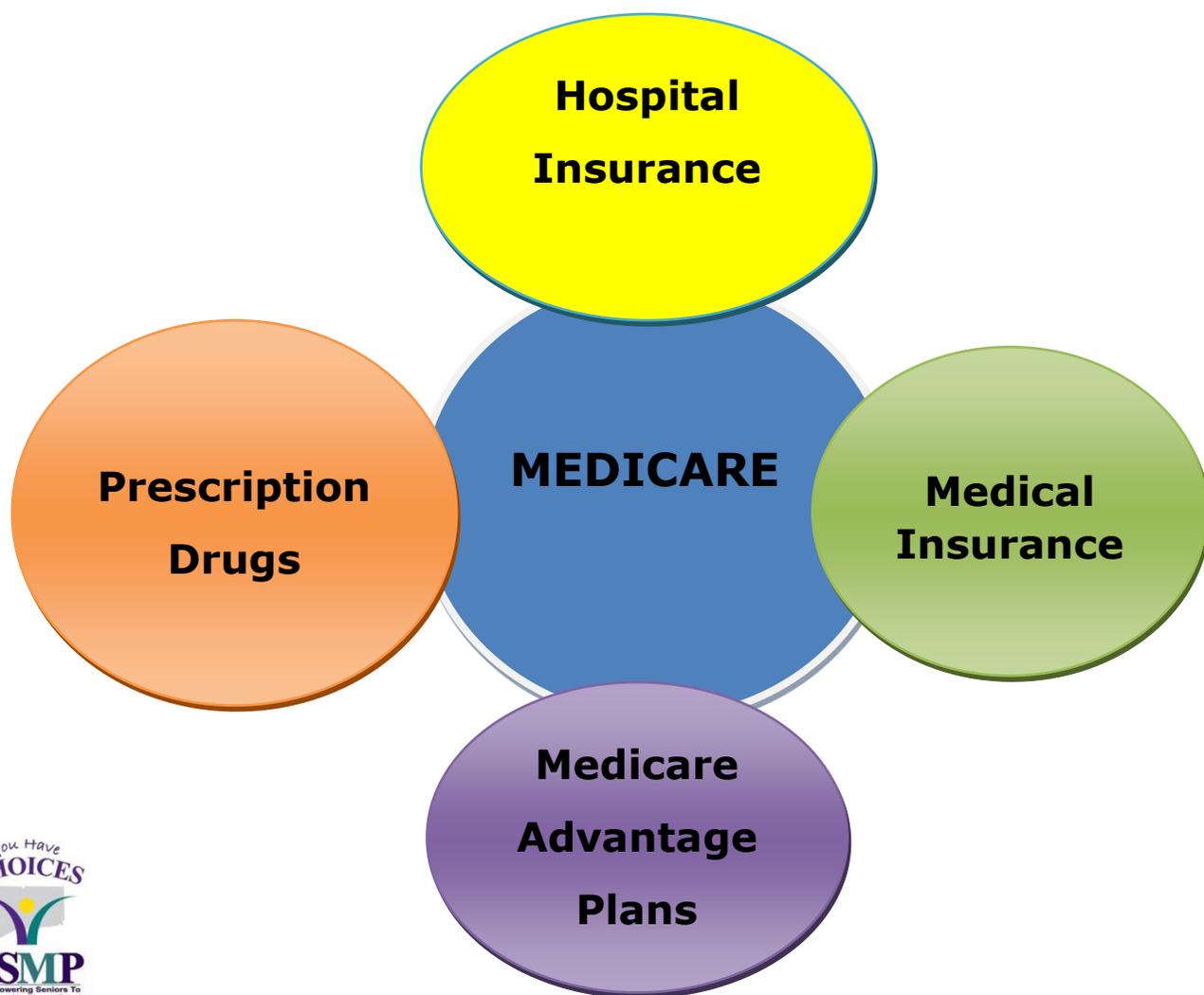


SCAM JAM

MEDICARE FRAUD

AND ABUSE



The production of this booklet was supported in part by Grant No. 90MP0237 from the Administration on Aging, Administration for Community Living (ACL).

