Protect yourself against spam calls

How to Identify and Handle Spam Calls

- **Never give out personal information** such as Social Security numbers, credit card details, or bank information over the phone, especially if you did not initiate the call.
- **Hang up immediately** if a caller pressures you to act fast, asks for immediate payment for a bill you haven't seen, or demands payment via gift cards or wire transfers.
- **Be suspicious of "Caller ID spoofing,"** where the number appears to be from a local hospital or clinic. Scammers use this tactic to build false trust.
- **If you doubt a call is legitimate, hang up and call back using a trusted, official phone number** found on an account statement, the back of your insurance card, or the official website of the organization.
- **Do not answer calls from unknown numbers**. If you do answer a suspicious call, hang up right away and do not respond to any prompts, even by saying "yes".

What Real Healthcare Providers Do and Don't Do

- **Real providers will not demand immediate payment** over the phone.
- When a legitimate representative calls, they will clearly identify themselves and provide a way for you to verify their identity and the call's purpose.
- **Legitimate calls may include appointment reminders or lab results**, which are exempt from certain robocall prohibitions, but these calls still follow strict protocols and do not ask for sensitive financial data.

How to Protect Yourself and Report Scams

- **Register your phone number** on the official National Do Not Call Registry at no cost.
- **Use call-blocking services** offered by your phone carrier or a third-party app.
- **Report scam calls** to federal authorities to help them track and stop these criminals.
    - File a complaint with the Federal Trade Commission (FTC).
    - Report Medicare-related fraud to Medicare.
    - File a complaint with the Federal Communications Commission (FCC) if the call violates robocall rules.