Misinformation runs rampant in the health care industry. And while some types of misinformation are found on social media platforms and are more opinions than facts, there is also the type of misinformation that aims to exploit seniors.

“Unfortunately, seniors are prime targets for misinformation as it pertains to Medicare and Medicare Advantage,” advised Darragh O’Carroll, M.D., medical director at naviHealth. “It is important that seniors are able to know the difference between the facts and the misinformation being provided by potential scams and know where to go if they have questions. Providers and caregivers must stay a vigilant trusted adviser.”

The number one piece of advice that Dr. O’Carroll advises for providers is to recognize that seniors are a more vulnerable population to misinformation and scams and that they need to be extra diligent when it comes to discussing medical information, personal information or benefits with other parties.

Medicare scams can take many forms including communication over the phone, email, text or even in the mail. Scammers will try to leverage personal information about an individual to then gather even more information. This can look like an effort to verify an identity, offer medical supplies or even offer a refund. At the end of the day, scammers are only seeking enough personal information to file bogus Medicare claims under beneficiaries’ accounts.

Here is some information that providers can share with their senior patients to lower their chance of being involved in a scam:

1. **Be wary** — Dr. O’Carroll advises that the best thing that seniors can do to protect themselves from misinformation or scams is to be mindful of suspicious callers, texts, emails and mailers. Scammers may seem very empathetic and knowledgeable and may even have some personal information on hand like mailing address, full name and birthdates to make them look and sound legitimate. Seniors must always be wary of phone numbers that they don’t recognize or someone reaching out with information that they didn’t ask for. The Centers for Medicare & Medicaid Services (CMS) will generally not call beneficiaries unless a call back from 1-800-MEDICARE was requested or the beneficiary receives an official letter requesting a phone interview. CMS will never call to sell a product or service. Additionally, Medicare cards do not expire, so calls requesting an update to existing cards are typically fraudulent.
2. **Don’t give out personal information** – Always be sure to protect personal information such as social security numbers or CMS beneficiary numbers located on member identification. Generally, if someone is asking for personal information, individuals should not share it over the phone or email. Medicare advises that

beneficiaries should only give out private information to individuals who they know and trust including doctors, insurers acting on their behalf, insurance providers, and State Health Insurance Assistance Program (SHIP) counselors.

3. **Don't believe everything online** — When looking for Medicare or even medical information, Dr. O'Carroll advises to always rely on reputable websites like the Medicare website or the CDC website. As a rule of thumb, rely on information from websites that end in .gov instead of .com.
4. **Rely on trusted sources —** At the end of the day, if a patient has medical questions or questions about their Medicare benefits, they should rely on trusted advisors and check with their doctor, advisors at Medicare or local State Health Insurance counselors. If a person notices any charges that are unfamiliar, be sure to alert CMS right away.

Being aware that scammers are seeking personal information and will leverage Medicare to do so is half the battle. Knowing how to protect your patients is just as important.