The Western CT Area Agency on Aging, Inc. (WCAAA) is a private, non-profit CT corporation that was designated as one of five CT Area Agencies on Aging by the CT State Legislature and Access Agency by the CT Department of Social Services.

Mission statement: The Western CT Area Agency on Aging, Inc. develops, manages and provides comprehensive services through person centered planning for seniors, caregivers, and individuals with disabilities in order to maintain their independence and quality of life”.

Through a variety of federal, state and private funds, the WCAAA administers programs that provide direct services in community homes, provides grants and contracts to community non profit groups serving western area seniors to maintain community living and helps seniors with Medicare, Medicaid and other benefits’ issues. Our Medicare fraud initiative is one of our center piece programs as we work with state and federal agencies to find and report fraud.

The Western CT Area Agency on Aging, Inc. (WCAAA) is pleased to distribute the “Scam Jam, Medicare Fraud and Abuse” and "Scam Jam Fraud and Scams" Booklets. The WCAAA Senior Medicare Patrol, (SMP) staff has spent many hours developing these two booklets for the different Fraud and Scams in Medicare on the hope that seniors and others will become highly aware of potential fraudsters. Please feel free to call the WCAAA with corrections and specific comments relative to these two booklets at 1-800-994-9422 (within 41 town area) or 203-757- 5449.

CONTENTS

WHAT IS SMP?	4
WHAT IS A FRAUD?	5
FREQUENT VICTIMES OF FRAUD OR SCAMS	5
WHO ARE THE SCAMMERS?	5
SHOCKING NUMBERS	6
CRIMINAL AND CIVIL PENALTIES	7
MEDICARE FRAUD AND ABUSE	8-11
MEDIARE ADVANTAGE VIOLATIONS	12
FRAUD DONE BY AMBULANCE SERVICES	12
FRAUD DONE BY PROVIDERS	13
FRAUD DONE BY SUPPLIERS & RECRUITERS	13-16
FRAUD DONE BY COMPANIES	16
FRAUD DONE BY BENEFICIARIES	17
NEW MEDICARE CARD	18-19
TIPS TO PREVENT FRAUD AND SCAMS	20-21
INFORMATION SOURCES	22
WHO TO CONTACT IF YOU ARE BEING A VICTIM OF HEALTHCARE FRAUD / SCAM	22
FOR ALL OTHER TYPES PF FRAUD OR SCAMS CONTACT	23

WHAT IS SMP?

SMP is an acronym for the **Senior Medicare Patrol** Program. It started in 1997 and the U.S. Administration on Aging (AOA) is responsible for overseeing the SMP program which is part of the US Administration for Community Living (ACL).

Senior Medicare Patrols (SMPs) empower and assist Medicare beneficiaries, their families, and caregivers to prevent, detect, and report health care fraud, errors, and abuse through outreach, counseling, and education. SMPs are grant-funded projects of the federal U.S. Department of Health and Human Services (HHS), U.S. Administration for Community Living (ACL). Their work is in three main areas.

- 1) Conduct Outreach and Education:** SMPs give presentations to groups, exhibit at events, and work one-on-one with Medicare beneficiaries. Since 1997 more than 30 million people have been reached during community education events, more than 6.5 million beneficiaries have been educated and served, and more than 46,000 volunteers have been active.
- 2) Engage Volunteers.** Protecting older persons' health, finances, and medical identity while saving precious Medicare dollars is a cause that attracts civic-minded Americans. The SMP program engages over 5,200 volunteers nationally who collectively contribute more than 155,000 hours each year.
- 3) Receive Beneficiary Complaints.** When Medicare beneficiaries, caregivers, and family members bring their complaints to the SMP, the SMP makes a determination about whether or not fraud, errors, or abuse is suspected. When fraud or abuse is suspected, they make referrals to the appropriate state and federal agencies for further investigation.

If you have questions or concerns about health care fraud, are interested in volunteering, or would like to schedule a free speaker, call the Western CT Area Agency on Aging at 203-757-5449 (1-800-994-9422).



