2024 HMIS User Policy

Each authorized HMIS user will be issued a unique user ID and provided instruction on creating a unique and private password. Sharing of passwords and user IDs is expressly forbidden. HMIS users must take all reasonable precautions to ensure that his/her password is physically and digitally secure. Each authorized HMIS user will attend an HMIS New User training and successfully complete a basic HMIS skills evaluation prior to being granted access to their agency's program data.

HMIS users have an obligation to maintain client privacy and to protect and safeguard the confidentiality of each client's protected personal information (PPI). PPI shall include, but is not limited to, the client's name, address, telephone number, social security number, date of birth, type of care provided, medical condition or diagnosis, veteran status, employment information, and all other information relating to the services provided to the client by any agency. Only authorized HMIS users and the client about whom the information pertains may view a client's information in the HMIS. HMIS users must never discuss PPI with anyone in a public area. Information in the HMIS may only be viewed, obtained, disclosed, or otherwise used to enable the authorized HMIS user to successfully perform their job.

If client information from the HMIS must be saved in a digital format, then such information must be saved in a secure folder or drive that is accessible only to authorized HMIS users. Hard copies of HMIS data must be kept in a secure file and must not be left in public view. All digital and hard copies of HMIS data will be destroyed when no longer needed.

All authorized HMIS users must log off of the HMIS prior to leaving the work area where the computer is located. A computer that has the HMIS "open and running" shall never be left unattended for any length of time. Failure to log off of the HMIS appropriately may result in a breach of client-confidentiality and system security. Authorized HMIS users who notice or suspect a security breach must immediately notify the Participating Agency HMIS Administrator.

Minimum Data Entry

HUD's HMIS Data Standards set forth specific requirements related to client- and program-level data collection and entry in the HMIS. Universal Data Elements must be entered in the HMIS for all persons served, including rostered clients and household members. While the Universal Data Elements are required in accordance with HUD's HMIS Data Standards, entering this information into the HMIS accurately and in a timely manner allows agencies to generate the HUD APR and other reports quickly and with ease.

Recommended Data Entry

The HMIS is a tool to assist agencies in focusing services and locating alternative resources to help homeless persons. Therefore, agency staff should use the client information in the system to target services to the client's needs. Data which may prove to be useful toward this end include:

- Client progress notes
- Client goals and outcomes
- Supportive and financial services provided
- Referrals

Other data, when entered into the HMIS and reported to a CoC in the aggregate, assist the CoC in applying for and receiving both renewal and new funding from HUD. Such data include:

- Agency program information
- Bed utilization and quarterly occupancy rates
- Data necessary for the annual point-in-time (PIT) homeless count

2024 HMIS User Agreement

Name: _____

HMIS Participating Agency: _____

HMIS participating agencies and each authorized user within any HMIS participating agency are bound by various restrictions regarding Protected Personal Information ("PPI"). The employee, contractor, or volunteer whose name appears above is the **User**.

Your user ID and password give you access to the LI HMIS. Initial each item below to indicate your understanding and acceptance of the proper use of your user ID and password. Failure to uphold the confidentiality standards set forth below is grounds for immediate suspension or termination of your access to the HMIS.

_____ *Initial* I understand that I have an obligation to maintain client privacy and to protect and safeguard the confidentiality of a client's PPI. PPI shall include, but is not limited to, the client's name, address, telephone number, social security number, date of birth, type of care provided, medical condition or diagnosis, veteran status, employment information, and all other information relating to the services provided to the client by me and other agencies.

_____ *Initial* My login information is for my use only and must not be shared with anyone.

_____ *Initial* I must take all-reasonable precautions to keep my password physically secure.

_____ *Initial* I understand that the only individuals who can view information in the HMIS are authorized users and the clients about whom the information pertains.

_____ *Initial* If I must save client information from HMIS in a digital format, I agree to save such files and information in a secure folder or drive that is only accessible to me. Such files will be destroyed when no longer needed.

_____ *Initial* I may only view, obtain, disclose, or use the database information that is necessary to perform my job.

_____ *Initial* If I am logged into the HMIS and must leave the work area where the computer is located, I **must log-off** of the HMIS before leaving the work area.

_____ *Initial* A computer that has the HMIS “open and running” shall never be left unattended for any period of time.

_____ *Initial* I will not discuss PPI with anyone in a public area.

2024 HMIS User Agreement

_____ *Initial* Failure to log out of the HMIS appropriately may result in a breach in client confidentiality and system security.

_____ *Initial* Hard copies of HMIS data must be kept in a secure file. I will not leave hard copies in public view, on my desk, or on a photocopier, printer or fax machine.

_____ *Initial* When hard copies of HMIS data are no longer needed, they must be properly destroyed to maintain confidentiality, i.e. shredded or otherwise rendered unreadable.

_____ *Initial* If I notice or suspect a security breach, I must immediately notify the Participating Agency HMIS Administrator.

_____ *Initial* If I DO NOT log into the HMIS system for 90 days or more my login will be disabled by the Participating Agency HMIS Administrator. To regain HMIS access the disabled user must attend New User/Refresher training session.

HMIS User Code of Ethics

A. HMIS users must treat all HMIS participating agencies with respect, fairness and good faith.

B. Each HMIS user should maintain high standards of professional conduct in their capacity as an HMIS user.

C. HMIS users have the responsibility to relate to the clients of all HMIS participating agencies with full professional consideration.

By signing below, you are indicating that you understand and agree to comply with all requirements set forth in the HMIS User Policy, HMIS User Responsibilities and HMIS User Code of Ethics.

_____ _____

HMIS User Signature Date

_____ _____

Participating Agency HMIS Administrator Signature Date

_____ _____

HMIS Participating Agency Executive Director or CEO Signature Date