



Homeless Management Information System: Policy and Procedures Manual

August 2021



I. Table of Contents

I. Table of Contents 1
II. Introduction.....2
A. Potential Benefits of HMIS..... 3
III. Roles & Responsibilities 4
B. WellSky Information Systems 4
C. Continuum of Care 4
D. Homeless Alliance of Western New York (HAWNY)..... 4
E. HAWNY Board of Directors 5
F. HMIS Advisory Committee 5
G. HMIS Administrator (System Admin)..... 5
H. HMIS Agency Administrator 6
I. HMIS Agency Users..... 6
IV. Policies and Procedures..... 7
A. Participation 7
B. Equipment, System Requirements, Software Information and Licensure 7
C. Security Plan..... 9
D. HMIS Lead Agency Security Responsibilities..... 10
E. Participating Agencies Security Responsibilities 11
F. Security Incidents..... 12
G. Access Control and Access Level..... 14
H. Privacy and Data Sharing Plan 18
I. Disaster Recovery Plan: 23
V. Data Collection, Types, and Usage24
J. Data Quality Plan 25
K. Data Timeliness..... 27
L. HMIS Monitoring 28
M. HMIS Coordinated Entry 29
N. Grievances 29
O. Termination of HMIS Participation..... 30

II. Introduction

Homeless Management Information System (HMIS) is a database which allows authorized personnel at homeless housing and service provider agencies to enter, track, and report information on the clients they serve. HMIS provides opportunities for service providers that serve the same client to operate with a single case plan, reducing the amount of time spent in documentation activities and ensuring that care is coordinated and messages to clients are while meeting reporting requirements for the U.S. Department of Housing and Urban Development (HUD) and other funders.

In compliance with all federal requirements regarding client confidentiality and data security, HMIS is designed to collect and deliver timely and accurate data about services and homeless persons or persons at risk for being homeless. This information is collected via interviews conducted by trained service provider staff. Data is then analyzed in order to provide an unduplicated, aggregate count (void of any identifying client-level information). This information is made available to service providers, advocates, consumer representatives, and policy-makers. Information is also used to better understand current gaps in the homeless continuum of care and human service delivery system.

HMIS utilizes the Service Point Client Information Management System developed by WellSky Information Systems. Service Point is an Internet-based client information system that provides a standardized assessment of consumer needs, aids in the creation of individualized service plans, and records the use of housing and services. Communities can then use this information to determine how services are utilized, identify service needs, and develop outcome measurements.

Involvement in HMIS will allow service providers to generate automated APRs and reports which can aid in the development and evaluation of programming. At a community level, HMIS will provide aggregated data across the entire homeless service continuum for use in the annual Continuum of Care funding application and city and county consolidated plans. Findings can also be used to inform policy decisions aimed at addressing and ending homelessness at the local, state, and federal levels. Finally, and most importantly, HMIS will ease the process of securing services for homeless individuals and families in our area. A more complete list of the potential benefits of HMIS is available on the page that follows.

This document provides information about HMIS staffing, technology, and participation requirements, as well as an overview of policies, procedures, and standards that govern its operation especially with regard to confidentiality, security, and data expectations. Copies of all necessary supporting documents are also included in this manual as well as a glossary of commonly-used terms.

A. Potential Benefits of HMIS

For Clients	For Service Providers	For Community
Makes it possible to maintain intake information over time so the number of times a homeless person repeats their story to providers is reduced.	Provides real-time information about needs and available services for homeless persons.	Helps the community to define and understand the extent of homelessness throughout the CoC.
Offers an opportunity to conduct intakes and life histories once; illustrating that service providers consider the homeless person's time valuable and ensuring consumer dignity.	Assures confidentiality by keeping information in a secured system.	Provides greater focus for staff and financial resources to the geographical areas, agencies, and programs where services for the homeless are needed most.
Makes it possible to coordinate multiple services and streamline referrals. This will help to reduce consumer waiting time.	Decreases duplicative client intakes and assessments. Reduces time required to conduct intakes and assessments	Allows for better evaluation of the effectiveness of specific interventions, programs, and services.
	Tracks client outcomes and provides a client history.	Offers local, state, and federal legislators data and information about the homeless population.
	Generates data reports for local use and to meet funding requirements.	Makes it possible to meet all federal reporting requirements.
	Facilitates the coordination of services internally and externally with other agencies and programs.	
	Provides access to a community-wide database of service providers and allows agency staff to easily select a referral agency.	

III. Roles & Responsibilities

B. WellSky Information Systems

Responsible for the delivery of Internet-based client assessments and reporting features.

WellSky Information Systems will provide secure, on-going access to its Service Point, Shelter Point, Call Point, Community Point and Resource Point applications via the Internet. In addition, WellSky Information Systems will also provide information about any system modifications and/or upgrades.

C. Continuum of Care

- Must designate a single information system as the official HMIS software for the geographic area.
- Designate an HMIS lead to operate the HMIS
- Develop a governance charter which at minimum includes:
 - A requirement that the HMIS Lead enter into written HMIS Participation Agreements with each participating agency
 - The participation fee charged by the HMIS
 - Such additional requirements may be issued from time to time
- Maintain documentation evidencing compliance with regulations and with the governance charter
- Review, revise and approve the policies and plans required by regulation and any notices issued from time to time

D. Homeless Alliance of Western New York (HAWNY)

The HMIS Lead Agency. The HMIS Lead Agency is responsible for:

- Ensuring the operation of and consistent participation by recipients of funds from the Emergency Solutions Grant Program and from other programs authorized by Title IV of the McKinney-Vento Act.
- Developing written policies and procedures in accordance with regulations
- Executing a written HMIS Participation Agreement with each CHO.
- Serving as the applicant to HUD for grant funds to be used for HMIS.
- Monitoring and enforcing compliance by all CHO's.
- Submitting a security plan, data quality plan and privacy policy to the CoC for approval within six months of any changes to the regulations.
- Reviewing and updating HMIS documents at least annually that incorporates feedback from the HMIS Advisory Committee and CoC approval.

HAWNY will secure funding for the HMIS and provide organizational oversight through its Board of Directors and the HMIS Advisory Committee. HAWNY will also provide regular staffing for the project.

E. HAWNY Board of Directors

Responsible for providing organizational oversight for the HMIS through review of policy and procedures identified by the HMIS Advisory Committee.

F. HMIS Advisory Committee

Responsible for developing and reviewing all system-wide policies and procedures for HMIS.

