



Homeless Management Information System (HMIS)

Policies and Procedures Manual

November 2009

Table of Contents

| | |
|---|-----------|
| CONTACT INFORMATION..... | 4 |
| HMIS PARTICIPATION POLICY | 5 |
| Responsibilities: | 5 |
| Participation Requirements | 5 |
| Minimum Participation Standards | 6 |
| Participation Expectations and HMIS Agency Agreements | 6 |
| Hardware, Connectivity and Computer Security Requirements | 7 |
| Workstation Specification..... | 7 |
| Internet Connectivity | 7 |
| Security Hardware/Software | 7 |
| Agency Workstation Access Control | 8 |
| HMIS User Implementation | 8 |
| Eligible Users..... | 8 |
| User Requirements | 8 |
| Setting Up a New User | 9 |
| Enforcement Mechanisms | 9 |
| HMIS Agency Implementation | 10 |
| Agency Information Security Protocol Requirements | 10 |
| User Access Levels: | 11 |
| HMIS CLIENT DATA POLICIES AND PROCEDURES | 12 |
| Client Notification Policies and Procedures..... | 12 |
| Definitions and Descriptions of Client Notification and Consent Procedures | 12 |
| Written Client Consent for Alliance Network Data Sharing | 13 |
| Applicability of Consents | 13 |
| Specific Homelessness Prevention Call Center Exception to Written Consent Requirement | 15 |
| Specific Client Notification Procedures for Victims of Domestic Violence | 15 |
| Specific Client Notification Procedures for Unaccompanied Minor Youth..... | 15 |
| Privacy Compliance and Grievance Policy | 15 |
| HMIS DATA QUALITY POLICIES AND PROCEDURES | 16 |
| HMIS Data Quality Plan | 16 |
| Data Quality Standard..... | 16 |
| Data Quality Monitoring | 16 |
| Data Collection Requirements | 17 |
| Data Quality Training | 18 |
| Requirements..... | 18 |
| HMIS Data Access Control Policies..... | 18 |
| User Accounts | 18 |
| User Passwords..... | 19 |

| | |
|--|-----------|
| Password Reset..... | 19 |
| Temporary Suspension of User Access to HMIS | 19 |
| System Inactivity..... | 19 |
| Unsuccessful Login..... | 19 |
| Electronic Data Control..... | 20 |
| Hardcopy Data Control | 20 |
| HMIS De-Duplication Policies and Procedures | 20 |
| De-duplication Data Elements | 20 |
| HMIS Data Ownership Policies | 21 |
| HMIS Data Use and Disclosure Policy and Procedures..... | 22 |
| Privacy Notice Requirement | 22 |
| Alliance Approved Uses and Disclosures | 23 |
| HMIS Data Release Policies and Procedures | 24 |
| Client Identifying Data | 24 |
| Data Release Criteria | 24 |
| Aggregate Data Release Criteria: | 24 |
| Data Release Process | 24 |
| TECHNICAL SUPPORT..... | 25 |
| HMIS Technical Support Policies and Procedures..... | 25 |
| HMIS Application Support..... | 25 |
| User Training..... | 25 |
| Agency/User Forms..... | 26 |
| Report Generation | 26 |
| Programming Related Service Requests | 26 |
| HMIS System Availability Policies | 26 |

Contact Information

THE ALLIANCE TO END HOMELESSNESS IN SUBURBAN COOK COUNTY
1107 S MANNHEIM ROAD, SUITE 304
WESTCHESTER, IL 60154

PHONE: 708-345-4035
FAX: 708-345-7855
WEB: www.suburbancook.org

STAFF AND SUPPORT

JENNIFER HILL

EXECUTIVE DIRECTOR
PHONE: 708-345-4035 x01
EMAIL: jennifer@suburbancook.org

PEGGY TROYER

MANAGER OF INFORMATION SYSTEMS
PHONE: 708-345-4035 x02
EMAIL: peggy@suburbancook.org

JEREMY HEYBOER

DATA AND EVALUATION ADMINISTRATOR
PHONE: 708-345-4035 x03
EMAIL: jeremy@suburbancook.org

SHARON KING

OFFICE MANAGER
PHONE: 708-345-4035
EMAIL: sharon@suburbancook.org

For HMIS technical support please call Peggy or Jeremy.

