DAVIS BEHAVIORAL HEALTH
Community · Commitment · Change

Policies & Procedures

HMIS SECURITY PRACTICES

Section: Administrative Policies

Pages: 2

Subject: HMIS Security Practices

Effective Date: 04/01/2021

Revision Date:

PURPOSE

This policy with accompanying procedures set forth standards for employees using the HMIS within Davis Behavioral Health.

POLICY

DBH will follow the physical and technical safeguards suggested by UHMIS

PROCEDURE

Physical Safeguards

The HMIS lead agency and CHOs will take all reasonable, foreseeable, and protective actions to physically secure the PPI of clients. These actions are listed below but do not represent an exhaustive list of physical safeguards.

1. To secure protected personal information when transmitting written communication about clients, all users will use the ClientID to refer to the client.
2. Hard copies of client information or reports with protected personal information will be kept in a locked cabinet or storage area when unattended.
3. Loose papers or notes with client information not stored in the clients file will be securely destroyed.
4. The lead organization and CHOs will minimize the visibility of computer/tablet/phone screens used to limit HMIS access to unauthorized individuals.
5. Documents that contain passwords will be kept physically secure.

6. The servers that house UHMIS information will be kept in a secured and monitored facility.

Technical Safeguards

The HMIS lead agency and CHOs will take all reasonable, foreseeable and protective actions to technically secure the protected personal information of clients. These actions are listed below but do not represent an exhaustive list of technical safeguards.

1. Users will change their passwords at least once annually.
2. Terminals used to access HMIS will have locking screen savers and will be password protected.
3. Users will not leave UHMIS open and running when terminal is unattended.
4. Users will be automatically logged off after 30 or less minutes of inactivity.
5. Electronic Documents stored outside of a private protected local network that contain protected personal information must be password protected.
6. All computers accessing HMIS must have regularly updated anti-virus software installed that automatically scans files.

Data Disposal

1. The HMIS Lead will annually review PPI associated with clients for data no longer in use. Client records will be maintained on the HMIS system for a period of seven years from its last modification date after which, PPI will be removed, and the remaining information shall be stored in a de-identified format.