City of Philadelphia
Division of Social Services
Office of Supportive Housing

Homeless Management Information System
User Agreement

This agreement between the City of Philadelphia (City) and the undersigned user of its Homeless Management Information System (HMIS) specifies policies, rights and responsibilities, and ethical guidelines with regard to the use of the HMIS.

I. Background

The City's Office of Supportive Housing (OSH) is the entity designated by the US Department of Housing and Urban Development (HUD) as the administrator of Philadelphia's Continuum of Care (CoC)-wide HMIS. Entities using this HMIS currently include OSH and the agencies and organizations within the CoC. In accordance with HUD directives, HMIS participation will continue to expand to include additional agencies and organizations within the Philadelphia CoC.

II. Training

Any individual who has not received OSH-approved training on how to properly use the system should not use the HMIS. All HMIS users will therefore be required to complete HMIS training prior to using the system. Any OSH user who feels he or she needs refresher training should contact their supervisor. Non-OSH employees should contact the HMIS Site Administrator from their organization.

III. User Identifications Codes and Passwords

Upon successful completion of training and signing of this HMIS User Agreement, and subject to approval by the City, each HMIS user will be provided with a unique personal User Identification Code (User ID) and initial password to access the HMIS.

While the User ID provided will not change, HUD standards require that the initial password only be valid for the user's first access to the HMIS. Upon access with the initial password, the user will see a screen that will prompt the user to change the initial password to a personal password created by the user.

A. Only the user will know the personal password he or she creates. It is the user's responsibility to remember the password.

B. The password may not be stored in a publicly accessible location and written information pertaining to the User ID, password, or how to access the HMIS may not be displayed in any publicly accessible location.

C. The user is not permitted to divulge this password or to share this password with anyone.

IV. Security, Privacy, and Confidentiality of Client Data

The HMIS contains a range of Personal Protected Information (PPI) on clients and all such information must be treated carefully and professionally by all who access it. According to HUD, PPI is defined as "any information maintained by a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual." A Covered Homeless Organization (CHO) is defined as "any organization (including its employees, volunteers, affiliates, and associates) that records, uses or processes PPI on homeless clients for an HMIS." HMIS users are therefore subject to the following guidelines regarding the security, privacy, and confidentiality of client PPI.

A. The only individuals who may view or receive data from the HMIS are authorized users of the HMIS, users of other City databases for which clients have granted explicit informed consent to share data, and the individual clients to whom the data pertains. The User ID and password assigned to each individual HMIS user is to be used only for his or her access to the HMIS. An HMIS user may not allow access to the HMIS with his or her User ID and password to any other individual, regardless of whether or not the individual is an authorized HMIS user or whether or not the individual has the same job role or the same level of access rights.

B. Each HMIS user may only view, obtain, extract, or use the data from the HMIS that is necessary to perform his or her job. Each HMIS user may only operate the HMIS using the Job Roles assigned to him or her.

C. Failure to properly log off the HMIS may result in a breach of system security and the privacy of client data. A computer that has the HMIS application open must therefore never be left unattended. Every computer that is used to access the HMIS must have a password-protected screen saver that automatically turns on when the computer is temporarily not in use. If an HMIS user will be away from the computer for an extended period of time, he or she is required to log off from the HMIS before leaving the work area in which the computer is located.

D. The guidelines regarding the security of paper or other hard copy containing PPI that is either generated by or for the HMIS, including, but not limited to reports, data entry forms, and signed consent forms are:

1. A CHO must supervise at all times any paper or other hard copy generated by or for the HMIS that contains PPI when the hard copy is in a public area.
2. When CHO staff is not present, the information must be secured in areas that are not publicly accessible.
3. Written information specifically pertaining to user access (e.g., User ID and password) must not be stored or displayed in any publicly accessible location.

E. Information obtained by the HMIS user from the HMIS is to remain confidential even after the HMIS user's relationship with the City and/or the participating agency that employs him or her changes or concludes for any reason.

VI. Data Quality Control

A. To the extent that clients and other agencies supplying information have provided accurate data, HMIS users are responsible for the accuracy of the data they enter into the HMIS.

B. HMIS users are required to enter data into the HMIS in a timely manner and in accordance with OSH performance standards and with any existing applicable agreements between OSH and its provider agencies.

VII. Problems with the HMIS

An HMIS user employed by a provider agency encountering a problem using the HMIS should contact his or her supervisor(s) and the HMIS Site Administrator from their organization. If the HMIS Site Administrator is not able to answer the question or solve the problem, he or she will contact the OSH Information Technology Helpdesk at 215-686-7110 or HMIS@phila.gov. An OSH HMIS user encountering a problem using the HMIS should contact his or her supervisor(s) and the OSH Information Technology Helpdesk at 215-686-7110 or HMIS@phila.gov.

I affirm that I have read this Homeless Management Information System (HMIS) User Agreement and received training on how to use the HMIS. I agree that I will use the HMIS only for its intended use and in accordance with the training and access rights I have received. If I believe a security breach has occurred, I will notify the OSH Information Technology Helpdesk at 215-686-7110 or HMIS@phila.gov or the HMIS Site Administrator of the provider agency that employs me. I understand and agree to comply with the terms of this agreement.

My failure to uphold terms of this agreement may result in progressive disciplinary action, up to and including termination of my employment. There is no expiration date of this agreement.

HMIS User Signature **Date**

HMIS User Printed Name **Date**

HMIS Site Administrator or User's Supervisor **Date**

HMIS Site Administrator or User's Supervisor Printed Name **Date**