HMIS Participation Policy

Responsibilities:

Beginning with the 2003 Continuum of Care (CoC) and Emergency Shelter Grants (ESG) and continuing with the Homeless Prevention and Rapid Rehousing Program (HPRP), the United States Department of Housing and Urban Development (HUD) requires all grantees and sub-grantees to participate in their local Homeless Management Information System (HMIS). This policy is consistent with the Congressional Direction for communities to provide data to HUD on the extent and nature of homelessness and the effectiveness of its service delivery system in preventing and ending homelessness. The HMIS and its operating policies and procedures are structured to comply with the most recently released *HUD Data and Technical Standards for HMIS*. Recognizing that the Health Insurance Portability and Accountability Act (HIPAA) and other Federal, State and local laws may further regulate agencies, the Continuum may negotiate its procedures and/or execute appropriate business agreements with Partner Agencies so they are in compliance with applicable laws.

Participation Requirements

Mandated Participation:

All agencies that are funded to provide homeless services by the Alliance to End Homelessness in Suburban Cook County (the Alliance) must meet the minimum HMIS participation standards as defined by this Policy and Procedures manual. These participating agencies will be required to comply with all applicable operating procedures and must agree to execute and comply with an HMIS Agency Partner Agreement.

Voluntary Participation

Although funded agencies are only required to meet minimum participation standards, the Alliance strongly encourages funded agencies to fully participate with all of their homeless programs.

While the Alliance cannot require non-funded providers to participate in the HMIS, the Alliance works closely with non-funded agencies to articulate the benefits of the HMIS and to strongly encourage their participation in order to achieve a comprehensive and accurate understanding of homelessness in suburban Cook County.

Minimum Participation Standards

- ⇒ Collect the universal data elements, as defined by HUD, for all programs operated by the agency that primarily serve persons who are homeless or formerly homeless;
- ⇒ Collect program-specific data elements, as defined by HUD, for all clients served by programs funded by the Alliance to End Homelessness.
- ⇒ Enter client-level data into the HMIS within five working days of client interaction.
- ⇒ Comply with all HUD regulations for HMIS participation.

The Alliance uses all submitted data for analytic and administrative purposes, including the preparation of Alliance reports to funders and the Continuum's participation in the Federal Annual Homeless Assessment Report (AHAR).

Participation Expectations and HMIS Agency Agreements

Agencies that receive funding from the Alliance must meet specific funding requirements related to data submittal.

- ⇒ Authorized agency users directly enter client-level data into the HMIS database. Users have rights to access data for clients served by their agency and use HMIS functionality based on their user level privileges. The agency's data are stored in the HMIS central database server, which is protected by numerous technologies to prevent access from unauthorized users. Unless a client requests that his/her identifiers remain hidden at the time that his/her record is created, or if the program serves clients that require a heightened level of privacy protection, primary client identifiers (e.g. name, SSN, DOB and gender) will be available for query by HMIS users from partner agencies to prevent the duplication of client records in the database. However, other individual client data will not be accessible by HMIS users from other agencies outside of the client notification and interagency data sharing procedures.
- ⇒ When a client is not willing to share any of his/her identifying information, or if the program serves clients that require a heightened level of privacy protection, the client record should be completely closed at the time that his/her record is created. All individual client data then remains hidden and is not accessible to HMIS users from other agencies. The de-duplicating of records takes place at the server level. Agencies are responsible for identifying and ensuring unduplicated client analysis at the agency level.
- ⇒ Each agency shall designate at least one Agency Administrator who is the agency's point person/specialist regarding HMIS. The Agency Administrator is responsible for organizing its agency's users, making sure proper training has taken place for the

users and that all paperwork and confidentiality requirements are being followed by all users from that agency.

