Security Best Practices for Member and PA Download Files

Some of the best security practices for Member and PA Download Files are as follows:

- **Make it harder for people to get access to data on your computer**,
  - Choose a good password that is not easily guessable for your computer (8 or more characters, complex, changes every 90 days)
  - Don’t share your password with others.
  - Don’t leave your device unattended.
- **Encryption is a must-have,**
  - Use hard drive encryption.
  - Don’t use removeable media (thumb drives, portable drives, etc.)
- **Limit sharing to authorized individuals,**
  - Emailing data set is not recommended.
  - Screen sharing/remote sessions are not recommended for these reports.
  - Saving in shared locations (cloud-hosted storage, network drives) is not recommended for these reports.
- **Properly dispose of devices/media,**
  - Deletion of files does not remove the data from hard drives.
  - Devices should be properly scrubbed or destroyed using specific tools/processes before decommissioning, recycling, or disposal of the device.
  - Get a certificate of destruction if you use a 3rd party to dispose of hard drives/computers.

If you have additional questions, please contact Therap at kysupport@therapservices.net