The information and examples provided in this booklet about Medicare frauds and scams are **NOT MEANT TO ALARM OR FRIGHTEN YOU**. They are to **educate you** and help you identify signs of frauds and scams.

WHAT IS A FRAUD?

Fraud, commonly known as a scam; is a crime involving deception, dishonesty and / or cheating. People who commit fraud are known as scammers (Scammers, scam artists). The fraudsters try to get your money or personal information such as social security number, Medicare number, bank accounts or credit cards. Then scammers use your personal information to get goods or services on your behalf or to take money from your accounts.

FREQUENT VICTIMS OF FRAUD OR SCAMS?

Experts say that seniors are the most frequent victims of scams, and here are some reasons why.

Seniors often:

- Have money (pensions, Collecting Social Security, savings) or properties (a house, stocks and bonds)
- Are in the house during the day and it is easy to contact them.
- Tend to trust people, especially people who are respectful.
- Are isolated and more willing to talk to unknown people.
- More easily intimidated and less likely to take action or complain.

WHO ARE THE SCAMMERS?

UNKNOWN PEOPLE: We all know that we should be careful with unknown people but it is easy to be a victim of them. Be very careful of any new person in your life, even if it is a new romantic couple, people who wants to help you with your finances, and stay away from those who ask for money or your information.

FAMILY, FRIENDS AND NEIGHBORS: While it is sad, loved ones are often the ones who take advantage. Use good judgment before

sharing your personal information with anyone, including your children.

SHOCKING NUMBERS!

Centers for Medicare and Medicaid Services (CMS), the federal agency that administers Medicare, reports that every year, millions of dollars are lost due to fraud, waste, abuse and improper payments. Below you will find recent statistics on National Healthcare fraud takedowns.

NATIONAL HEALTH CARE FRAUD TAKEDOWNS		
DATE	# OF PEOPLE CHARGED	AMOUNT OF LOSS
July 2010	94	\$251 million
February 2011	111	\$225 million
September 2011	91	\$295 million
May 2012	107	\$452 million
October 2012	91	\$430 million
May 2013	89	\$223 million
May 2014	90	\$260 million
June 2015	243	\$712 million
June 2016	275	\$800 million
TOTAL	Approx. 1,200	Over \$3.5 billion

Based on the statistics, the amount money lost increases every year, along with the number of victims. It for this reason that SMP considers a priority reaching out to the community and helping them prevent being a target of health care fraud

CRIMINAL AND CIVIL PENALTIES

Defrauding the Federal Government and its programs is illegal.

Criminal and civil penalties for Medicare fraud reflect the serious harms associated with health care fraud and the need for aggressive and appropriate intervention. Providers and health care organizations involved in health care fraud risk exclusion from participating in all Federal health care programs and risk losing their professional licenses.

MEDICARE FRAUD AND ABUSE



MEDICARE FRAUD AND ABUSE

A Serious Problem That Needs Your Attention

WHAT YOU SHOULD KNOW ABOUT MEDICARE FRAUD!

Medicare fraud typically includes any of the following:

- Knowingly submitting false claims or making misrepresentations of fact to obtain a Federal health care payment for which no entitlement would otherwise exist.
- Knowingly soliciting, receiving, offering, and/or paying remuneration to induce or reward referrals for items or services reimbursed by Federal health care programs.
- Making prohibited referrals for certain designated health services.
- Billing Medicare for appointments the patient failed to keep.
- Knowingly billing for services at a level of complexity higher than services actually provided or documented on file; this includes misusing codes on a claim, such as up coding or unbundling codes.
- Knowingly billing for services not furnished, supplies not provided, or both, including falsifying records to show delivery of such items.
- Paying for referrals of Federal health care program beneficiaries.

Real Life Case Example of Medicare Fraud:

A podiatrist committed several different types of fraud, but the one he commonly used was upcoding. The podiatrist would travel to nursing homes and complete basic procedures such as clipping toenails. Rather than billing for basic services, the podiatrist billed patients for different types of surgeries. Two patients billed for certain type of foot surgery were both double amputees, which eventually lead to the podiatrist getting caught.