In selecting participants for this committee, HAWNY will attempt to secure and maintain representation from each:

- Homeless housing and service type;
- HUD-identified homeless subpopulation;
- Continuum of Care municipality; and from

The HMIS Advisory Committee will provide input on an on-going basis for the local HMIS project. The Committee will share its recommendations with the HAWNY Board of Directors and CoC membership meetings on the key issues that follow:

- Determining guiding principles for HMIS;
- Selecting data elements to be collected in addition to HUD requirements by participating agencies;
- Defining parameters for the release of aggregated HMIS data;
- Evaluating HMIS compliance with HUD data and technical standards;
- Reviewing the HMIS-related performance of participating agencies especially adherence to local policies and procedures; and
- Addressing issues that arise from use of HMIS including, but not limited to, client grievances and policy adjustments.

G. HMIS Administrator (System Admin)

The HMIS Administrator is responsible for the implementation and coordination of the local HMIS. The administrator will be the primary contact for HAWNY, the HMIS Advisory Committee, and HMIS Agency Administrator.

Responsibilities include:

- Orienting prospective HMIS participants to system;
- Maintaining a list of agency contacts and HMIS participants;
- Providing oversight on all contractual agreements;
- Assessing agency readiness for HMIS;
- Developing training manual and providing regular trainings;
- Authorizing access to the HMIS (Set-Up);
- Developing client assessment tools not already included;
- Providing basic technical assistance to participating agencies;
- Facilitating access to hardware/other technical support;
- Documenting database and policy/procedure changes;

- Developing and evaluating performance objectives;
- Updating “Standard Operating Procedures Manual;”
- Monitoring, reporting, and resolving access control violations;
- Auditing HMIS usage system-wide;
- Developing reports and queries for Continuum of Care;
- Presenting research findings to community stakeholders;
- Coordinating regular user-group meetings; and
- Communicating with participating agencies/larger community.

The System Administrator also serves as the Security Officer of the HMIS lead agency.

H. HMIS Agency Administrator

The HMIS Agency Administrator will serve as the agency contact for the project and will facilitate access to the HMIS at the user organization level.

Each HMIS Agency Administrator will be responsible for:

- Participating in HMIS readiness assessment;
- Identifying HMIS users and facilitating access to training;
- Granting HMIS access staff members that have received training and demonstrated proficiency in system use and understanding of policies and procedures;
- Monitoring staff compliance with standards of client consent and confidentiality and system security;
- Enforcing business controls and practices to ensure organizational adherence to policies and procedures including detecting and responding to violations;
- Providing on-site support for the generation of agency reports and managing user licenses;
- Ensuring stability in the agency Internet connection either directly or in communication with a technician; and
- Notifying users about interruptions in service.

I. HMIS Agency Users

HMIS Agency Users are responsible for entering client data into the system as well as identifying needs and concerns regarding HMIS to their Agency Administrator.

HMIS Agency Users will be responsible for:

- Being aware of the confidential nature of data and taking appropriate measures to prevent any unauthorized disclosure of client information;
- Accurate and timely data entry;
- Complying with all local HMIS policies and procedures; and
- Reporting security violations to their HMIS Agency Administrator.

Agency users are also responsible for their own actions or any actions undertaken with their usernames and passwords.

IV. Policies and Procedures

A. Participation

All homeless services and housing providers are encouraged to participate. Participation in HMIS can be mandatory as required by funder(s). Non-mandatory HMIS participation is at the discretion of the HMIS Lead agency. HMIS participation may incur fees where applicable.

In order to participate in HMIS, providers must agree to each of the following:

- **Agency Participation Agreement:** Agencies are required to sign a participation agreement stating their commitment to adhere to the policies and procedures for effective use of HMIS and proper collaboration with HAWNY. A copy of the Agency Agreement is available in the Supporting Documents section of this manual and on the HAWNY website.
- **Identification of HMIS Agency Administrator(s):** Agencies will designate one or more key staff persons to serve as HMIS Agency Administrator(s). The Agency Administrator is the primary liaison with the system administrator and serves as the agency contact for the project and will facilitate access to the HMIS at the user organization level.
- **Training:** HMIS Agency Administrators will be responsible for identifying HMIS Users and coordinating initial and any subsequent training sessions. Each new User must complete training prior to gaining access to HMIS.
- **Client Consent:** Agencies will maintain signed copies of the Client Consent and Release of Information form in a secure, on-site location. These forms authorize the input of personal information electronically into HMIS and specify what information may be included. A copy of the form should be provided to each client upon request.
- **Data Collection:** Agencies agree to collect client information on all HUD- and locally- required data elements. HUD-required elements are identified through Data and Technical Standards. Local elements will be established by the HMIS Advisory Committee.

B. Equipment, System Requirements, Software Information and Licensure

The following are the minimum requirements for operating Service Point as recommended by the vendor, Wellsky Information Systems.

Memory

- If Win7 – 4 Gig RAM recommended, (2 Gig minimum)
- If Vista – 4 Gig RAM recommended, (2 Gig minimum)
- If XP – 2 Gig RAM recommended, (1 Gig minimum)

Up-to-Date Anti-Virus Protection

Other device recommendations

To maximize the performance of HMIS:

1. *Browser:*
 - o Google Chrome, version 11.0.696.65 or above (Recommended)
 - o Microsoft Internet Explorer, version 7 or above.
 - o Mozilla Firefox, version 3.5 to 4 (soon to be 3.5, 4, 5 and beyond)
 - o Apple Safari, version 4 or 5
2. *Internet Connection: Broadband (recommended) or LAN connection.*
3. *Monitor: Screen Display - 1024 by 768 (XGA) or higher (1280x768 strongly advised)*
4. *Processor: Avoid using single-core CPUs*

System Availability

The HMIS is available 24 hours a day, 7 days a week, 52 weeks a year with the exception of scheduled system upgrades and routine maintenance.

- *In the event of planned downtime*, the HMIS Administrator will inform agencies via email
- *Unexpected service interruption*, the HMIS Administrator will contact the HMIS Agency Administrators to inform them of the cause and possible duration of the service interruption. Contact will be made via email.

Technical Support

The HMIS Administrator will provide system support by phone, email, computer shadowing, and/or in-person consultations. The HMIS Agency Administrator should act as the first level of contact when a system problem arises and should determine if the problem requires immediate rectification.

- If the HMIS Agency Administrator cannot resolve the problem the Agency Administrator should call HMIS Administrator. HMIS Administrator will respond to the call as soon as possible.

Participating agencies are responsible for their own computer hardware and Internet connections, thus will be responsible for accessing technical following their Agency's protocols.

Data Ownership

Participating agencies are the owners of all client data collected and stored within HMIS. This data is protected and secured by the policies, technologies, and security protocols held in place. All participating Agencies must take full responsibility of ownership and confidentiality protection of any and all data that is collected at their agency and/or downloaded from HMIS.

C. Security Plan

WellSky Information Systems Security Responsibilities

Document, WellSky Information Systems Securing Client Data, can be found in our website: www.wnyhomeless.org for information on how WellSky ensures security of all client data on ServicePoint Site.

