Privacy & Security

Potential risks of HMIS, like any system for managing data about individuals, include risks to personal privacy. Before being able to use the system, agencies and end-users within agencies must sign User's Agreements indicating that they will uphold data privacy standards. Please review the End-User's agreement and signed prior to use HMIS system.

HMIS Computer Requirements/ Workstation Security

- Do not share your Account Data security goes beyond your computer.
- You need to ensure that the PPI that is gathered and input into the HMIS is secured.
- Each HMIS user is also required to submit a signed receipt of the HMIS User Agreement prior to system access.
- Passwords are only known by the individuals, which are not even known by the HMIS Administrator Agency or Lead Agency. Everything in the system is tracked and may be audited. You, as the user, are solely responsible for what happens under your account.

Download of client data on home computers

If completing work at home/approved remote locations, plan for the process, control/restrict downloads, and ensure hard drives are properly cleaned.

Application Security

The following standards must be observed when working with the HMIS system in Clarity:

- Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location.
- You may not log on to more than one workstation at a time.
- You may not log on to the network at more than one location at a time.
- Workstation Security Access to the HMIS system in Clarity must always be secured.
- Computers in public areas used to collect and store HMIS data must always be staffed.
- When workstations are not in use and staff is not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals.
- After a short period of time, workstations should automatically turn on a password protected screensaver when the workstation is temporarily not in use.
- If staff will be gone for an extended period, staff should log off the data entry system and computer.
- Written information pertaining to user access should not be stored or displayed in any publicly accessible location.
- Lock Workstation Anytime you leave your workstation unattended, for any amount of time, LOCK YOUR WORKSTATION.

- Password-Protected Screensaver Password-protected screensavers should be set to activate within 5 to 8 minutes when the workstation is not in use.
- Only use Unique Identifier in the email, do not use client identifying information such as name or SSN
- Passwords must be changed after every 60 days
- 5 consecutive unsuccessful attempts to login will disable the user ID until account is re activated by system administrator
- If you will be gone from your workstation for 30 minutes or more, log-off Clarity.
- If you will be gone from your workstation for 4 hours or more, log-off your computer.

Disposing of Confidential Client Information Printing and Disposing of Hard Copy Data

- Hard copy data containing Personal Protected Information (PPI) may only be printed from the HMIS system attached to the physical agency/jurisdiction location(s) and only on printers secured from public access.
- An agency/jurisdiction is responsible for disposing of documents that contain PPI by shredding paper records.