Medicare Fraud Most Commonly Occurs In: Billing for institutional facilities such as nursing homes, residential facilities, hospitals and hospices.

- Billing for physician visits and services.
- Billing for durable medical equipment such as wheelchairs, body jackets, incontinence supplies or diabetic supplies.
- Improper marketing through phone calls, door-to-door sales and flyers.

Anyone can commit health care fraud. Fraud schemes range from solo ventures to broad-based operations by an institution or group. Even organized crime has infiltrated the Medicare Program and masqueraded as Medicare providers and suppliers.

Your Plan

- Never surrender Social Security, Medicare or health insurance numbers to anyone you don't know and trust.
- Be particularly wary of free health checks offered at shopping malls, fitness clubs and retirement homes (so-called rolling labs). If they ask to photocopy your cards or ask you to sign a blank insurance claim form, don't do it, (After all, it's supposed to be free.)
- Review all statements from your insurance provider. If there are any charges you don't understand, call immediately. And when shopping online for prescription drugs or other health-related items, remember that if a price seems too good to be true, it probably is.
- Always read your "**Medicare Summary Notice and Explanation of Benefits**" that is mailed to you after you have been to the doctor, had lab tests, therapy, ambulance transportation had a hospital stay and more. **YOU** should check these notices to make sure the YOU have received the services on them, if not you should report it to your doctor, Medicare or the Senior Medicare Patrol at the Western Ct Area Agency at 203-757-5449.
- You also receive a **Medicare Summary Notice 3 times** a year if you have had any medical services paid for by Medicare. These also need to be checked to make sure that you have the services that these notices are reporting.

REDESIGNED MEDICARE SUMMARY NOTICE For Part B (Medical Insurance)

Page 1



Medicare Summary Notice for Part B (Medical Insurance)

Page 1 of 5

The Official Summary of Your Medicare Claims from the Centers for Medicare & Medicaid Services

Facility Name
Your Name Here
Street Address
City, State 12345-6789

THIS IS NOT A BILL

Notice for Your Name

Medicare Number	XXX-XX-1234A
Date of This Notice	September 16, 2011
Claims Processed Between	June 15 – September 15, 2011

Your Claims & Costs This Period

Did Medicare Approve All Services?	NO
Number of Services Medicare Denied	2

See claims starting on page 3. Look for **NO** in the "Service Approved?" column. See the last page for how to handle a denied claim.

Total You May Be Billed	\$150.86
-------------------------	----------

Your Deductible Status

Your deductible is what you must pay for most health services before Medicare begins to pay.

Part B Deductible: You have now met **\$85** of your **\$162** deductible for 2011.

Be Informed!

Register at www.MyMedicare.gov for direct access to your Original Medicare claims, track your preventive services and print an "On the Go" report to share with your provider. Visit the Web site to sign up and access your personal Medicare information.

Providers with Claims This Period

June 18, 2011
Jane Doe, M.D.

June 28, 2011
John Doe, M.D.

June 29 – June 30, 2011
Any Doctor, M.D.

This Is The Current Version Being
Used. If You Have Medicare Fraud
Concerns Call 1-800-MEDICARE

MARKETING VIOLATIONS WITH MEDICARE ADVANTAGE PLANS

- Making unsolicited calls to beneficiaries to market items such as diabetes supplies or back braces.
- Requesting beneficiaries' health information, such as Medicare numbers and physician names, during unsolicited calls.

To learn about real-life cases of Medicare fraud and abuse and the consequences for culprits, visit the Stop Medicare Fraud Newsroom.

FRAUD DONE BY AMBULANCE SERVICES

Medicare's ambulance benefit is frequently misunderstood. Sometimes providers bill beneficiaries directly rather than billing Medicare and the beneficiaries wonder why. Sometimes beneficiaries



are seen being transported by ambulance when the trip doesn't seem medically necessary and bystanders suspect fraud or abuse. At other times, Medicare denies coverage of an ambulance ride and beneficiaries wonder why their trip wasn't covered.

