

HOMELESS MANAGEMENT INFORMATION SYSTEM

City of Philadelphia

Site Administrator Manual

DISTRIBUTED BY THE

Office of Supportive Housing

1401 J.F.K. Boulevard
Municipal Services Building, 10th floor
Philadelphia, PA 19102
Phone 215.686.7110 • Fax 215.686.7142

Table of Contents

Background.....	1
Current Implemenation Status.....	1
Procedural Guidelines	1
HMIS Site Administrator.....	1
Training	3
User Agreement.....	3
User Identification Codes and Passwords	3
Job Roles	4
HMIS Installation.....	5
Instructions.....	5
Troubleshooting	5
Technical Requirements.....	5
Internet Access.....	5
Firewall	6
Personal Computers and Printers	6
Operating Systems	7
Virus Protection.....	7
Connectivity	7
Contact Information.....	8
Technical Issues Related to the HMIS.....	8

Background

Current Implementation Status

The Office of Supportive Housing (OSH) has initiated the implementation of an electronic Homeless Management Information System (HMIS), which will be used throughout OSH and by all contracted providers. Implementation of the system began in 2004 and will continue through 2007.

The OSH Information Technology (IT) Unit will assist you in installation and maintenance of the HMIS at your locations. We have expertise in all facets of IT.

Procedural Guidelines

HMIS Site Administrator

Each provider agency will be asked to identify at least two individuals from its organization (a primary and a backup) who will serve as HMIS Site Administrator for its facilities. The HMIS Site Administrator will be the liaison between HMIS users at a provider site and OSH's Information Technology (IT) Unit, which performs system administration for the HMIS. HMIS users will first contact their HMIS Site Administrator with any problems they encounter in using the HMIS. If the HMIS Site Administrator is not able to resolve the problem, he or she will contact the OSH IT Unit for assistance. The HMIS Site Administrator, however, should provide the first line of HMIS troubleshooting at the site.

Should the server go down, the HMIS Site Administrator is responsible for rebooting the hub and router within two hours of the server going down. If the computers are not able to access the Internet, the HMIS Site Administrator should contact the facility's Internet Service Provider (ISP). If the computers are able to access the Internet, but not the HMIS, the HMIS Site Administrator is responsible for contacting the OSH IT Unit within two hours.

The HMIS Site Administrator must ensure that the OSH IT Unit has his or her up-to-date contact information, especially email addresses, as these are essential for communication regarding HMIS issues such as updates, service interruptions, application changes, etc. The OSH IT Unit endeavors to send email communication with as much advance notice as possible, but occasionally circumstances will dictate that emails are sent out with relatively short notice. The HMIS Site Administrator is responsible for timely monitoring of email communication from the OSH IT Unit.

The HMIS Site Administrator will also be responsible for communicating all staff departures and new hires to the OSH IT Unit. Please ensure that all staff departures and new hires are communicated to us here in the OSH IT Unit in a timely manner so that we can inactivate user profiles for departed staff, create user profiles for new staff, and arrange training for new staff. For new staff, please provide us with the following information:

- ◆ Full name
- ◆ Job title
- ◆ Email address
- ◆ Telephone number
- ◆ Permanent or temporary employee? (If temporary, projected end date of employment)
- ◆ Immediate supervisor
- ◆ Tasks that the employee performs either regularly or occasionally:
 - Maintaining the configuration of beds/units – 1a
 - Admitting clients into the shelter (accepting POSSs) – 2c
 - Taking attendance – 3e
 - Recording incidents – 4g
 - Discharging clients – 5i
 - Transferring clients between beds/units – 6k
 - Case management – 7m

Please notify us at Dorothy.Haug@phila.gov AND Bernard.Jackson@phila.gov.

Specific HMIS Site Administrators may be asked by OSH to assume the responsibility for creating and maintaining the profiles of their site's HMIS users in the system. When an HMIS user is no longer employed by a provider, the proper procedure for the HMIS Site Administrator is to remove that particular site from the user's profile and, if this is the only site assigned to the user, to inactivate the user. Should this individual then become employed by another provider, OSH's HMIS System Administrator or the new provider's HMIS Site Administrator will be able to choose the user from the user list that includes inactive users, add the new site onto the profile, and reactivate the user.

