gave out your Social Security number, report it to Social Security and make a recovery plan using the Federal Trade Commission's tips at www.IdentityTheft.org



Contact your **Senior Medicare Patrol (SMP)** to report medical identity theft!

Visit www.smpresource.org or call 877-808-2468.

Medical Identity Theft

Who to contact for more information:

- **Senior Medicare Patrol (SMP):** Contact your local SMP if you believe your medical information has been compromised.
- **State Health Insurance Assistance Program (SHIP):** Contact your local SHIP if you have other questions about your Medicare health coverage.

Local SHIP contact information	Local SMP contact information
SHIP toll-free:	**SMP toll-free:**
SHIP email:	**SMP email:**
SHIP website:	**SMP website:**
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
© 2025 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 $3,000,000 with 100 percent 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.

Medicare Minute Teaching Materials — November 2025
Medical Identity Theft

1. What is medical identity theft?
Medical identity theft occurs when someone fraudulently gets and uses your personal information (such as your name, Medicare number, or Social Security number) for medical treatment, equipment, prescription drugs, or submits claims to your health insurance for services that are not needed, requested, or medically necessary.

Medical identity theft can affect your medical and health insurance records. Every time a scammer uses your information, a record is created with incorrect medical information about you. This could affect the medical care you're able or unable to get.

Medical identity theft can also impact your finances. Scammers won't pay for the fraudulent services they bill with your information, potentially leaving you with unpaid bills or even medical debt that can ruin your credit.

2. How can I protect my medical information from theft?
First, be careful about who you give your medical information to. Some doctors' offices may ask you for information to confirm your identity. If they ask for your Social Security number, ask if you can instead use your birth date or just the last four digits of your Social Security number. Be very careful if someone other than your doctor's office asks for your medical information. Even if it's a business or organization that you trust, ask lots of questions. Ask why they need the information, what they will do with the information, who they will share the information with, and how they will protect the information. Protect it like you would your credit card.

Second, beware of unexpected texts, calls, or emails. Whether the message or call is directly asking for your medical information or encouraging you to click on a link or act fast, this is potentially a scammer trying to steal your information. Instead of responding or clicking on links, confirm the information is real by logging into your health insurance account using a link you know is real or a phone number you know is accurate. If the message is from a company you know is real and you use, contact them separately from unexpected calls or messages by using contact information that you know and trust. Remember that Medicare and Social Security will never reach out to you and ask you for your Medicare number, Social Security number, or mailing address.

Third, keep documents that contain your medical information somewhere safe. This might include things like your health insurance card, insurance enrollment forms, prescription drug bottles, and billing statements. If you receive these types of documents in the mail, try to avoid leaving them in an unlocked mailbox for long. And if you need to get rid of these things, use a shredder or wait for a local shred day in your community. Before throwing out pill bottles, use a dark pen or marker to cross out any of your personal information on the bottle.

3. What are common fraud schemes used to steal medical identity information?
Certain types of care and equipment are popular for medical scammers and identity thieves. It's helpful to know some of the common scams, so you can recognize the red flags.

COVID-19 scams: Do not share any information with someone who comes to your door or calls you unexpectedly to offer you "free" COVID-19 tests, treatment, or supplies. Fraudsters can bill Medicare for sham tests or treatments you may never receive, to illegally obtain money or Medicare numbers.

Durable Medical Equipment (DME) scams: Don't accept offers for "free" equipment or supplies in exchange for your Medicare number. DME is crucial for many Medicare beneficiaries. But many fraudulent companies across the country are charging beneficiaries for equipment without showing its medical necessity or without even sending the equipment to you. Look out for charges on your Medicare statements for items you don't need, weren't requested, or didn't receive. Beware of suppliers who try to get your information during a presentation, at a health fair, with a sales pitch, or from an unsolicited phone call.

Genetic testing scams: Reject offers of "free" testing without your doctor's order and do not give out your Medicare number or driver's license number at health fairs, senior centers, or other public spaces. Scammers may offer Medicare beneficiaries cheek swabs for genetic testing to get your medical information. Genetic testing may also be advertised as a cancer screening, DNA test, hereditary cancer screening, dementia test, pharmacogenetics (medication metabolization), or Parkinson's screening. Look for any charges (usually for thousands of dollars) for a broad range of genetic tests that you did not request or receive.