Ambulance Fraud Schemes

- Falsification of documentation to provide the appearance of medical necessity, when medical necessity did not exist.
- Billing for more miles than traveled for transport.
- Billing nonemergency trips as emergency trips.
- Billing the beneficiary instead of Medicare, if the provider participates in Medicare and the trip met Medicare's coverage criteria.

Real Life Case Example

At local restaurant in CT older gentlemen passed out. An ambulance was called. On their way out, a young man came up to the ambulance driver and said " Could you please give me the keys to my

Dad's car so I can follow you to the Hospital?" This is a situation where unfortunately there are people who take advantage of the critical situation of the patient. Our job is to help our community become aware of these malicious people and give them the tools to avoid becoming a victim.

FRAUD DONE BY PROVIDERS

Providers commit fraud when they...

- **Submit bills for services not provided, or unnecessary services.** One common fraud is a "gang visit," when a provider visits a nursing home and bills for services as if they had treated most of its residents. In another instance, a provider may perform a service regardless of whether each resident needs it.
- **Upcode a service.** This is when a provider charges Medicare for a more expensive service than was provided. For example, a provider may bill for surgery, when only a bandage was placed over a cut.
- **Unbundle services.** This occurs when a provider submits separate bills for lab services that combine three or four tests, which are intended to be billed as one service. As a result, Medicare pays the provider more for each service than if the services were billed as a group.
- **Bill non-covered services as covered services.** This occurs when a provider bills a service such as routine toenail clipping (non-covered service) as foot surgery (covered service).



FRAUD DONE BY SUPPLIERS AND RECRUITERS

Suppliers and recruiters commit fraud when they...

- Bill for different equipment than what the beneficiary received.
- Bill for home medical equipment **after it's returned.**
- Solicit, offer or receive a bribe or kickback. Recruiters may stop Medicare beneficiaries on the street or make an at-home visit, offering money and promotional gifts as incentives to take "free"

medical exams, after which they give the beneficiary a list of durable medical equipment they do not need.

Free equipment: In a Medicare scam, callers might offer products that are “covered” by insurance, such as blood pressure cuffs, knee braces or glucose measurement devices. The scammers offer to file a claim on behalf of the senior to gain information like Medicare number, address, Social Security number and other details that can be used for medical identity theft. Sometimes, products do arrive, but they’re often shoddy quality, and worth far below the cost that the scammers might submit to Medicare.

What About Those Back And Knee Braces!

You receive a colorful postcard stating that the sender has been trying to contact you about ordering a Medicare-covered back or knee brace or saw an ad on TV all they need is for you to give them your Medicare information. What’s to lose?

This scam is particularly deceptive because you may actually receive something in the mail, usually a Velcro-style band for your back or knee. The scammer then bills Medicare for a device worth hundreds or thousands of dollars more than the one you received; and armed with your Medicare information, they can continue to bill Medicare for services not rendered.

Medicare has strict coverage rules for its services and supplies, and it pays to keep these tips in mind: Never respond to open solicitations for Medicare-covered supplies/services. Medicare only covers **Durable Medical Equipment (DME)** that is medically necessary **AND prescribed by a doctor**. The request should originate from your doctor, not a supplier. DME, like prosthetics, orthotics, and medical supplies must be prescribed and are for use in the patient’s home

The types of practices below are considered abusive or fraudulent.

Dumping of Supplies

Excessive amount of supplies delivered to a recipient that cannot possibly be used within the prescribed time frame. Supplies delivered for equipment the recipient no longer uses.

- Supplies delivered when there is no prescribed equipment to justify the delivery of supplies.
- Delivery of supplies or equipment that the beneficiary does not need or did not ask for.

Billing Practices

- Billing for rental equipment after date of return.
- Billing for equipment before it is delivered.
- Billing for equipment or supplies never provided.
- Billing that inappropriately overlaps with patient's hospital or skilled nursing facility stays.
- Refusing to pick up equipment after contact by recipient or physician and continuing to bill.
- Providing off-the-shelf items, such as shoe inserts, but billing Medicare for more expensive or custom-made items, such as custom diabetic shoes.
- Billing for unnecessary or excessive repair or maintenance costs.