HMIS Lead Agency and Participating Agency Security Responsibilities

- 1) All Agencies (HMIS Lead Agencies and CHOs) must assign a Security Officer (Agency or System Administrator can also serve as the Security Officer) (Finalization of the HMIS regulations will be released in the near future. Further clarification will be provided.). The Security Officer is responsible for:
 - a) Ensures that all staff using the System complete annual privacy & security training.
 - b) Ensures the removal licenses to the HMIS when a staff person leaves the organization or revision of the user's access level as job responsibilities change.
 - c) Reports any security or privacy incidents to the HMIS administrator. The System Administrator investigates the incident including running applicable audit reports. If the System Administrator and/or Security Officer determine that a breach has occurred and/or the staff involved violated privacy or security guidelines, the System Administrator will report to the Executive Director of the Homeless Alliance. A Corrective Action Plan will be implemented for the agency. Components of the Plan must include at minimum supervision and retraining. It may also include temporary suspension of HMIS license, client notification if a breach has occurred, and any appropriate legal action.
- 2) Criminal background checks must be completed on all Security Officers and System Administrators. (Finalization of the HMIS regulations will be released in the near future. Further clarification will be provided.).
- 3) HAWNY conducts routine audits of participating Agencies to ensure compliance with the Standard Operating Procedures Manual. HAWNY will use a checklist to guide the inspection and make recommendations for corrective actions.
- 4) Agencies are required to maintain a culture that supports privacy.
 - a) Staff does not discuss client information in the presence of others without a need to know.
 - b) Staff eliminates unique client identifiers before releasing data to the public.
 - c) The Agency configures workspaces for intake that supports privacy of client interaction and data entry.
 - d) User accounts and passwords are not shared between users, or visible for others to see.
 - e) Program staff is educated to not save reports with client identifying data on portable media as evidenced through written training procedures or meeting minutes.



- 5) All staff using the System must complete Privacy and Security Training annually. Certificates documenting completion of training must be stored for review upon audit.
- 6) Victim Service Providers may be prohibited from entering client level data in HMIS. These providers that receive McKinney-Vento funding must maintain a comparable database to be in compliance with grant contracts.

D. HMIS Lead Agency Security Responsibilities

Physical Security

The Homeless Alliance of Western New York is at 960 Main Street, Buffalo, NY 14202. Passwords are required to access individual workstations. Any raw data or system information is stored in locked cabinets to maintain confidentiality and security.

System Access Monitoring

Service Point automatically tracks and records access to every client record by use, date, and time of access. HMIS Administrator will monitor access to HMIS by regularly reviewing user access frequency and deactivate license when users no longer require access.

The System Administrator will confirm (through the monitoring process) that the Agency provides HMIS workstation(s) that:

- Has and uses a hardware or software firewall.
- Has and uses updated virus/spy protection software
- Has and uses screens saver and require a password to re-activate
- Has screens positioned so that data is not visible to others; (ie . – other staff, clients, etc. who are in the immediate area)
- Do not have usernames and/or passwords posted in visible and/or accessible locations

User Authentication

HMIS will only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent theft. If a user enters an invalid password four consecutive times, HMIS automatically marks them inactive. User/ agency administrator will need to contact the System Administrator to obtain a temporary password. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Administration and System-wide Data

The HMIS Administrator(s) will have full access to HMIS. The System Administrator can add, edit, and delete users, agencies, and programs and reset passwords. Access to system-wide data will be granted based upon need to access the data. The HMIS Administrator(s) is responsible and accountable for the work done under system information and personal identifiers.

E. Participating Agencies Security Responsibilities

Physical Security

Agencies must develop rules to address physical access to workstations.

The Agency Administrator will ensure that the Agency provides HMIS workstation(s) that:

- Has and uses a hardware or software firewall.
- Has and uses updated virus protection software
- Has and uses screens saver and require a password to re-activate
- Has screens positioned so that data is not visible to others; (i.e. other staff, clients, etc. who are in the immediate area)
- Do not have usernames and/or passwords posted in visible and/or accessible locations

Access to Data

- **User Access:** Users will only be able to view the data entered by users of their own agency or with user agencies that have agreed to share data. HMIS has security measures in place which prohibit agencies from viewing each other's data unless Inter-Agency Data Sharing Agreements have been negotiated and client consent has been signed.
- **Raw Data:** Users who utilize Report Writer and/or ART have the ability to download and save client level data onto their local computer. Once this information has been downloaded from HMIS in raw format to an agency's computer, the data becomes the responsibility of the agency.
- **Policies Restricting:** Each HMIS participating agency must establish internal policies on access to data protocols. These policies should include who has access, for what purpose, user account sharing and how they can transmit this information. Issues to address include storage, transmission, and disposal of data.

Client Paper Record Protection

Partner agencies must establish procedures to handle client paper records. Issues to be addressed include:

- Identifying which staff has access to client paper records and for what purpose.
- Allowing staff access only to the records of clients whom they work with or for data entry purposes.
- How and where client paper records are stored.
- Length of client paper record storage and disposal procedures; and
- Disclosure of information contained in client paper records.
- Authorized employees, using methods deemed appropriate by the participating agency, may transport HMIS data which meets approved security standards.

- However, a record of the transport – including information about the nature and type of information - must be maintained as well as a notification of information return.

Access Monitoring

The Agency Administrator will be responsible for monitoring all user access within their agency. Any violations or exceptions should be documented and forwarded to the HMIS Administrator immediately.

- All suspected data, system security, and/or confidentiality violations will incur immediate user suspension from the HMIS until the situation is effectively resolved. Serious or repeated violation by users of the system may result in the suspension or revocation of an agency's access to HMIS.
- Any user/agency found to be in violation of data, system security, and/or confidentiality protocols will be sanctioned accordingly. Recommended sanctions may include but, are not limited to, a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of employment, and criminal prosecution.

F. Security Incidents

A security incident is defined as any occurrence that adversely affects or has the potential to adversely affect the integrity and/or confidentiality of the information contained within HMIS or its operation.

Categories and Definitions

Security incidents can be categorized as the following:

1. *Data or file extraction*

Unauthorized, electronic removal of information from HMIS.

2. *Introduction of Malicious Code or Virus*

Intentional or unintentional, unauthorized introduction of malicious code or virus onto the HMIS or agency computer equipment.

3. *Misrepresentation of data*

Intentional or unintentional, misrepresentation of client/ agency level information.

4. *Attempts to modify passwords or access rights*

Intentional or unintentional attempt to modify HMIS user passwords or access rights.

5. *Compromised or lost password*

A compromise in a password occurs when staff believes that an individual other than the one to which the password is assigned becomes aware of the password. Sharing a license is considered a compromise.

