Medicare Fraud

TexanPlus® HMO, TexanPlus® HMO-POS, TexanPlus® HMO-SNP, Today's Options® PFFS, or Today's Options® PPO (hereinafter, the Plan) has ways to fight Fraud, Waste and Abuse.

The Problem of Healthcare Fraud

The National Health Care Anti-Fraud Association (NHCAA) website reports that the United States spends more than $2.5 trillion on healthcare every year and estimates that tens of billions of dollars are lost to healthcare fraud, waste and abuse. Healthcare loss due to fraud, waste and abuse impacts patients, taxpayers and the government because it leads to higher healthcare costs, insurance premiums and taxes. Healthcare fraud often hurts patients who may receive unnecessary or unsafe healthcare procedures or who may be the victims of identity theft. Healthcare fraud is not a victimless crime and can have long lasting devastating effects.

What is Healthcare Fraud?

Healthcare fraud is knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any healthcare benefit program or to obtain (by means of false or fraudulent pretenses, representations, or promises) any of the money or property owned by, or under the custody or control of any healthcare benefit program. 18 U.S.C §1347

According to the NHCAA, whether you have health insurance through your employer or you purchase your own insurance policy, healthcare fraud causes higher premiums and out-of-pocket expenses for patients, and reduced benefits or coverage. For employers, healthcare fraud increases the cost of providing insurance benefits to their employees and increases the overall cost of healthcare.

Healthcare fraud also has a human face to it. These are people who may have been taken advantage of or subjected to unnecessary or dangerous medical procedures. A patient's medical records may be stolen and used to fraudulently bill insurance companies; this may affect a patient's medical history.

Examples of Healthcare Fraud

- A healthcare provider bills for medical services, supplies or items that were not provided.
- A healthcare provider bills for a more expensive service or procedure than what was actually provided or performed.
- A healthcare provider performs medically unnecessary services to obtain the insurance payment.
- A healthcare provider misrepresents a non-covered service as medically necessary to obtain the insurance payment.

- Falsifying a patient's diagnosis to justify tests, surgeries or other procedures that are not medically necessary.
- Accepting payment for medical referrals.
- A healthcare provider or pharmacy charges a beneficiary a price over the copay amount.
- A healthcare provider or pharmacy waives the patient's copay amount and overbills the insurance plan to recoup the cost.
- A pharmacy bills for prescriptions that were not dispensed.
- A pharmacy dispenses a generic drug, but bills for a brand-name drug.
- A pharmacy shorts prescriptions (e.g., billing for 60 tablets, but dispensing 30).
- A pharmacy adds unauthorized refills to prescriptions.
- A pharmacy, beneficiary, or policyholder forges or alters a prescription.
- A beneficiary or policyholder misrepresents personal information such as identity, eligibility, or medical condition in order to illegally receive a benefit.
- Someone steals or purchases a beneficiary's or policyholder's personal information to submit false or phantom claims to obtain the insurance benefit.
- A beneficiary or policyholder allows somebody else to use his or her health benefits to obtain medication and/or medical services.
- Somebody pretends to represent Medicare, the Social Security Administration, or an insurance plan for the purpose of obtaining personal and/or financial information.

Phishing Schemes for Bank Information and Identity Theft

The Plan CANNOT ask for member identification numbers (e.g. bank account numbers, credit card number, Health Insurance Claim Number "HICN") EXCEPT as required to verify membership, determine enrollment eligibility or process an enrollment request). The Plan will NEVER ask for your social security number.

Phishing is a type of theft used by fraudsters to lure people into a false sense of security with the intent to steal a person's private information by phone calls, emails or copy-cat websites. Identity theft happens when someone steals a person's information and uses it without his or her permission or knowledge. Medical identity thieves may use a person's name and personal information such as his or her health insurance number to make doctor's appointments, obtain prescription drugs, and file claims with his or her insurance company. This may affect the person's health and medical information and can potentially lead to misdiagnosis, unnecessary treatments, or incorrect prescription of medication. There are many ways an identity thief can obtain a person's health information, such as: paying for it, offering free services, supplying food or gifts, or providing free "health screenings."

Protect Yourself Against Fraud

- Treat your Medicare card, Social Security card, and insurance ID card like you would your most valuable possessions so that it doesn't fall into the wrong hands.

- Review your Explanation of Benefits (EOB) when you receive it in the mail. Look for:
    - Charges for services, drugs, equipment, and/or supplies you did not get
    - Billing for the same service, drug, equipment, and/or supplies twice
    - Services that were not ordered by your doctor
- Do not give out personal information over the phone or through mail unless you have initiated the contact or are communicating directly to your insurance company.
- Be cautious of providers who offer "free" testing or screening but require your Medicare and/or insurance card first. This may be a scam to get your personal information.
- Avoid using a healthcare provider or pharmacy who tells you that the item or service is not usually covered, but they know how to bill Medicare to get it paid for.

Our Commitment

The Plan is committed to fighting healthcare fraud, waste, and abuse.

We have a dedicated Special Investigations Unit (SIU) whose mission is to protect our, members, providers, employees, other related parties, and the Medicare Trust Fund by administering a plan to prevent and detect fraud, waste, and abuse.

The SIU works to investigate all allegations, correct offenses, recover lost funds, and partner with Federal and state agencies to prosecute violators to the fullest extent of the law.

Help Fight Fraud

Here are some simple measures to protect yourself and helping the fight against healthcare fraud:

- Report all suspicious acts regarding your healthcare, and call your insurance plan immediately. The SIU will investigate all allegations and complaints.
- Maintain good records of all your medical care and closely review the medical bills you receive.
- Read and carefully examine your Explanation of Benefits (EOB), healthcare policy, and any paperwork you receive from your insurance company.

If you suspect someone of committing insurance fraud against the Plan or think you may be a victim, please report immediately the suspicious activity to the SIU:

By Phone: Fraud, Waste, and Abuse Hotline - 1-800-388-1563
By Email: fraud@UniversalAmerican.com

In writing:
Universal American SIU
PO Box 17008
Austin, TX 78760-7008

All communications are confidential and may be anonymous.

TexanPlus® HMO, TexanPlus® HMO-POS, Today's Options® PPO and Today's Options® PFFS are Medicare Advantage plans with a Medicare contract. Enrollment in these plans depends on contract renewal. A Private Fee-for-Service plan is not Medicare supplement insurance. Providers who do not contract with our plan are not required to see you except in an emergency. TexanPlus® HMO-SNP is a Medicare Advantage plan with a Medicare contract and a contract with the State Medicaid Program. Enrollment in TexanPlus® HMO-SNP depends on contract renewal. This plan is available to anyone who has both Medical Assistance from the State and Medicare.