- ⇒ HMIS Management Team consists of the Manager of Information Systems and the Data and Evaluation Administrator who work for the Alliance to End Homelessness in Suburban Cook County. They organize training, provide technical assistance and on-site help when needed.

Hardware, Connectivity and Computer Security Requirements

Workstation Specification

Computers should meet the **minimum** desktop specification:

- ⇒ Operating System: Any system capable of running a current Internet browser as specified below
- ⇒ Processor: 2 GHz Pentium processor or higher
- ⇒ Memory: 512MB RAM
- ⇒ Hard Drive: 40 MB available space
- ⇒ Web Browsers: The most current version of MS Internet Explorer or Mozilla Firefox

Internet Connectivity

Partner Agencies must have Internet connectivity for each workstation accessing the HMIS. To optimize performance, all agencies are encouraged to secure a high speed Internet connection with a cable modem, DSL, or T1 line. Agencies expecting a very low volume of data may be able to connect using a dial-up connection; however, HMIS management cannot guarantee satisfactory performance with this option.

Security Hardware/Software

All workstations accessing the HMIS need to be protected by a Firewall. If the workstations are part of an agency computer network, the Firewall may be installed at a point between the network and the Internet or other systems rather than at each workstation. Each workstation also needs to have anti-virus and anti-spyware programs in use and properly maintained with automatic installation of all critical software updates. Good examples of anti-virus software include McAfee and Symantec (Norton) Security systems, among others.

Agency Workstation Access Control

Access to the HMIS will be allowed only from computers specifically identified by the Partner Agency's Executive Director or authorized designee and HMIS Agency Administrator. Laptop computers will require an additional security statement indicating that they will not be used for unauthorized purposes from unauthorized locations. Access to these workstations will be controlled through both physical security measures and a password. Each agency's HMIS Agency Administrator will determine the physical access controls appropriate for their organizational setting based on HMIS security policies, standards and guidelines. Each workstation, including laptops used off-site, should have appropriate and current firewall and virus protection as specified above under *Security Hardware/Software*.

HMIS User Implementation

Eligible Users

Each Partner Agency shall authorize use of the HMIS only to users who need access to the system for data entry, editing of client records, viewing of client records, report writing, administration or other essential activity associated with carrying out participating agency responsibilities.

The HMIS Management Team shall authorize use of the HMIS only to users who need access to the system for technical administration of the system, report writing, data analysis and report generation, back-up administration or other essential activity associated with carrying out central server responsibilities.

User Requirements

Prior to being granted a username and password, users must sign an HMIS confidentiality agreement that acknowledges receipt of a copy of the agency's privacy notice and that pledges to comply with the privacy notice.

Users must be aware of the sensitivity of client-level data and must take appropriate measures to prevent its unauthorized disclosure. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with all policies and standards described within this Policies and Procedures Manual. They are accountable for their actions and for any actions undertaken with their username and password.

Agency Administrators must ensure that users have received adequate training prior to being given access to the database.

Setting Up a New User

If the Partner Agency wants to authorize system use for a new user, the agency's Executive Director or authorized designee must:

- ⇒ Determine the access level of the proposed HMIS user; and
- ⇒ Execute an HMIS user confidentiality agreement

The Agency Administrator must:

- ⇒ Review HMIS records about previous users to ensure that the individual does not have previous violations with the HMIS Policies and Procedures that prohibit their access to the HMIS;
- ⇒ Verify that an HMIS user confidentiality agreement has been correctly executed;
- ⇒ Verify that appropriate and sufficient training has been successfully completed; and
- ⇒ Create the new user ID and password in ServicePoint.

Once the user ID is established, the Agency Administrator is responsible for maintaining the user account. If any user leaves the agency or no longer needs access to the HMIS, the Agency Administrator is responsible for immediately terminating user access by deleting or inactivating the user account.