6. *Theft of HMIS equipment or media*

This includes stolen PCs, towers or media that may contain client information

7. *Dissemination of protected client information from HMIS in electronic or paper form*

Intentional or unintentional, unauthorized dissemination of client information in an electronic format. This includes sending email or a FAX to an unintended recipient.

Security Incident Documentation

All security incidents must immediately be reported to the HMIS Administrator via phone call. The HMIS Administrator will provide direction as needed to the individual(s) responding to the security incident and to evaluate the necessity of mobilizing additional resources. The HMIS Administrator is also responsible for ensuring that immediate action is taken to protect the security and integrity of the HMIS and client data.

After the security incident, the staff member must complete a written Security Incident Report as soon as possible and forward it to the HMIS Administrator. The purpose of the report is to provide subsequent readers with an accurate image of the security incident through written documentation.

The report should be written in a clear, concise, and specific manner and should focus on the facts and events that occurred immediately prior to the incident, the incident itself, and the events that occurred immediately after the incident.

In addition to the above items, the report should include:

- Parties involved including each staff member's full name;
- A summary of each party's actions;
- Time and location of the incident; and
- Observations of any environmental characteristics that may have contributed to the incident.

The HMIS Administrator will take responsibility for reporting the incident to the HAWNY Executive Director, and when appropriate, law enforcement officials.

If the security incident occurred at the HMIS Lead, it should be reported to the Executive Director who will assign the appropriate staff to investigate and report to the HMIS Advisory Committee.

Review of Security Incidents

Severe security incidents will be reviewed at the next regularly scheduled meeting of the HMIS Advisory Committee to ascertain if the incident could have been avoided or the impact minimized. Each incident will be scrutinized to determine the appropriateness of staff actions and protocols. Recommendations about the need for additional resources, staff training, security modifications, and protocols will also be noted.

More specifically, the Advisory Committee will:

- Evaluate the timeliness, thoroughness, and appropriateness of the staff member's response to the security incident;
- Ascertain if the security incident could have been prevented;
- Recommend corrective actions, if warranted;
- Evaluate security incidents for trends and patterns;
- Monitor the agency's compliance with the security policies and protocols;
- Monitor the implementation of any preventative or corrective action; and
- Recommend changes to the HAWNY Board of Directors regarding policies, procedures and practices, and working agreements that will reduce the likelihood that similar security incidents would occur.

An aggregate report of security incidents will be compiled by the HMIS Administrator on a quarterly basis for review by the HMIS Advisory Committee. At minimum, these incidents will be analyzed by type of incident, location, employee/organizational involvement, time and date. Records of security incidents will be maintained by the HMIS Administrator.

On-Going Review of Security Measures

The HMIS Administrator and HMIS Advisory Committee will be responsible for providing on-going monitoring of agency compliance with HMIS Standard Operating Procedures. This monitoring will include review of security policy and procedures and will occur on an annual basis.

G. Access Control and Access Level

Access Control

Access to HMIS will be controlled based on need and is at the discretion of the HMIS lead agency. Need exists only for those administrators, project staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients or who have data entry responsibilities.

HMIS access for law enforcement and law enforcement contracted agencies is prohibited to protect client and service provider relationships. Access may only be granted by court order or as outlined in the HMIS privacy policy.

Access is controlled through user identification and authentication. Users are responsible and accountable for work done under their personal identifiers. Security violations will be monitored, reported and resolved. An agency or an individual user's access may be suspended or revoked for suspected or actual violation of the security protocols.

Passwords

Passwords are automatically generated by the HMIS when a new user is created or if a password is forgotten and needs to be reset. HMIS Agency Administrators or

system admin will communicate the system-generated password to each respective agency user.

Each user will be required to change the password the first time they log onto the HMIS. The password is alphanumeric and case sensitive. It must be at least 8 characters, Upper- and lower-case letters, and contain at least 2 numbers or symbols. Passwords are the individual's responsibility and users cannot share passwords under any circumstances even with staff members at their own agency. Passwords should not be easily guessed or found in any dictionary. They should be securely stored and inaccessible to other persons. The use of password managers for HMIS passwords is prohibited.

Passwords expire every 45 days. A password cannot be re-used until one entirely different password selection has expired.

Access Levels

User accounts can be created and deleted by the HMIS Agency Administrator or System Administrator. User access levels will be directly related to the user's job responsibilities and need for access to HMIS data.

Below is a list of "Access Levels" and chart of activity designations within the HMIS.

1. Resource Specialist I

Resource Specialist I users are limited to the ResourcePoint module. This allows users to search for area providers/organizations and view their details. These users have no access to client or service records. A Resource Specialist cannot modify or delete data.

2. Resource Specialist II

Resource Specialist II users have access to ResourcePoint. These users are also considered agency-level I&R specialists who update their own organization's information. To perform these tasks, they also have access to Admin Providers and Agency Newsflash.

3. Resource Specialist III

Same as Resource Specialist II, but also includes access to System Newsflash and limited range of reports.

4. Volunteer

Volunteers have access to ResourcePoint. These users can also view or edit basic demographic information about clients on the Profile screen, but they are restricted from viewing other assessments. A volunteer can create new client records, make referrals, or check clients in and out of shelters. Administrators often assign this user level to individuals who complete client intake and refer clients to agency staff or a case manager. In order to perform these tasks, volunteers have access to some areas of ClientPoint and ShelterPoint.

5. *Agency Staff*

Agency Staff users have access to ResourcePoint and ShelterPoint. These users also have limited access to ClientPoint, including access to service records and clients' basic demographic data on the Profile screen. Agency Staff cannot view other assessments or case plan records. Agency Staff can also add news items to Agency Newsflash.

6. *Case Manager*

I, II and III Case Managers have access to all ServicePoint features except those needed to run audit reports and features found under the Admin tab. They have access to all screens within ClientPoint, including assessments and service records. Case Manager II users can also create/edit client infractions if given access by an Agency Administrator or above. Case Manager III users have the added ability to see data down their provider's tree like an Agency Admin.

7. *Agency Administrator*

Agency administrators have access to all ServicePoint features, including agency level administrative functions. These users can add and remove users to and from their organization, as well as edit their organization's data. They also have full reporting access with the exception of five reports: Client/Service Access Information, AHAR Annual Homeless Assessment Report, Duplicate Client Report, Exhibit 1: HUD-40076 (CoC)-M), and Call Record Report. Agency Admins cannot access the following administrative functions: Assessment Administration, Direct Access to Admin>Groups, Picklist Data, Admin>Users>Licenses, or System Preferences.

Agency Administrators can delete clients that were created by organizations within their organizational tree. They cannot, however, delete clients who are shared across organizational trees. Additionally, Agency Admins can delete needs and services created within their own organizational tree, unless the needs and services are for a shared client.