Medicare card scams: Do not share your Medicare number with someone claiming they need to confirm it before sending you a new card or to make sure you have the up-to-date Medicare card. They may claim that you are getting a new Medicare card (perhaps plastic, with a chip in it, or in black and white). In 2018, Medicare updated the Medicare card, removing a person's Social Security number and instead including a random identifier. That was the last time the card was updated, and there is no plan to update it again.

Telehealth scams: Do not agree to services offered by someone asking about your pain or family history who then transfers you by phone to someone else so you can "get approved" for a service. Medicare covers telehealth services, also known as teledoc services or telemedicine. But scammers may try to use telehealth services to steal from beneficiaries and the Medicare program. They may fraudulently bill for telehealth services as well as other services such as a back brace, knee brace, or genetic testing that you don't need or want, in exchange for your information.

4. What are some signs of medical identity theft?

If someone fraudulently steals and uses your medical information, be on the lookout for:

- Charges and providers on your Medicare statements that you don't recognize.
- Shipments of back or knee braces, testing kits, or other medical supplies that you didn't ask for.
- Contact from a debt collection company for a provider bill that you don't owe.
- Medicare and/or your Medicare Advantage (MA) plan denies or limits your coverage or benefits because of a medical condition you do not have or says you already received a product or service when you did not.

5. What should I do if I think someone is using my medical information?
If you believe someone has stolen and is using your medical information, contact your Senior Medicare Patrol (SMP). SMPs empower and assist Medicare beneficiaries, their families, and caregivers to prevent, detect, and report Medicare fraud, errors, and abuse. Contact information for your local SMP is on the last page of this document.

Your local SMP can help guide you through what to do if you think your medical information has been compromised. Along with reporting your concerns to the appropriate entities, an SMP may encourage you to:

Review your Medicare statements. Look for any services, items, or prescriptions that you did not receive or any providers you don't recognize.

Get copies of medical records. Contact each doctor's office, hospital, pharmacy, and health insurance company where the thief may have used your information. Explain that your medical identity has been compromised and request that they send you your records. You may have to complete records request forms or pay a fee for copies to be made.

Report errors. Report any mistakes you find in your medical records to your health care provider. Report the errors in writing, including a copy of the incorrect medical record.

Report your compromised Medicare number. Contact Medicare at 1-800-MEDICARE (633-4227). If you have a Medicare Advantage plan you should also contact your plan to let them know your information may be compromised.

Review your credit reports. Visit www.AnnualCreditReport.com or call 877-322-8228 to get your free credit report. Look for medical billing errors, like medical debt collection notices that you don't recognize. Report errors with the help of your SMP.

6. Who can I contact for more help?

Senior Medicare Patrol (SMP): Contact your local SMP if you believe your medical information has been compromised. Contact information for your local SMP is on the last page of this document.

Social Security Administration (SSA): If you gave our your Social Security number, report it to SSA. From there you can also make a recovery plan using the Federal Trade Commission's website www.IdentityTheft.gov.

State Health Insurance Assistance Program (SHIP): Contact your local SHIP if you have other questions about your Medicare health coverage. Contact information for your local SHIP is on the last page of this document.

Case study

Bill is 72 years old and has Medicare. He got a call recently from someone claiming to work for a local physical therapy office. They asked if he's been experiencing knee or back pain, because if so, they could send him a free brace as part of a current promotion that will be expiring today. Bill confirmed that he does have knee pain and would appreciate a free knee brace. The caller asked for Bill's Medicare number, explaining that the brace was free, but that they still needed to send the claim to Medicare. Bill provided his information, and a week later received a package with multiple knee and back braces. Bill didn't request a back brace. Bill's wife started asking questions about this caller and promotion, and Bill realized he doesn't remember or even know the name of the person he spoke to. He is growing worried that he gave out his Medicare number to someone that he maybe shouldn't have trusted.

What should Bill do?