Volunteers have the same user requirements that paid staff have. They must have an individual user account, go through the same training, and have the same confidentiality and privacy documents signed and on file with the agency they are serving.

The Executive Director or authorized designee is responsible for ensuring that the user understands and complies with all applicable HMIS policies and procedures.

Enforcement Mechanisms

The HMIS Management Team will investigate all potential violations of any security protocols. Any user found to be in violation of security protocols will be sanctioned.

Sanctions include, but are not limited to:

- ⇒ A formal letter of reprimand
- ⇒ Suspension of system privileges
- ⇒ Revocation of system privileges

A Partner Agency's access may also be suspended or revoked if serious or repeated violation(s) of HMIS Policies and Procedures occur by agency users.

HMIS Agency Implementation

Prior to setting up a new Partner Agency within the HMIS database, the HMIS System Administrator shall:

- ⇒ Review HMIS records to ensure that the agency does not have previous violations with the HMIS Policies and Procedures that will prohibit their access to the HMIS;
- ⇒ Verify that the required documentation has been correctly executed and submitted or viewed on site, including:
 - Certification of Initial Implementation Requirements;
 - Partner Agreement;
 - Information Security Protocol;
 - Additional Documentation on Agency and Program(s);
 - Designation of Agency Administrator; and
 - Fee Payment, if applicable
- ⇒ Request and receive approval from the HMIS Management Team to setup a new agency;
- ⇒ Work with the Agency Administrator to input applicable agency and program information; and
- ⇒ Work with HMIS Management Team to migrate legacy data, if applicable.

Agency Information Security Protocol Requirements

At a minimum, Partner Agencies must develop rules, protocols or procedures to address the following:

- ⇒ Internal agency procedures for complying with the HMIS Notice of Privacy Practices and provisions of other HMIS client and agency agreements;
- ⇒ Maintaining and posting an updated copy of the agency's Notice of Privacy Practices on the agency's website;
- ⇒ Posting a sign in the areas of client intake that explains generally the reasons for collecting personal information;
- ⇒ Appropriate assignment of user accounts;
- ⇒ Preventing user account sharing;
- ⇒ Protection of unattended workstations;
- ⇒ Protection of physical access to workstations where employees are accessing HMIS;
- ⇒ Safe storage and protected access to hardcopy and digitally generated client records and reports with identifiable client information;

- ⇒ Proper cleansing of equipment prior to transfer or disposal; and
- ⇒ Procedures for regularly auditing compliance with the agency's information security protocol.

User Access Levels:

All HMIS users must be assigned a designated user access level that controls the level and type of access the user will have within the system. Each user will have access to client-level data only that is collected by their own agency unless a client specifically consents in writing to share their information.

HMIS Client Data Policies and Procedures

Client Notification Policies and Procedures

The Alliance has prepared standard documents for HMIS Notice of Privacy Practices and Client Consent to Release Information. Partner Agencies may either use these forms or incorporate the content of the HMIS documents in their entirety into the agency's own documentation. All written consent forms must be stored in a client's case management file for record keeping and auditing purposes.

Agencies must make reasonable accommodations for persons with disabilities throughout the data collection process. This may include, but is not limited to, providing qualified sign language interpreters, readers, or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability.

Agencies that are recipients of federal assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the program.

Definitions and Descriptions of Client Notification and Consent Procedures

Client Notice

A written notice of the assumed functions of the HMIS must be posted and/or given to each client so that he/she is aware of the potential use of his/her information and where it is stored. No consent is required for the functions articulated in the notice. However, as part of the notification process, clients must be informed of their right to designate their client records as hidden/closed. The client also has a right to view a copy of his/her record upon request. To fulfill this requirement, the agency may either adopt the HMIS Notice of Privacy Practices or may develop an equivalent Privacy Notice that incorporates all of the content of the standard HMIS Notice. If the agency has a website, the adopted Notice of Privacy Practices or equivalent privacy notice must also be posted on the website.

