Vishing Awareness

Tips to identify phone call scams

Team members or providers occasionally receive reports from patients and health plan members of individuals calling and pretending to be from our organization.

These calls are a scam, called "vishing." The caller will use flattery and threats to pressure individuals into giving them information, money and even access to personal devices. These fake phone calls can even "spoof" caller ID and appear to be from a phone number within our organization.

Follow these tips when you are uncertain of the identity of the caller:

Do not share account passwords or temporary verification codes with anyone. The organization will never ask you for this information when you need support.

Do not provide personal information such as birthdate, social security number or home address.

Do not confirm your employment or your personal information.

Do not give out any financial information.

Ask for the name of the person calling and a number to call back. Scammers won't provide a valid number that would allow you to call back.

If you receive a vishing call, you should report it to the **FTC Consumer Complaint Center** as an Unwanted Call Complaint. Also, if you think you may have mistakenly given out health record information, click here, **Protect yourself from phone scams** for more information as soon as possible.

9-22-22