8. *Executive Director*

Executive Directors have the same access rights as Agency Administrators; however, they are ranked above Agency Administrators.

9. *System Operator*

System Operators have access to administrative functions. They can set up new providers/organizations, add new users, reset passwords, and access other system-level options. They can also order and manage user licenses. These users have no access to Client Point, Shelter Point, or Reports. System Operators help maintain Service Point, but cannot access any client or service records.



Homeless Management Information System Policy and Procedures Manual

10. System Administrator I

System Administrator I users have access to all ServicePoint features and functions except the Client/Service Access Information audit report, and System Preferences.

System Administrator I users cannot merge clients and do not have access to the following reports: AHAR Annual Homeless Assessment Report, Duplicate Client Report, Exhibit 1: HUD-40076 (CoC)-M), and Call Record Report. System Administrator I users can delete clients that were created by organizations within their organizational tree. They cannot, however, delete clients who are shared across organizational trees. Additionally, System Admin I users can delete needs and services created within their own organizational tree, unless the needs and services are for a shared client.

11. System Administrator II

System Administrator II users have full and complete access to all ServicePoint features and functions. This includes access to Provider Groups and the ability to generate reports for these groups.

System Administrators II can delete clients, needs, and services created across organizational trees.

Detail access features and ability can be found in this user role spreadsheet:

http://sp5help.Wellskysystems.com/ServicePoint5_Help/57x/ServicePoint_Help/default.htm?url=WordDocuments%2Fsecurityanduserlevels.htm

Plan for Remote Access

All HMIS Users are prohibited from using a computer that is available to the public or from accessing the System from a public location through an internet connection that is not secured. For example, staff is not allowed to use Internet Cafes, Libraries, Airport Wi-Fi or other non-secure internet connections. Agency Privacy Policy must have a plan for remote access if staff will be using HMIS outside of the office such as doing entry from home. Concerns addressed in this plan should include the privacy surrounding the off-site entry.

- a) The computer and environment of entry must meet all the standards defined above.
- b) Downloads to the off-site computer may not include client identifying information.

User Termination or Extended Leave from Employment

The HMIS Agency Administrator should terminate the rights of a user immediately upon suspension or termination from their current position. If a staff person is to go on leave for a period of longer than 45 days, their password should be inactivated within 2 business days of the start of their leave. The HMIS Agency Administrator is responsible for removing users from the HMIS. The HMIS Agency Administrator

should also review the agency access list and signed agreements on a quarterly basis to ensure that records are up-to-date. The HMIS Agency Administrator must provide information about changes to the HMIS Administrator.

Report Access and Transport

Select HMIS users will have access to agency-level HMIS data in the form of reports and client case files. Access to this information is based on User Level and is determined based on need. Reasonable care should be taken when reviewing HMIS materials to ensure information is secure.

- Media and documents containing client-identified data should not be shared with any agency other than the owner of the data (and their partners) for any reason. An inter-agency sharing agreement and client consent must be secured before the agency shares information with another member of the system. Copies of the Inter-agency Data Sharing Agreement and the Client Consent and Release of Information Authorization forms can be found in the Supporting Documents section of this manual and on the HAWNY website.
- Printed HMIS information should be stored or disposed of properly.
- All client records containing identifying information that are stored within the Participating Agency's local computers are the responsibility of the participating agency.
- Media containing HMIS data that is released and/or disposed of by the participating agency should first be processed to destroy any data residing on that media. Degaussing, shredding and overwriting are acceptable methods of destroying data.

H. Privacy and Data Sharing Plan

There are two levels of data sharing in the HMIS. The CoC is encouraging participating agencies to share all data relevant to providing housing and services to the homeless with client consent. Sharing data will reduce the amount of time that agencies and clients will need to spend at intake repeating the same information that has already been shared with multiple providers in the community and will allow for better coordination of services for clients in the homeless system. Sharing data will also support the CoC's goal of designing a centralized point of entry using a common assessment tool (will be located in HMIS) that will ensure clients are being directed to the housing and services that best meet their household's needs.

Level 1 Data Elements

Name, last four digits of Social Security Number, Veteran Status, and year of birth. These elements will prevent duplication of records in the system. (Although the first five digits of Social Security Number will not be shared, we still highly recommend you input them in the system for de-duplication purpose.)

Level 2 Other Data Elements:

Client data may be shared with partnering agencies only with client approval

- a) All sharing practices with partnering agencies will be documented and governed by an Inter-Agency Data Sharing Agreement that defines the agency-determined sharing practice.
- b) Agency defaults within the HMIS will be set to “closed” with the exception of first name, last name, last four digit of Social Security Number and year of birth. Data elements will be set to “Open” as guided by the Inter-Agency Data Sharing Agreement and any additional sharing agreements negotiated between agencies.
- c) A completed HMIS Client Release of Information (ROI) Form is needed before information may be shared electronically.
 - i) The HMIS release is customized to inform the client about what is shared and with whom it is shared. The customization reflects the data elements agreed to be shared in the Inter Agency Data Sharing Agreement.
 - ii) The client accepts or rejects the sharing plan.
 - iii) If the client rejects the sharing plan, agency staff is responsible to close the record in HMIS. Services will continue with the agency.
- d) Clients will be informed about the benefits, risks, and available alternatives to sharing their information prior to signing an ROI, and their decision to sign or not sign shall be voluntary.
- e) Clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.
- f) All Client Authorization for ROI forms related to the HMIS will be placed in a file to be located on premises and will be made available to HAWNY for periodic audits.
- g) HMIS-related Authorization for ROI forms will be retained for a period of **7** years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
- h) No confidential/restricted information received from the HMIS will be shared with any organization or individual without proper written consent by the client, unless otherwise permitted by applicable regulations or laws.
- i) Restricted information, including progress notes and psychotherapy notes, about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence concerns shall not be shared with other participating Agencies without the client’s written, informed consent as documented on the Agency-modified Authorization for Release of Confidential Form.

- Sharing of restricted information is not covered under the general Client Consent and Release of Information Authorization template.
- If a field that normally contains non-confidential information discloses confidential information.
 - (1) The staff completes an Authorization to release Confidential Information.
 - (2) If the client refuses to authorize the release, the staff closes the Assessment/data elements by clicking the lock on the screen and removing any exceptions.
- j) If a client has previously given permission to share information with multiple agencies, beyond basic identifying information and non-restricted service transactions, and then chooses to revoke that permission and the record will be locked by the agency from future sharing. Record prior to the revocation will remain shared.
- k) All client ROI forms will include an expiration date. ROI expiration date should be determined by the expected length of time the client will be enrolled in the program. If the client remains active in the program past the expiration date, the agency may not enter any additional information into HMIS until after a new ROI has been executed.

