|  |  |
| --- | --- |
|  | BW300%20_smallcopyWFNJ SAI/BHI and FVO |

 MEMO

**To**: All CCS Staff

**From:** Stacey Wolff

**CC:** Lisa Griffith, Rob Hightower, Laura Abramowitz

**Date:** January 10, 2018

**Re:** POLICY UPDATE: Storage of ePHI

In an effort to maintain strong management and governance around electronic protected health information (ePHI) under HITECH, HIPAA and CFR 42, Part 2, NCADD-NJ has implemented policies and procedures for the management and storage of ePHI.

Maintaining the privacy and security of client information is critical in treating individual identifiable heath responsibly and in accordance with the provisions of HIPAA, HITECH, and other state and federal

requirements.

**Storage of ePHI on PCs/Laptops:**

Any identifiable electronic client information should never be stored in files or file directories on your laptop/PC hard drives. You are required to delete all downloaded reports, and empty the recycle bin, of any client data that has been saved from the database as soon as you have printed the necessary information or completed the tasks for which the information was required. All ePHI must be destroyed (electronic or hard copy) once you have performed the necessary tasks requiring the client data.

**Storage of ePHI in Email:**

Any identifiable electronic client information and emails containing ePHI should never be stored in inboxes, file directories on your laptop/PC hard drives, USB/flash drives, CD/DVDS, or other external hard drives.

Emails sent or received on your computer or smart phones should never contain ePHI data. If any identifiable and confidential client information is received in an email, it should be removed immediately. Storage of ePHI in emails on your laptop/PC or smart phones is strongly discouraged.

Emails sent containing protected health information must be password protected, with the access password sent to the recipient in a secondary email. Contact it@ncaddnj.org for instructions on this process.

**Small storage devices:**

No ePHI should be stored or transferred on external storage devices such as USB/flash drives, CD/DVDS, or other external hard drives. Encrypted thumb drives and external hard drives are also not recommended and strongly discouraged for storing or transferring any confidential files.