Falsely Documenting Medical Necessity

- Completing documentation to show medical necessity for a patient not professionally known by the physician or treating practitioner.
- A supplier completing sections of necessary documentation reserved for the physician or treating practitioner.
- Falsifying documents to justify providing (or billing for) supplies to beneficiaries who do not otherwise meet the medical necessity requirement.

- Sending faxes to physicians requesting they sign off on equipment and supplies for individual patients is one way unethical suppliers attempt to obtain documentation regardless of true medical necessity. *These faxes are sometimes the consequence of information gained through marketing violations.*

Phony services: Similar to promises of “free” medical equipment, a caller might offer specialized services that are specifically geared toward seniors. These might include physical therapy for arthritis, pain management for chronic conditions and home nurse visits. Some scammers even claim that Medicare covers housecleaning services.

FRAUD DONE BY COMPANIES

Companies commit fraud when they...

- Offer a Medicare drug plan that hasn’t been approved by Medicare.
- Use false information to mislead beneficiaries into joining Medicare plans.
- Do not follow Medicare marketing rules. For example, a company may not send out an advertisement mailing with the Medicare or Centers for Medicare and Medicaid Services (CMS) logo on it. They also cannot offer financial incentives to their insurance agents and brokers that would encourage them to maximize commissions by inappropriately moving, or churning, beneficiaries from one plan to another each year.

FRAUD DONE BY BENEFICIARIES

Beneficiaries commit fraud when they...



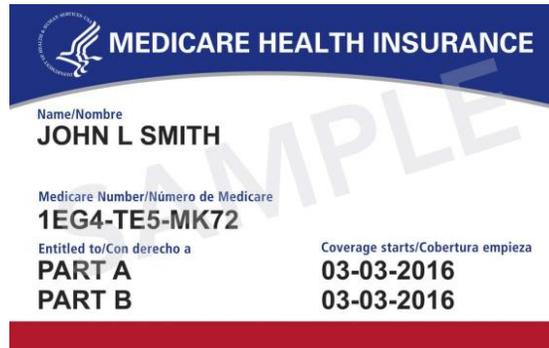
- **Let someone use** their Medicare card to get medical care, supplies or equipment.
- **Sell** their Medicare number to someone who bills Medicare for services not received.
- Provide their Medicare number in **exchange** for money or a gift. In some cases, beneficiaries may unknowingly commit fraud in this way.

“FREE” OFFERS

- Offering free supplies in exchange for Medicare numbers (and then billing Medicare, of course).
- Offering free meals, food, or nutritional supplements, then billing Medicare for costly liquid nutritional supplies only given through tube feedings.



NEW MEDICARE CARDS WHAT YOUR NEW MEDICARE WILL LOOK LIKE



New Card, New Number: Facts About Your NEW Medicare Card What People with Medicare and Caregivers Should Know

- ✓ **Your new Medicare card will NOT have your Social Security number. This will help protect your identity.** Medicare is removing Social Security Numbers from Medicare cards. Your new Medicare card will have a new Medicare number which is unique to you, and will be an 11 digit identifier that's a mix of numbers and letters.
- ✓ **You will not see your new cards before April 2018.** CMS will mail out cards no earlier than April 1, 2018 and will continue through April 2019. Understand that mailing everyone a new card will take some time. Your card might arrive at a different time than your friend's or neighbor's.
- ✓ **You do not need to do anything!** This change will be automatic. **CMS will send you your new card in the mail.** If someone calls you and says they need to confirm your identity, or your Medicare number, **it's a SCAM.** If you get a call from someone and you're just not sure, **hang up** and call the PA-SMP for help.

- ✓ **Your benefits will stay the same.** The new Medicare numbers will **not** change anything in your coverage. You can start using your new card as soon as you receive it. When you receive your new card, ***shred your old card.***

- ✓ **There is no charge for the new card. The card is free.** No one should tell you there is a one-time fee, or that you will lose benefits if you don't pay a fee or answer their questions.

