Telehealth Safety Checklist

This checklist will help patients and providers prepare for safe telehealth sessions. Review each step before your appointment to protect your privacy, ensure quality of care, and stay compliant with security best practices.

- Use a secure, private location for your telehealth session (avoid public spaces).
- Ensure your device (phone, tablet, computer) has up-to-date software and security patches.
- Connect only through a secure WiFi network (avoid public WiFi); consider using a VPN.
- Confirm the telehealth platform is HIPAA-compliant and uses encryption.
- Use strong, unique passwords for telehealth apps or patient portals.
- Ask your provider whether the session will be recorded, and give consent only if comfortable.
- Have headphones available to protect privacy and reduce background noise.
- Close other apps or programs to avoid interruptions and minimize data sharing.
- Verify your provider’s identity before sharing sensitive health information.
- Keep emergency contact numbers handy in case technology fails during a critical situation.
- Know when in-person care is necessary (e.g., chest pain, breathing difficulty, stroke symptoms).
- Ask how your health data will be stored, who has access, and how long it will be retained.
- Providers: Train staff on privacy, consent, and telehealth best practices.
- Providers: Run regular risk assessments and audits of telehealth platforms.
- Providers: Establish protocols for switching to in-person visits when telehealth is insufficient.