Telehealth Privacy Tips for Providers

What are the data privacy and security risks in telehealth?

- ☐ **Privacy risk** is when an individual lacks control over the collection, use, and sharing of their health data.
- ☐ **Security risk** is when there is unauthorized access to an individual's health data during the collection, transmission, or storage.
- ☐ These risks can affect trust between the patient and provider and contribute negatively to adherence and continuity of care.

How do I fulfill privacy obligations during a telehealth session?

- ☐ **Privacy and security risks** are present for in-person, remote monitoring, and virtual visits. Electronic transmission of data means greater privacy and security risks.
- ☐ Make sure you are up-to-date on security and protections requirements for HIPAA compliance and are aware of other legal considerations.
- ☐ Providers have an **ethical obligation** to discuss privacy and security risks. These discussions can be part of a patient-centered care plan to help ensure confidentiality.

How do I communicate privacy protections to patients?

- ☐ Make privacy part of the workflow by confirming identities of everyone present at each telehealth session and communicate how any third-parties may be involved.
- ☐ **Set up and communicate the below safeguards to your patients:**
  - Create unique user identification numbers
  - Use password protected platforms
  - Establish automatic logoff

How do I protect my own privacy and reduce risk of breaches?

- ☐ Health data breaches are costly and can involve investigations, notifying patients, and recovering data, so providers need to be familiar with their security features.
- ☐ **Establish the below processes:**
  - Routinely review your telehealth privacy and security policies.
  - Schedule regular deletion of files on mobile devices.
  - Utilize data back-up and recovery processes in case of breach.
- ☐ Conduct a **security evaluation** from an independent party on your telehealth system to verify security features such as authentication, encryption, authorization, and data management.
- ☐ Check out more security tips from the Office of the National Coordinator for Health Information Technology.