SCAM ALERT ON THE NEW MEDICARE CARE

Scammers posing as Medicare reps will call asking for your current Medicare number & offer to send you a new card. Stay Alert. *Never* give your information to anyone who calls you on the phone or comes to your door!

Contact the Senior Medicare Patrol at The Western CT Area Agency on Aging at 1-800-994-9422 OR 203-757-5449 to report this. Help is always FREE and confidential.



HOW CAN YOU PREVENT THIS FROM HAPPENING TO YOU?

The purpose of all scams is the same: To obtain your personal information and to have access to your credit cards, bank accounts or investments, and / or health insurance.

Therefore, it is important that you

PROTECT yourself from Fraud, abuse and scams.

DETECT: Learn to detect potential fraud, abuse or scams.

REPORT: If you suspect that you have been a target of fraud, abuse or scams, always report it.

USEFUL TIPS:

Although anyone can be a victim of scams, here are some tips to avoid being one.

- Never provide your personal information by phone, email or online, unless you know the company or person, or it was you who initiated the contact. **REMEMBER**, Medicare, your bank, IRS or other legitimate companies will never ask for your personal information by phone, email or online.
- Treat your Medicare, Medicaid and Social Security numbers like a credit card number. Never give these numbers to a stranger. **REMEMBER**, Medicare doesn't call or visit to sell you anything
- Don't carry your Medicare or Medicaid card unless you will need it. Only take it to doctor's appointments, visits to your hospital or clinic, or trips to the pharmacy.
- Record doctor visits.
- Save Medicare Summary Notices and Part D Explanation of Benefits.
- Always review your Medicare Summary Notice (MSN) and Part D Explanation of Benefits (EOB) for mistakes. And compare

your MSN and EOB to your personal health care journal and prescription drug receipts to make sure they are correct.

- **Look for three things on your healthcare billing statement:**
 1. **Charges for something you didn't get.**
 2. **Billing for the same thing twice.**
 3. **Services that were not ordered by your doctor.**
- **Shred** the documents when they are no longer useful.
- **Never send money** to anyone unless you are sure that it is someone you know.
- Do not deposit a check you received in the mail unless you are sure you trust who the sender is.
- Do not fall into the trap of "Be Rich Faster." **if something sounds too good** to be true, it is probably a scam.
- Always check any phone number, email address or website asking for money or your personal information.
- **Do not respond** to emails from financial institutions or companies that ask you to verify your personal information.
- **Do not click on any internet link** that you receive by email, especially if it comes from someone you do not know.
- **Do not make charitable donations by phone.** Ask the caller to send you a printed form to make your donation.
- **Do not pay** any vendor or contractor who insists that you give or send money immediately prior to receive or initiate services.
- Make sure you are on a legitimate internet site before entering your personal information when shopping. **Look for the lock symbol** in the address block showing that the site is secure.
- Before signing a contract or buying an expensive product, consider talking it over with a relative, friend or lawyer you trust.
- **If you have questions** about information on your Medicare Summary Notice or Part D Explanation of Benefits, call your provider or plan first.

INFORMATION SOURCES:

- Federal Trade Commission
- Better Business Bureau
- Consumer Specialist, Federal Trade Commission
- Senior Medicare Patrol Navigator
- The Consumer Law Project for Elders
- Centers for Medicare and Medicaid Services (CMS)
- Office of Inspector General: US. Department of Health and Human Services.

WHO TO CONTACT IF YOU SUSPECT YOU ARE BEING A VICTIM OF HEALTHCARE FRAUD OR SCAM?