Hidden/Closed Client Record

After learning about the HMIS, if a client does not wish to have his/her Primary Identifiers accessible to all HMIS users, the originating HMIS user should close the client record by locking the security setting on the client screen. Closing a client record will

allow the agency to access the client's information for agency purposes. This action will allow HMIS System Administrators to view client-identifying information, but will prevent any personal client-identifying information from being accessed by HMIS users outside of the originating agency.

Written Client Consent for Alliance Network Data Sharing

At the initial intake, the Client should be provided an oral explanation and written documentation about the option of sharing his/her Information within the Alliance HMIS.

If a client is interested in sharing his/her information within the HMIS, he/she must provide written consent (see exception below for Homelessness Prevention Call Center). The consent must be specific regarding:

- ⇒ Purpose,
- ⇒ The expiration of the sharing,
- ⇒ Affected data elements,
- ⇒ Function, and
- ⇒ Involved parties.

The client maintains a right to revoke written authorization at any time, in which case, any currently shared information will become non-shared from that point forward. To fulfill this requirement, the agency may adopt the Alliance's "Client Revocation Form" or may develop an internal form that incorporates the content of the Alliance's form.

Client Authorization

HMIS Users may share client information only if the client authorizes that sharing with a valid Client Release of Information form.

Authorized users will be able to grant permission based on appropriate client consent to share individual client information with another agency's users. Random file checks for appropriate client authorization, audit trails, and other monitoring tools may be used to monitor that this data sharing procedure is followed. Specific monitoring procedures around program enrollment will be implemented to ensure appropriate client information access.

Applicability of Consents

The Partner Agency shall uphold Federal and State Confidentiality regulations to protect client records and privacy. If an agency is covered by the Health Insurance Portability and Accountability Act (HIPAA), the HIPAA regulations prevail.

The table below summarizes the client data categories and the related notification/consent rules that relate to each data category. These minimum procedures should not imply that all providers would perform all of these functions.

| Client Data Categories | Summary of Notification/Consent and Data Sharing Procedures |
|--|--|
| <p>Primary Identifiers:</p> <ul style="list-style-type: none"> • Name and Aliases • Birth Date • Gender • Social Security Number | <p><u>Open Client record</u>: If the client does not ask to hide his/her identifiers, the primary identifiers will be available to all HMIS users in the Client Search to locate an existing client. None of the other client information will be viewable, except as described below.</p> <p><u>Closed Client record</u>: If a client asks to hide his/her primary identifiers, the record will appear on the Client Search List only for the originating agency. It will be hidden to all other agencies. Some system-level users will have access to hidden records for system administration purposes.</p> |
| <p>General Client Information (Shared Cook County MDR assessment screen):</p> <ul style="list-style-type: none"> • Ethnicity • Race • Veteran status and information • Family/Relationship Information • Housing History • Non-confidential notes • Services Provided | <p><u>Open Assessment</u>: With a signed release of information (ROI), these data can be shared with HMIS users from partner agencies by opening/unlocking the Shared Cook County MDR assessment.</p> <p><u>Closed Assessment</u>: If written consent is not provided, this information is accessible only within the originating agency and some system-level users for system administration purposes.</p> |
| <p>Protected Information:</p> <ul style="list-style-type: none"> • Disability information • Mental Health Assessment • Substance Abuse Assessment • HIV/AIDS Information • Domestic Violence Information | <p><u>Protected Information</u>: Generally, this information is available only within the originating agency to users that have an authorized access level and to authorized, system-level users for system administration purposes. Any other sharing of this data should be limited to specific partner agencies as a closed exception and requires signed consent from the client.</p> |

Specific Homelessness Prevention Call Center Exception to Written Consent Requirement

The Homelessness Prevention Call Center will not be required to obtain written consent to share primary and general client information collected primarily through telephonic or other electronic means. However, all clients must be informed of their right to participate in HMIS. Clients will be read the Call Center Consent and Notifications script. Clients can view the Privacy Notice on the Call Center website or pick up a copy at the Call Center. Callers who do not want their information shared in HMIS will have their records closed and may be limited in their ability to obtain an agency referral.