- Bill should contact his local Senior Medicare Patrol (SMP), who can help review the concern with him and report it to appropriate entities. They can also help him with the next steps:
    - If Bill doesn't know how to contact his local SMP, he can visit www.smpresource.org or call 877-808-2468.
- Bill should call Medicare to report his compromised information. He may be issued a new Medicare number and card if Medicare determines it necessary.
- Bill should keep an eye on his upcoming Medicare statements for any services, equipment, or prescriptions he doesn't recognize. He should be carefully reading his Medicare Summary Notices (MSNs) or Explanations of Benefits (EOBs).
- Bill should look out for any communications from Medicare or his plan. A red flag would be Medicare or his Medicare Advantage plan denying or limiting his coverage for reasons unfamiliar to him, such as a health condition they mistakenly claim he has.
- Bill should request medical records from any health care provider or facility where he thinks a scammer used his medical information.
- Bill should review upcoming credit reports for anything suspicious, like medical debt that he doesn't owe.
- Bill's SMP should help him through this process—both to report his compromised medical identity and to recover it. Bill can also visit www.IdentityTheft.gov to make a recovery plan.

Local SHIP Contact Information	Local SMP Contact Information
SHIP toll-free: **SHIP email:** **SHIP website:** **To find a SHIP in another state:** Call 877-839-2675 and say "Medicare" when prompted or visit www.shiphelp.org.	**SMP toll-free:** **SMP email:** **SMP website:** **To find an SMP in another state:** Call 877-808-2468 or visit www.smpresource.org.

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 $3,000,000 with 100 percent 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.

SHIP Technical Assistance Center: 877-839-2675 | www.shiphelp.org | info@shiptacenter.org
SMP Resource Center: 877-808-2468 | www.smpresource.org | info@smpresource.org
© 2025 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.

Medicare Minute Script – November 2025
Medical Identity Theft

Point 1: Understand medical identity theft.
Medical identity theft is when someone fraudulently gets and uses your personal and medical information to get treatment, equipment, or prescriptions. Every time a scammer uses your information, a record is created with incorrect medical information about you. This could affect future care you're able or unable to get. Medical identity theft can also impact your finances. Scammers won't pay for fraudulent services they billed with your information. This can potentially leave you with unpaid bills or medical debt that can affect your credit.

Point 2: Protect yourself from medical identity theft.

- Be careful about who you give your personal information to. This includes your Medicare number, Social Security number, credit card numbers, and driver's license number.
- Never give out your Medicare number to anyone who contacts you through unexpected calls, texts, or emails. Remember that Medicare and Social Security will never reach out to you to ask for your personal information.
- Keep documents that contain your medical information somewhere safe. This includes your health insurance card, insurance enrollment forms, prescription bottles, and billing statements. If you want to get rid of these things, shred them or wait for a local shred day. Before throwing out prescriptions, use a marker to cross out any personal information on the bottle.
- Look out for common fraud schemes used to steal personal information. These include scams offering to "free" COVID-19 tests, durable medical equipment such as back and knee braces that you didn't ask for, genetic testing or cancer screening kits, and "new" Medicare card scams.

Point 3: Identify the signs of medical identity theft.
If someone steals and then uses your medical information, there will likely be signs, such as:

- You see charges on your Medicare statements for services, equipment, or medications you didn't receive, didn't need, and you didn't request.
- You get a shipment of braces, testing kits, or other medical supplies in the mail that you didn't request.
- You are contacted by a debt collection company for a provider bill you don't owe.
- You review your credit report and see a note of medical debt collection that you don't recognize.
- Medicare and/or your Medicare Advantage (MA) plan denies or limits your coverage or benefits because of a medical condition you do not have or says you already received a product or service when you did not.

Point 4: Respond to and report medical identity theft.
If you believe someone has stolen and is using your medical information, contact your local Senior Medicare Patrol, or SMP. Your SMP will encourage you to:

- Review your Medicare statements. Look for any services, items, or prescriptions you didn't receive or any providers you don't recognize.
- Get copies of medical records. Explain the situation to your health care providers and request that they send you your records.
- Report errors. Report any mistakes you find in your medical records to your health care provider.
- Review your credit reports. Visit www.AnnualCreditReport.com or call 877-322-8228 to get your free credit report. Look for medical billing errors. This includes medical debt collection notices that you don't recognize.
- Report your compromised Social Security number (if you gave it out) to SSA.
- Make a recovery plan. Use the Federal Trade Commission's www.IdentityTheft.org to report identity theft and get a recovery plan.