Client Informed Consent and Release of Information (ROI)

Participating agencies are required to inform clients about HMIS and to gain their consent prior to entering data into the computerized system. In addition, the agency must agree not to release any confidential information received via HMIS to any organization or individual without proper written consent. A signed and dated Client Release of Information(s) must be stored in the Client Record (paper or scanned onto the System) for all Automated ROIs that release data between different agencies – external sharing.

The Agency should summarize to each client the following information:

What HMIS is

- An Internet-based information system that homeless services agencies use to capture information about the persons they serve.

Why the Agency Uses It

- To understand their client's needs
- To help the programs plan to have appropriate resources for their clients
- To inform public policy to reach the goal of ending homelessness

Security

- Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records.

Privacy Protection

- Information is transferred over the internet through a secure connection.
- No client information will be released to another agency without written or verbal consent.
- Client has the right to not answer a question(s), unless admission to the program requires it.
- Client has the right to know who has added to, deleted, or edited their record.

Benefits for Clients

- Clients will not have to repeat their story to multiple providers.
- Case manager and client can use information to make linkages to community resources.

The agency is responsible for ensuring that this procedure takes place at the initial contact for each client. In instances where the client does not speak English or seems to have difficulty understanding; it is the responsibility of the agency to make sure consent is informed.

IMPORTANT INFORMATION:

- Clients cannot be refused services solely based on their refusal to participate in HMIS!

Written Informed Consent

At entry into the program, the Agency will provide a verbal explanation of both the HMIS project and the terms of consent and provide the client with the ROI. The client will complete, sign and date the HMIS ROI.

A copy of the Client Consent and Release of Information Authorization form is available in the Supporting Documents section of this manual and on the HAWNY website.

Verbal Informed Consent

Verbal consent can be only accepted in the case of phone interview for agencies/ programs only contact clients by phone. Agency staff will provide a verbal explanation of both the HMIS project and the terms of consent. Agency staff will complete, sign and date the release on the client's decision.

Consumer Notice

All participating agencies must post a Consumer Notice in a conspicuous area to inform clients of participation in HMIS. A copy of the Consumer Notice is included in

the Supporting Documents section of this manual and on the HAWNY website. The notice should be made available to clients upon request.

Privacy Notice

A notice detailing all privacy protections should be made available to clients upon request. A Privacy Protection Notice template is included in the Supporting Documents section of this manual and on the HAWNY website.

Entering Consent into HMIS

In the Service Point system, it is necessary to indicate that a release was granted in all cases.

- If a client permits open sharing of his or her records or agrees to the default settings of the agency and signs a release to that effect, the agency user should indicate under the ROI tab in Client Point that a release was granted and that there is a “Signed Statement from the Client.”
- When an Agency agrees to share and a client does not permit any sharing of his or her information other than name, last four digits of SSN and year of birth outside the agency, **the agency needs to select “no” for release granted in HMIS. The record will not be shared with other agencies.**

Revocation of Consent

If a client chooses to revoke the ROI it should be understood that only data going forward will not be shared. Historical data will remain shared.

A client has the right to revoke consent for data sharing at any time. When a client makes such a request, the agency staff person should ask the client to sign a Revocation of Consent form (see supporting documents) to be forwarded to the HMIS Agency Administrator and immediately change the end date of the ROI in HMIS as the date of the revocation.

Using the completed Revocation of Consent form, the HMIS Agency Administrator will ensure that the client’s record was properly closed for future sharing. This policy will be reviewed with staff periodically.

In the event that a client would like to “re-open” their file to sharing, staff members should follow standard consent procedures including written and electronic documentation of the decision.

Use of Unnamed Client Feature

In the rare instances where a client is not willing to share any data because of security concern, like domestic violence, Wellsby Information Systems has developed a client entry option that allows the input of client information without showing the client’s name into the database. It uses an algorithm similar to the one used for “Named Clients” and provides a more accurate unduplicated client count than using the “Anonymous Client” record. Although this feature does not use the Social

Security Number to create the identifier, it will allow organizations to include this information after initial intake.

Access of the Unnamed Client Feature will only be granted with the Agency Administrator's approval, it must only be used for clients who are unwilling to disclose their personally identifying information (i.e., name) because of domestic violence or other special concerns.

To use the Unnamed Client Feature, Agency Administrators must first contact the HMIS Administrator in order to activate the function. Agency Administrator should contact System Administrator once finish editing the unnamed client.

Note: Agencies should be aware that once the Agency or System Administrator enables "Manage Unnamed Clients" feature, the user will be unable to create Named Clients until the Unnamed Client feature is disabled and the user's profile is returned to its original state.

When enabled, users will observe that the first and last name of the client do not appear in the profile. Instead, "Unnamed" appears in the first name field and the client number appears in the last name field. Users will not be able to modify these fields. The data entered for Date of Birth, Gender, and Race are retained within the system for the purposes of aggregate reporting. All other features and assessments are available.

Without the client's Unnamed Client ID number, users will not be able to search for or locate a client previously entered into the system. Therefore, a protocol should be established by the agency to securely retain client id information. Providers should include the assigned code in the client record to ensure that they will be able to access the file.

It is not possible to share the records of unnamed clients with other HMIS participating organizations.

I. Disaster Recovery Plan:

The HMIS can be a critically important tool in the response to catastrophic events. The HMIS data is housed in a secure server bank in Shreveport, LA with nightly off-site backup. The solution means that data is immediately available via Internet connection if the catastrophe is in New York and can be restored within 24 hours if the catastrophe is in Louisiana.

1) HMIS Data System:

- a) HMIS is required to maintain the highest level disaster recovery service by contracting with Wellsky Information Systems to provide Premium Disaster Recovery that includes off-site storage.
- b) Back-up recovery is completed nightly.

- c) Validation of Off-Site storage occurs at least annually.
- 2) Communication between staff of the Lead Agency, the CoC, and the Participating Agencies in the event of a disaster is a shared responsibility and will be based on the type of disaster.
- 3) Agency Emergency Protocols must include:
 - a) Emergency contact information including the names / organizations and numbers of local responders and key internal organization staff, designated representative of the CoC and the HMIS Lead Agency
 - b) Persons responsible for notification and the timeline of notification.
- 4) In the event of System Failure:
 - a) The System Administrator will notify Agency Administrators should a disaster occur at Wellsky Information Systems or in the HAWNY Administrative Offices. Notification will include a description of the recovery plan related time lines.
 - b) After business hours, HMIS staff report System Failures to Wellsky System using the Emergency Contact protocol.
- 5) The System Administrator will notify Wellsky Information Systems if additional database services are required.