Specific Client Notification Procedures for Victims of Domestic Violence

A mainstream agency that is serving a victim of domestic violence must explain the potential safety risks for domestic violence victims and the client's specific options to protect her/his data, such as designating her/his record as hidden/closed to other agencies. Thus, the client notification form must clearly state the potential safety risks for domestic violence victims and delineate the information sharing options. All staff must be trained on the protocol for educating domestic violence victims about their individual information sharing options.

Specific Client Notification Procedures for Unaccompanied Minor Youth

Based on their age and potential inability to understand the implications of sharing information, the HMIS cannot be used to share information about unaccompanied minor youth outside of the originating agency. Thus even with written client authorization, users cannot share any client information of unaccompanied minor youth. For the purposes of this policy, minor youth are defined as youth under 18.

Privacy Compliance and Grievance Policy

Partner Agencies must establish a regular process of training users on this policy, regularly auditing that the policy is being followed by agency staff (including employees, volunteers, affiliates, contractors and associates), and receiving and reviewing complaints about potential violations of the policy. Agencies may want to appoint a Chief Privacy Officer to be responsible for these tasks.

HMIS Data Quality Policies and Procedures

HMIS Data Quality Plan

The Continuum has defined a data quality plan that:

- Specifies the data quality standard to be used by all participating agencies;
- Provides a mechanism for monitoring adherence to the standard;
- Provides the necessary tools and training to ensure compliance with the standard; and
- Includes strategies for working with agencies who are not in compliance with the standard.

Data Quality Standard

- All names will be accurate
- Blank entries in required data fields will not exceed 5% per month
- All services provided will be compatible with providing program
- Data entry must be complete within five working days of data collection

Data Quality Monitoring

The System Administrator will perform regular data integrity checks on the HMIS data. Any patterns of error at a Partner Agency will be reported to the Agency Administrator. When patterns of error have been discovered, users will be required to correct data entry techniques and will be monitored for compliance.

- Run Universal Data Element (UDE) Completeness Reports, Data Incongruities Reports, and other data quality reports as appropriate.
- Notify Agency Administrator of findings and timelines for correction.
- Rerun reports for errant agencies/programs. Follow up with Agency Administrators if necessary.
- Create notification for Agency Executive Director and submit to Alliance Manager of Information Systems for approval.

Data Collection Requirements

Universal Data Elements

A Partner Agency is responsible for ensuring that a minimum set of data elements, referred to as the Universal Data Elements (UDE's) as defined by the *HUD Data and Technical Standards*, will be collected and/or verified from all clients at their initial program enrollment or as soon as possible thereafter. Partner Agencies are required to enter data into the HMIS within five days of collecting the information.

The UDE's are all included collectively on the Client Profile, SubCook Shared MDR Assessment, and SubCook HUD 40118 Entry and Exit assessments, which are on the ServicePoint Entry and Exit screens, respectively.

Partner Agencies must report client-level UDE's using the required response categories detailed in the "Required Response Categories for Universal Data Elements" section of the *HUD Data and Technical Standards*. These standards are already incorporated into the HMIS.

Program-Specific Data Elements

All Partner Agencies are also responsible for ensuring that the Program-specific Data Elements, as defined by the *HUD Data and Technical Standards*, are collected from all clients that are served by applicable HUD funded programs. These Program-specific Data Elements are required to be entered into the HMIS within five working days of collecting the information.

Partner Agencies must provide client-level data for the Program-specific Data Elements using the required response categories detailed in the "Required Response Categories for Program-specific Data Elements" section of the *HUD Data and Technical Standards*. These standards are already incorporated into the HMIS.

The Program-specific Data Elements are located in the SubCook HUD 40118 Entry and Exit assessments, which are on the ServicePoint Entry and Exit screens, respectively.