Training

All provider staff who will be users of the HMIS will be required to complete HMIS training prior to using the system. Specialized training modules exist for all of the Job Roles within the HMIS application.

User Agreement

All provider staff who will be users of the HMIS will be required to sign an HMIS user agreement prior to using the system. The user agreement will address such issues as IDs and passwords, system security, proper use of the system, and preventing the theft of information. Each staff person who will use the HMIS must sign the user agreement upon completion of HMIS training.

User Identification Codes and Passwords

Upon receiving training, new HMIS users will be provided with a user identification code (User ID) and a temporary password for logging on to the system. Federal standards require that upon first login onto the HMIS with the temporary password, the user be prompted to change the password. Below is the naming convention that must be used to create the personal password when the prompt appears. Only the user will know the personal password he or she creates. 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.

Federal and application-enforced guidelines for creating an HMIS are as follows:

- The password must be at least eight characters long.
- The password must contain at least one letter.
- The first character of the password must be a letter.
- The password must contain at least one number.
- The password must contain at least one symbol or punctuation character.
- The password may not contain your User ID.
- The password may not contain the consecutive upper- or lower-case letters "HMIS" or "hmis."

The User ID and password are not case-sensitive.

When the user is creating the password, the system will enforce these requirements through pop-up windows indicating which requirement was missed. The user may create a password that contains names, numbers, and dates familiar to the user that will make it easier for the user to remember the password, but the password should not be so predictable that it may be easily guessed.

Job Roles

Users access the HMIS through their assigned “Job Role.” A Job Role provides a grouping of screens used to carry out the tasks performed by someone in that Job Role. The Job Roles correspond to workers’ roles in OSH’s Continuum of Care, but are not necessarily the same as workers’ official job titles. Below are a few HMIS job roles followed by a few of the tasks that they perform on the system. This should aid in determining which staff will need which training.

Case Managers:

- Have a caseload assigned to them
- Create Service Plans for their clients
- Are meeting with their clients on a regular basis
- May be responsible for the upkeep of their caseload’s POSS
- Work toward completion of the transitional housing application (where applicable)
- Close cases (where applicable).

Case Manager Supervisors:

- Oversee the activity of a group of case managers (as defined above)
- May review and approve service plans, protocol violations, and case close-outs
- May assign cases to case managers
- May run case reviews and have need of access to data on all clients that their case managers oversee.

After Hours Processing Clerks: (evening, weekend, winter intake)

This job role is limited to workers from RHD/Ridge after-hours front desk staff, Eliza Shirley intake staff, and all sites designated by OSH to serve as winter initiative intake centers. Supervisors for this job role will need to attend the training(s) for this job role and may also want to attend the Shelter Service Supervisor job role trainings.

- Serve as nighttime, weekend, or winter initiative intake workers
- Complete initial intake form and write initial short term POS for all new and returning clients
- Is the first worker to meet with new clients or clients who are returning to shelter after some break.

Shelter Staff (including Shelter Staff Supervisors, and Shelter Staff Administrators)

It is understood that at some of the smaller sites a single person may have all three of the above roles.

- Administrative position on site at the shelter
- Is responsible for sign-in sheets and maintaining an accurate list of who is in shelter
- May be responsible for notification of vacancy to OSH or other intake sites

- May be responsible for taking day-to-day attendance
- Has occasional need to document incidents with clients and/or look up information on individual clients staying at the shelter
- May oversee day-to-day operations of the shelter
- Some shelters may use this position to update all long-term POSs.

HMIS Installation

Instructions

Complete documentation for HMIS installation is attached in the appendix.

Troubleshooting

Make sure that you have network connectivity and no PC problems such as viruses. Be sure that you are running the current version of the HMIS application. Under the File menu, the System Configuration option gives you information about the installation.

Screen shots of error messages can be made using ALT PRINT SCREEN and are essential information to include when reporting errors and bugs, along with what conditions produced the errors and on what screen they were encountered.