V. Data Collection, Types, and Usage

Mandatory Data Collection

Each participating agency is responsible for ensuring that all clients are asked a set of questions which answer HUD or local required data elements.

Besides the required elements, the HMIS Administrator will work with the Agency Administrator to identify the most appropriate assessments to complete. In doing so, the HMIS Administrator will ensure that each program is completing the required data elements as part of their regular client assessments.

System Changes

Any system change(s), i.e. – new required data elements, merging data elements or programs, etc. must be presented to HMIS Advisory Committee for approval. The System Administrator will determine whether HAWNY has the capability to make the changes or contracted out to Wellsky Information Systems or other third party. System Administrator will keep record of all requests and changes made. HMIS documents will be updated as needed to reflect the changes.

Agency/Program Reports:

1. *Self-Generated*

User Agencies can run their own reports using Report Writer or Advance Report Tool (ART). ART requires the purchase of an ART viewer license. Basic Report training is available upon request to HAWNY. User Agencies can only run reports using their own client's data. HAWNY is not responsible for the accuracy of any reports produced by a User Agency.

2. *HAWNY Produced*

The Agency Administrator may request a program report(s) from the HMIS Administrator by email or phone. HAWNY expects requests to be made within a reasonable amount of time of when it is needed.

Release of Data

1. *CoC Reports*

HAWNY will periodically publish public reports about homelessness in the CoC. No confidential client data will be included in these reports. The HMIS Advisory Committee and HAWNY Board of Directors will review reports before being released to the public.

2. *Requests for System Wide Data:*

Any organization or individual who would like to request system wide homeless data must complete a Data Request form and submit it to the HMIS Administrator (see supporting documents). The form will include the purpose of the request, type of data needed, timeframe, etc. HAWNY will attempt to fulfill routine requests in a timely manner. HAWNY has the right to accept or reject any request, i.e. – information requested is at a level of detail we can't provide, or data elements that may not be reliable, etc. If data will be used for publication Homeless Alliance of Western New York (HAWNY) should be credited as the source of the data. The System Administrator will keep record of requests and the information that was provided.

Domestic Violence Dedicated Programs

DV programs are prohibited from participating in HMIS by the Violence Against Women Act (VAWA). Based on funding, DV programs may still be required to use a comparable database. In this case, those programs are responsible for creating/contracting for this database and that it meets regulations. HAWNY will cooperate with these programs to ensure that accurate reporting of aggregate, de-identified data is counted in annual reports.

J. Data Quality Plan

Agencies must require documentation at intake of the homeless status of clients according to the reporting and eligibility guidelines issued by HUD. The order of priority for obtaining evidence of homeless status are

- third party documentation,
- worker observations, and
- certification from the person.

Lack of third-party documentation may not be used to refuse emergency shelter, outreach or domestic violence services.

- a) Clients must be entered into or exited from HMIS within 72 hours of intake or exit from the program.
- b) All staff are required to be trained on the definition of Homelessness.
 - i) HMIS can provide a Homeless Definition to support agency level training if requested. (see Supporting Documents)
 - ii) Documentation of training must be available for audit.
 - iii) There should be congruity between the following HMIS data elements, based on the applicable homeless definition: (Is Client Homeless, Housing Status, Prior Living Situation and Length of stay at prior living situation are being properly completed).
- c) If using paper, the intake/exit data collection forms should correctly align with the HMIS work flow. (HAWNY will provide a template for Participating Agencies, see Supporting Documents)
- d) Agency has a process to ensure that First and Last Names are spelled properly and the DOB is accurate.
 - i) An ID is requested at intake to support proper spelling of the clients name as well as the recording of the DOB.
 - ii) If no ID is available, staff will request the legal spelling of the person's name.
 - iii) Data for clients with significant privacy needs or those who choose not share any data may be entered under the "Un-Named Record" feature of the System. However, while identifiers are not stored using this feature, great care should be taken in creating the Un-Named Algorithm by carefully entering the first and last name and the DOB. Names and ServicePoint Id #s Cross-Walks (that are required to find the record again) must be maintained off-line in a secure location.
- e) HMIS data are being updated when Agency becomes aware of a change when possible, or at minimum annually and at exit
- f) Agencies have an organized exit process that includes:
 - i) Clients and staff are educated on the importance of planning and communicating regarding discharge. This is evidenced through staff meeting minutes or other training logs and records.
 - ii) HMIS provides a Destination Definition Document (see supporting documents) to support proper completion of exits.
 - iii) There is a procedure for communicating exit information to the person responsible for data entry.
- g) System Administrator regularly runs data quality reports.

- i) The System Administrator will distribute a data quality report upon request to all HMIS Participating programs which provides the percentage of missing or unknown/refused required HUD data elements. The agency can also run reports manually to find data issues. The requirement of percentage for missing or unknown/refused entries for each data element is less than 5%.
- ii) The HMIS data collection year is based on the federal fiscal year, 10/1 – 9/30. All data for the data collection year must be complete and accurate no later than 12/31 of that year.
- iii) Data quality screening and correction activities may also include the following:
 - (1) Missing or inaccurate information in Universal Data Element Fields.
 - (2) Un-exited clients using the Length of Stay and Un-exited Client Data Quality Reports.
 - (3) Count reports for proper ratio of children to adults in families. (at least 1.25)
- h) It is recommended that Agencies use HMIS to monitor their performance at least quarterly. HAWNY will provide system-wide performance report annually.

K. Data Timeliness

Participating CoC agencies must accurately enter data within 72 hours of entry/exit of the program or when provided with updated information. The Homeless Alliance of WNY will monitor agencies remotely to ensure these data completeness and timeliness policies are being followed.

All of the documentations related to the HMIS and CoC policies and procedures are available on our website at www.wnyhomeless.org

Reporting Process

1. A ServicePoint User Last Login Report will be run every month. This report shows all user activity for agencies in HMIS. All users must be actively engaged in using HMIS.
2. All projects will also be subjected to random user audits to ensure that data is being entered and HMIS is being used correctly.
3. Client Served Reports:
 - a. For Emergency Shelters, SSO, and Transitional Housing Projects we will run monthly Entry/Exit reports. If the total number of clients served is off by 25% from the previous year, an inquiry e-mail will be sent to the Agency Administrator. The Agency Administrator must write back within 48 hours with an explanation as to why the reported number of clients served does not match the typical number of clients served in previous years.
 - b. For PSH projects we will conduct monthly random checks on a rotating basis. This will consist of Entry/Exit reports of your grant year and spot

checking of client files in HMIS to see if interim reviews and ROI's are being utilized. The Agency Administrator must write back within 48 hours with an explanation as to why the reported number of clients served does not match the typical number of clients served in previous years and explain any discrepancy in client files.

