Telehealth Privacy Tips

For UConn Health Patients and Providers

Patients

- Hold healthcare-related conversations and calls in a private space.
- Enable and use two-factor authentication when possible for logging on to those systems that hold your healthcare information, including MyChart.
- Avoid using unsecured public internet networks, such as those at an airport or coffee shop.
- Unlink, or log out of, social media applications on the device used for the call.
- Disconnect security cameras and smart speakers to avoid unintended capture of sensitive information.

- Keep anti-virus and malware software up to date on electronic devices.
- Run system updates and patches for your electronic devices.
- Use secure, encrypted methods to communicate with your providers, such as MyChart.

Video visits with most UConn Health providers are conducted within MyChart and utilize a HIPAA-compliant version of Zoom.

Providers

- Obtain and document the patient's consent to telehealth.
- Confirm the patient's location, e.g., home.
- Verify the identity of the patient and anyone else present in the audio or visual session before discussing healthcare information.
- Notify patients about how they will be contacted about telehealth visits.
- Integrate all notes from a telehealth session in the patient's chart.
- Use only those secure platforms approved by UConn Health, and use only UConn Health issued or approved devices, including laptops and cellphones.

Questions?

Contact the Office of Healthcare Compliance & Privacy
x6060 or ohcp@uchc.edu