Take Action:

1. Contact your Senior Medicare Patrol (SMP) if you believe your medical identity has been compromised.
2. Contact SSA if you gave out your Social Security number. Also make a recovery plan at www.IdentityTheft.org.
3. Visit www.AnnualCreditReport.com or call 877-322-8228 to get your free credit report and look for any medical billing errors.
4. Contact your State Health Insurance Assistance Program (SHIP) if you have other questions about your Medicare coverage.

Local SHIP Contact Information	Local SMP Contact Information
SHIP toll-free: **SHIP email:** **SHIP website:** **To find a SHIP in another state:** Call 877-839-2675 and say "Medicare" when prompted or visit www.shiphelp.org.	**SMP toll-free:** **SMP email:** **SMP website:** **To find an SMP in another state:** Call 877-808-2468 or visit www.smpresource.org.

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 $3,000,000 with 100 percent 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.

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
© 2025 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.

Posted here: https://www.shiphelp.org/about-medicare/blog

Medicare Minute Blog — November 2025

Medical Identity Theft

By Shea Corti

Medical identity theft is when someone fraudulently gets and uses your personal and medical information for treatment, equipment, or prescriptions. Every time a scammer uses your information, a record is created with incorrect medical information about you. This could affect future care you're able or unable to get. Medical identity theft can also impact your finances. Scammers won't pay for fraudulent services they billed to Medicare with your information. This may leave you with unpaid bills or medical debt that can affect your credit.

Let's discuss how you can prevent, detect, and report medical identity theft.

First, protect yourself from medical identity theft:

- Be careful about who you give your personal information to. This includes your Medicare number, Social Security number, credit card numbers, and driver's license number.
- Never give out your Medicare number to anyone who contacts you through unexpected or unknown calls, texts, or emails. Remember that Medicare and Social Security will never reach out to you to ask for your personal information.
- Keep documents that contain your medical information somewhere safe. This includes your health insurance card, insurance enrollment forms, prescription bottles, and billing statements. If you want to get rid of these things, shred them or wait for a local shred day. Before throwing out prescriptions, use a marker to cross out any personal information on the bottle.
- Look out for common fraud schemes used to steal personal information. These include scams offering "free" COVID-19 tests, back or knee braces that you didn't ask for, genetic testing or cancer screening kits, and new Medicare card scams.

Identify the signs of medical identity theft.

If someone steals and uses your medical information, be on the lookout for:

- Charges and providers on your Medicare statements for services, equipment, or medications you didn't receive.
- Shipments of back or knee braces, testing kits, or other medical supplies in the email that you didn't request.
- Contact from a debt collection company for a provider bill you don't owe.
- Medicare and/or your Medicare Advantage (MA plan denies or limits your coverage or benefits because of a medical condition you do not have or says you already received a product or service when you did not.

Report medical identity theft.

If you believe someone has stolen and is using your medical information, contact your local Senior Medicare Patrol, or SMP. Find your local Senior Medicare Patrol using the online SMP Locator or by calling 877-808-2468.

Your SMP will encourage you to:

- Review your Medicare statements for any additional concerns.
- Get copies of medical records from providers the scammer may have used. Explain the situation to your health care providers and request that they send you your records.
- Report errors. Report any mistakes you find in your medical records to your health care providers and your compromised number to Medicare, 1-800-MEDICARE (633-4227) or your MA plan.
- Review your credit reports. Visit www.AnnualCreditReport.com or call 877-322-8228 to get your free credit report. Look for medical billing errors. This includes medical debt collection notices that you don't recognize.
- If you gave out your Social Security number, report it to Social Security and make a recovery plan using the Federal Trade Commission's tips at www.IdentityTheft.org.

Still have questions?

Your SHIP is here for you! You can contact your SHIP for any Medicare-related questions or concerns you have. SHIP counselors are government funded to provide trusted, unbiased Medicare counseling at no cost to you. (Depending on your state, your SHIP may go by another name.) Use our online SHIP Locator or call 877-839-2675 (and say "Medicare" when prompted) to find your local SHIP.

If you think you have experienced potential Medicare fraud, errors, or abuse contact your local Senior Medicare Patrol using the online SMP Locator or by calling 877-808-2468.