Telehealth Privacy Tips for Patients

Understand your privacy and security risks when it comes to the collection, sharing, and storage of your data.

What are your rights when it comes to data privacy?

- [ ] Providers are increasingly able to collect your health data through advancements in telehealth and related health technologies.
- [ ] You have the right to maintain privacy over your protected health information.
- [ ] You have the right to know how your health data is being stored. Your health data cannot be shared with third parties, such as employers or for marketing purposes. Learn more about the Health Insurance Portability and Accountability Act (HIPAA).
- [ ] Providers are responsible for using HIPAA compliant telehealth platforms which have safeguards to prevent unauthorized users from accessing your health information and payment methods. Safeguards include firewall, encryption, and two-step authentication, among others.

How can you protect your privacy during a telehealth visit?

- [ ] Avoid scheduling a telehealth visit in a busy area, over a public Wi-Fi network, and on a platform that did not require a password along with other forms of authentication, such as a code sent to your cell phone.
- [ ] Limit communications about health information over unencrypted email or other text messaging services.

What can you do to maintain your data privacy?

- [ ] Remove or secure any transmitted data during a telehealth session from your personal computer or mobile device.
- [ ] Limit privacy risk associated with social media connections on your computer or mobile device, such as inadvertent linking to social media accounts.
- [ ] Let your provider(s) or health insurance companies know if there is health information you do not wish to share with certain people, groups, companies, or other third parties.

These steps reduce risk of your identifiable information, such as name, social security number, email address, and phone number, from being shared.