4. For any agency that has not logged in within the past month, an informal inquiry e-mail will be sent to the Agency Administrator. The Agency Administrator must write back within 48 hours as to why ServicePoint has not been utilized within the report time period.
 - a. All agencies must log in to ServicePoint within the last two calendar months. If there has not been any user logged in within two calendar months, a more formal disciplinary action will be taken.

Disciplinary Process

Each agency must be logged in and actively using ServicePoint. The following describes the disciplinary process for not following the agreed upon terms:

- If not logged into HMIS within the last calendar month OR if data is not being entered in a timely manner, an informal inquiry e-mail will be sent. The Agency Administrator must respond within 48 hours.
- If the agency is still not logging into HMIS within the last two calendar months OR if data is still not being entered in a timely manner, an official warning letter will be sent to the Agency Administrator and Executive Director. An official warning letter will also result in a deduction of points for your HMIS score for the CoC competition.
- If an agency receives two warning letters within the calendar year, this will result in a 0 for your HMIS score for the CoC competition.
- If an agency is still not utilizing ServicePoint correctly after two warning letters in a calendar year, a meeting with the Executive Director, Agency Administrator, and applicable HAWNY staff will take place to discuss further discipline. This can include loss of federal CoC funding.

L. HMIS Monitoring

Based on the **HMIS Proposed Rule 580.9 (e)** The Homeless Alliance of WNY is the HMIS Lead and is responsible for monitoring and enforcing compliance by all Covered Homeless Organizations (CHOs) with all the HUD requirements and report on compliance to the Continuum of Care and HUD. Our Agency Participation agreement explicitly states that each agency will be monitored. Each agency will be monitored at minimum every three years.

Monitoring addresses compliance with the following: national objectives; client eligibility; project performance; confidentiality and privacy policies; agency agreements with HAWNY; overall management systems; financial management and audits; adherence to federal grant regulations; client records; records maintenance; anti-discrimination, affirmative action and equal employment opportunity.

All of the documentation related to the HMIS monitoring procedure will be posted on HAWNY's website.

Our objective is to monitor HMIS project recipients to:

- Ensure HMIS Privacy and Security regulations are being met
- Ensure that client records match HMIS client records
- Ensure that projects are meeting national data quality objectives
- Ensure that project's and activities recipient's support operates in a consistent, effective and efficient manner, consistent with the project's intent.

M. HMIS Coordinated Entry

An effective coordinated entry process evaluates and connects those most in need in the community with the most appropriate available resources for their situation as swiftly as possible—the process should be low barrier, housing first oriented, person-centered, and inclusive.

In the coordinated entry process clients are assessed by a standardized survey at the point of entry and are prioritized accordingly. We use HMIS as part of this process. The system is used to:

- Store Assessments
- Run Reports
- Make Referrals

The assessment tool used by HAWNY in HMIS is The Vulnerability Index – Service Prioritization Decision Assistance Tool (VI-SPDAT). The use of this survey can help prioritize which clients should be given a full SPDAT assessment first. Because it is a self-reported survey, no special training is required to use the VI-SPDAT. The VI-SPDAT is used in tandem with local assessment fields to make appropriate and efficient referrals to reduce homeless episodes in accordance with Housing First policy.

N. Grievances

Client Grievances

Clients with a HMIS-related grievance should first identify their concerns to their regular staff member. Upon learning of the grievance, the staff member is required to communicate the concern to their HMIS Agency Administrator for review and possible resolution. The client should also be given the “HMIS Grievance Flow Chart” (available on HAWNY website) which details procedures and contact information.

Each participating agency is responsible for addressing client questions and complaints regarding the HMIS to the best of their ability and in accordance with their agency grievance policies. Possible actions may include further investigation of incidents, clarification or review of policies, or sanctioning of users (if users are found to have violated standards set forth in HMIS agreements or this Standard Operating Procedures Manual). Participating agencies are also obligated to report all HMIS-

related client grievances to the HMIS Administrator using the HMIS Grievance Form (see Section IV. Supporting Documents).

If a client grievance is not satisfactorily resolved at the Agency level, the client may contact the HMIS Administrator who will attempt to resolve the issue. If necessary, the System Administrator will present the problem to the HMIS Advisory Committee at their next meeting. The HMIS Advisory Committee will be given an opportunity to review the details and facts of a situation and will present recommendations towards resolution to the HAWNY Board of Directors. The HAWNY Board of Directors will have final decision-making authority.

Agency Grievances

Any problems related to the operation or policies of HMIS or its participating agencies should be directed to the HMIS Administrator. S/he is responsible for addressing agency-level questions and complaints regarding the HMIS to the best of their ability. Possible actions may include further investigation of incidents, clarification or review of policies, or sanctioning of participating agencies. The HMIS Administrator is also obligated to report all HMIS-related agency grievances to the HMIS Advisory Committee.

If an agency issue is not satisfactorily resolved by the HMIS Administrator, the agency may bring the issue to the HMIS Advisory Committee. The HMIS Advisory Committee will provide information related to the details and facts of a situation to the HAWNY Board of Directors as well as recommendations towards resolution. The HAWNY Board of Directors will have final decision-making authority.

The HMIS Administrator will be responsible for providing a summary of all grievances and their resolutions to the HMIS Advisory Committee on a monthly basis.

HMIS Staff Grievances

Any problems with the HMIS Support Staff should first be reported to the HMIS Administrator. The HMIS Administrator will seek to resolve the issue and will identify staffing concerns to the Executive Director of the Homeless Alliance of Western New York as appropriate.

Any grievances against the HMIS Administrator should be made directly to the Executive Director of the Homeless Alliance of Western New York for resolution.

O. Termination of HMIS Participation

Voluntary Termination

To discontinue participation in HMIS, an agency must submit written notice to the HMIS Administrator. Upon receipt of this written notice, all licenses assigned to that agency will be discontinued within 72 hours.

Involuntary Termination

In the event that the HMIS Advisory Committee decides to terminate an agency from the HMIS, the committee will submit a written notice to the agency's Executive Director identifying a termination date. On that termination date, all licenses assigned to that agency will be discontinued at 5pm, unless an effective date was otherwise established.

Regardless of the reason for termination of participation in HMIS:

- Any costs associated with transferring/exporting data out of the HMIS will be the responsibility of the terminated agency.

HMIS Project Termination

In the event that the HMIS Project ceases to exist, Agencies will be notified and provided reasonable time to access and save Client data on those served by the agency, as well as statistical and frequency data from the entire system. Thereafter, the information collected by the centralized server will be purged or appropriately stored by Wellsky Information Systems.

HAWNY Termination

In the event that HAWNY ceases to exist, the custodianship of the data within HMIS will be transferred by HAWNY to another organization for continued administration. All HMIS Agencies will be informed in a timely manner.