I. HOMELESS MANAGEMENT INFORMATION SYSTEM STANDARDS

Emergency Housing service providers are required to input client data into the City's Homeless Management Information System (HMIS). The following sections describe basic expectations regarding providers' use of the HMIS. Where applicable, reference is made to additional documents that provide greater detail regarding specific HMIS requirements.

Site Administrator

Providers are required to designate one or more staff persons to serve as HMIS Site Administrator(s). The HMIS Site Administrator is responsible for ensuring that the provider complies with the technology standards required to operate the HMIS. The HMIS Site Administrator also serves as the first-level responder for any of the provider staff's HMIS-related technical issues and is responsible for carrying out specific HMIS system administration tasks. The HMIS Site Administrator duties and HMIS technical requirements are outlined in the document "HMIS Site Administrator Manual," which is appended to the Emergency Housing Standards.

All provider staff persons that use the HMIS are required to complete HMIS training for their assigned job roles prior to using the system. Since OSH employs a train-the-trainer approach to HMIS training, the HMIS Site Administrator is required to designate one or more staff persons to serve as HMIS Site Trainer(s). The HMIS Site Trainers will receive training in specific HMIS functions from OSH or its designees and are responsible for in turn training provider staff.

Security

All computers from which the HMIS is accessed must be in a physically secure location.

Providers must apply system security provisions to all systems involved in accessing the HMIS including, but not limited to, networks, laptops, desktops, mini-computers, mainframes and servers. Such provisions must include user authentication, virus protection, public access, physical access and disaster protection and recovery.

Computers stationed in public areas that are used to collect and store HMIS data must be staffed at all times. When workstations are not in use and staff persons are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals.

After a short amount of time, workstations should automatically turn on a password-protected screen saver when the workstation is temporarily not in use. (Password-protected screen savers are a standard feature with most operating systems.) If staff will be gone for an extended period of time, staff should log off the data entry system and shut down the computer.

All HMIS users are required to accept the terms and conditions of the "Homeless Management Information System User Agreement" each time prior to logging into the system. This document addresses such issues as IDs and passwords, system security, proper use of the system, and preventing the theft of information and is appended to the Emergency Housing Standards.

Privacy

All providers are required to comply with privacy standards regarding the collection, maintenance and use of protected personal information recorded, used, or processed for the HMIS. These requirements are detailed in the document "Office of Supportive Housing Notice of Privacy Practices for Use with the Homeless Management Information System (HMIS)" which is appended to the Emergency Housing Standards. The privacy standards include, but are not limited to, the following:

- Posting a sign clearly visible to clients at all stations where HMIS users meet with clients to enter client data into the HMIS that informs of the existence of OSH's HMIS Notice of Privacy Practices and that states that the document is available upon request and making it available upon such request by any individual. (OSH's sign is the document "Notice of Privacy Practice" and is appended to the Emergency Housing Standards.)
- Allowing any individual who provided protected personal information to inspect and receive a copy of the information collected about that individual in the HMIS.
- Allowing any individual to submit questions or complaints about OSH's privacy and security policies and practices.
- Securing any paper or other hard copy containing protected personal information that is either generated by or for HMIS, including, but not limited to, reports, data entry forms and signed consent forms.

Client Attendance

Providers are required to manage and report their emergency housing attendance through HMIS. Providers must submit their HMIS Attendance by 10 a.m. on a daily basis, Monday through Sunday. When applicable, HMIS Attendance Problems Reports must be submitted by 10 a.m. on a daily basis, Monday through Sunday.

Providers must complete the HMIS Attendance Problems Report when one of the following occurs:

- The provider is unable to submit the attendance via HMIS because of technical and/or connectivity issues. Once the technical and/or connectivity issue is resolved, the provider must submit the attendance via HMIS for all past-due dates.
- The provider is unable to include all "attended" clients on the submitted HMIS Attendance. Providers are responsible for ensuring that clients listed on the HMIS Attendance Problem Reports receive an active POS and adjust the clients' attendance for the relevant time period.

It is important that providers meet all client attendance reporting requirements because the OSH Fiscal Management Unit relies solely on the data found within HMIS to validate monthly invoices.

Purchase of Service (POS)

Providers must proactively manage each client's POS within HMIS by:

- Tracking client POSs through the HMIS POS Reminder Screen;
- Extending and closing all case-managed POSs on a consistent and timely basis;
- Collaborating with OSH Intake Staff to ensure intake-supported POSs are extended and closed appropriately;
- Reviewing information entered into the HMIS regularly to ensure that data is entered appropriately and in a timely manner.

Case Management

Providers are required to utilize the HMIS for all case management responsibilities including, but not limited to:

- Reviewing information entered into the HMIS regularly to ensure that data is entered appropriately and in a timely manner;
- Maintaining POSs (e.g. extensions, changes, transfers) for all clients assigned to case management services;
- Ensuring that all cases are closed properly and that all appropriate information is entered in the HMIS.

Refer to the document "OSH Social Worker/Case Management Performance Standards" which is appended to the Emergency Shelter Standards for details on using the HMIS to fulfill case management standards.

Additional Requirements

Providers are required to enter data into the HMIS, even if there is no case management supports available. Providers are to identify staff that will be responsible for ensuring that pertinent information is entered and updated as needed. The following data is to be entered into HMIS for all consumers:

- Demographic Information (i.e. ethnicity, race, etc.) when not entered at intake
- Serious incidents that involve violence, calls to 911, and any other incidents that affect the health and safety of residents
- Income amount and income source, updated as necessary
- Discharge information, including destination upon discharge