Technical Requirements

Internet Access

The provider is required to order Digital Subscriber Line (DSL) service with an ISP in order to run the HMIS. The bandwidth requirements for the DSL are the following:

- Minimum speed 768 kilobytes per second (kb/s) downstream.
- Minimum speed 128 kb/s upstream.

The provider must provide CAT-5 Ethernet cabling at its facilities for any of its staff and any of the City staff that will need to run the HMIS. The City may provide assistance in terminating the cable if requested, but the actual cabling is the responsibility of the provider.

Firewall

The provider will be required to purchase additional networking equipment such as a hub (network ports) for connecting computers to the Internet and distributing access to the Internet, and a router/firewall device that the provider is responsible for installing and maintaining. This device needs to be capable of supporting the Network Address Translation [NAT] protocol unless Static IP Addressing (a more costly option that is not required) is used. The provider will be responsible for maintaining the operation of all of the above equipment and for making sure that the hub, PCs, Internet connection, and wiring are in working order. OSH will provide support with HMIS problems, as long as the Internet connection is working.

Personal Computers and Printers

The provider is responsible for supplying personal computers (PCs) to its employees and the PCs on which the HMIS will be accessed must have Internet Explorer, version 6 or later, installed on them. The provider will supply the cable and should observe all applicable codes when installing the cable. All the computers from which the HMIS will be run must be in a physically secure location.

Every PC on which the HMIS is installed must also have the Java Runtime executable installed.

Every PC on which the HMIS installed must have a password-protected screen saver that automatically turns on after a short amount of time when the PC is temporarily not in use. The amount of time after which the screen saver turns on may be regulated by your organization. (Furthermore, if HMIS users will be gone for an extended period of time, they are required to log off the HMIS and shut down the PC.)

All software installed on computers that run the HMIS must be legitimate, licensed software. There should be no software installed on these computers that is unofficially obtained or "bootlegged."

Give the OSH IT Unit the exact make and model number of the printers that will be connected with the PCs running the HMIS so that the printer drivers can be installed on the Terminal Server. Be sure to inform the OSH IT Unit of the new make and model information any time a printer is changed or added so that the new printer drivers can be properly installed.

If you are still experiencing printing problems, log off the HMIS and your Terminal Services connection. If you had been logged in under "HMIS 1," try

logging on under "HMIS 2" and vice versa. This may resolve your printing problem.

OSH will not be responsible for troubleshooting HMIS printing problems where computers running the HMIS are connected to "all-in-one" printers.

Operating Systems

The HMIS will run on certain PC operating systems and not on others. The PCs running the HMIS are required to have either Windows 2000 or Windows XP operating systems. Windows '98 and Windows ME will not support the HMIS.

Furthermore, Microsoft® periodically releases Service Packs with which the HMIS may or may not be compatible. Site Administrators should check with the OSH IT Unit prior to installing any new Service Packs on computers that will run the HMIS. For instance, testing has determined that Service Pack 2 for Windows XP may create potential problems with permissions. If any computers that are to run the HMIS have Windows XP, Service Pack 2, you are responsible for downloading, installing, and running the latest version of the patch that fixes the Windows XP, Service Pack 2 problem. The following is a link to the Microsoft® website where you will be directed to the latest patch:

<http://support.microsoft.com/default.aspx?kbid=884020>.

Virus Protection

Providers should maintain antivirus software on all PC's on their network. PC's that access the Internet should be configured to automatically download updated virus definitions. Steps should also be taken to prevent the intrusion of "adware" and "spyware" programs.

Connectivity

Providers connecting to the HMIS over the Internet may use either client based Virtual Private Networking (VPN) or Terminal Services. Installation and login instructions are provided in the Appendix for both.

Contact Information

Technical Issues Related to the HMIS

T The provider HMIS Site Administrator should contact the OSH IT Unit Helpdesk with any issues related to implementation and usage of the HMIS.

Telephone: 215-686-7110

Email: HMIS@phila.gov

If calling outside of normal business hours, please feel free to leave a voice mail message. Both emails and telephone calls will be answered promptly.