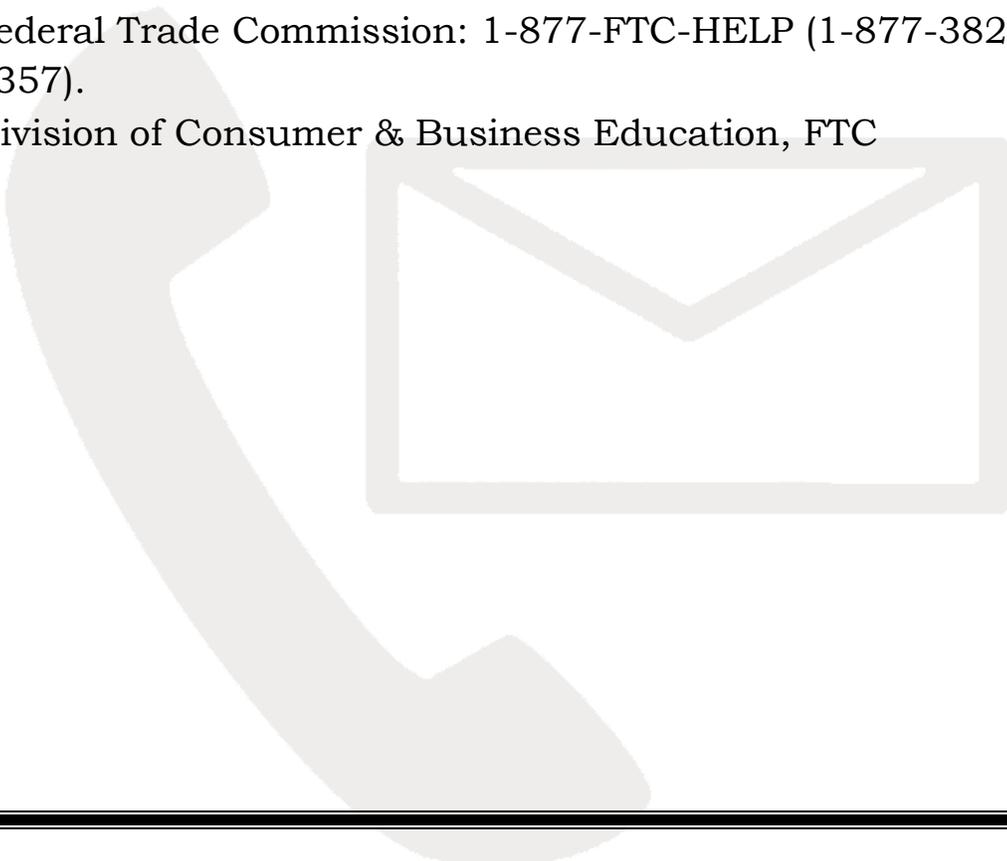
CT's Senior Medicare Patrol Program: 1800-994-9422 (Directed by the CHOICES program in your local Agency on Aging – Waterbury: 203-757-5449 EXT 160).

- Centers for Medicare & Medicaid Services:
Phone Number: 1800-633-4227
TTY: 1-800-486-2048
Postal Address: Medicare Beneficiary Contact Center
P.O. Box 39
Lawrence, KS 66044
- HHS Office of Inspector General
Phone Number: 1-800-477-8477
TTY: 1800-377-49-50
Website: <https://forms.oig.hhs.gov/hotlineoperations/report-fraud-form.aspx>
Postal Address: HHS Tips Hotline
P.O. Box 23489
Washington, DC 20026-3489

- U.S. Senate Special Committee on Aging-Fraud Hotline
Toll Free Number to report fraud: 1-855-303-9470
Website: www.aging.senate.gov/fraud-hotline
- Connecticut Attorney General's Office
Phone number: 860-808-5354
Fax: 860-808-5033
E-mail Address: ag.fraud@ct.gov
Postal Address: Office of the Attorney General
Antitrust and Government Program Fraud Department
Fraud Complaint
P.O. Box 120
Hartford, CT 06141-0120

**FOR ALL OTHER TYPES OF FRAUD OR SCAMS
CONTACT...**

- Local Police Department.
- The Consumer Law Project for Elders: 1800-296-1467.
- CT Department of Consumer Protection: 1800-842-2649.
- Better Business Bureau: 203-269-2700.
- Federal Trade Commission: 1-877-FTC-HELP (1-877-382-4357).
- Division of Consumer & Business Education, FTC



•

October 2017
Western CT Area Agency on Aging