Data Quality Training

Requirements

End-User Training

Each end user of the HMIS system must complete at least one (1) day of training with the Alliance before being given HMIS login credentials. It is preferred they receive more training from their Agency Administrator in order to understand Agency Specific nuances in how they enter data. Agency Administrators should notify the Alliance when they have specific training needs.

Agency Administrator

Each Agency Administrator must complete a second day of training after completing End-User training. This second day of training will include how to configure and manage an Agency's programs and users in the HMIS systems. It is preferred they also attend a reports training soon thereafter.

Reports Training

Reports training for Agency Administrators and other interested users will be made available as needed. These will include training on how to use existing canned reports in ServicePoint's ReportWriter and may include opportunities for training on ART-Advanced Reporting Tool (this may include Viewer licenses or ad-hoc licenses).

Alliance staff encourages Agencies to run their own data quality reports so that Agencies can monitor their own data quality and become more effective in serving our clients across the Continuum.

HMIS Data Access Control Policies

User Accounts

Agency Administrators are responsible for managing user accounts for their Agency. They must follow the procedures documented in the *HMIS User Implementation* section for user account set-up including verification of eligibility, the appropriate training, and the establishment of appropriate user type. The assigned user type will determine each user's individual access level to data, and Agency Administrators must regularly review user access privileges.

The Agency Administrator is responsible for removing users from the system. They should discontinue the rights of a user immediately upon that user's termination from any position with access. When a user will be on leave for an extended period (longer

than 30 days), his/her account should be temporarily suspended within 5 business days from the start of their leave.

User Passwords

Each user will be assigned a unique identification code (User ID), preferably the first initial and last name of the user.

A temporary password will be automatically generated by the system when a new user is created. The Agency Administrator should communicate the system-generated password to the user. The user will be required to establish a new password upon their initial log-in. This password will need to be changed every 45 days. A password cannot be used again until another password has expired. Passwords should be between 8 and 16 characters long, contain at least two numbers, and should not be easily guessed or found in a dictionary. The password format is alphanumeric and is case-sensitive.

Users are prohibited from sharing passwords—even with supervisors. Sanctions will be imposed on the user and/or agency if user account sharing occurs. Any passwords written down should be securely stored and inaccessible to others. They should not be saved on a personal computer.

Password Reset

Except when prompted by ServicePoint to change an expired password, users cannot reset their own password. The Agency Administrator and the Alliance System Administrator have the ability to temporarily reset a password. If an Agency Administrator needs to have his/her password set, the Alliance System Administrator will need to reset that password.

Temporary Suspension of User Access to HMIS

System Inactivity

Users must logoff from the HMIS application and their workstation if they leave the workstation. Also, HUD requires password protected screen-savers on each workstation. If the user is logged onto a workstation and the period of inactivity on that workstation exceeds 30 minutes, the user will be logged off the system automatically.

Unsuccessful Login

If a user unsuccessfully attempts to log in 4 times, the User ID will be “locked out”, their access permission will be revoked and they will be unable to regain access until their User ID is reactivated by the Agency Administrator or Alliance System Administrator.

Electronic Data Control

Agency Policies Restricting Access to Data

Partner agencies must establish protocols limiting internal access to data based on the final HUD Data and Technical Standards.

Raw Data

Users who have been granted access to the HMIS Report Writer tool have the ability to download and save client level data onto their local computer. Once this information has been downloaded from the HMIS server in raw format to an agency's computer, this data then becomes the responsibility of the agency. Any such data files should be password protected.

Ability to Export Agency Specific Data from the HMIS

Partner Agencies will have the ability to export a copy of their own data for internal analysis and use. Agencies are responsible for the security of this information.

Hardcopy Data Control

Printed versions (hardcopy) of confidential data should not be copied or left unattended and open to compromise. Media containing HMIS client identified data will not be shared with any agency, other than the owner of the data, for any reason. Authorized employees using methods deemed appropriate may transport HMIS data between the participating agencies that meet the above standard. Reasonable care should be taken, and media should be secured when left unattended. Magnetic media containing HMIS data which is released and/or disposed of by the participating agency and the central server should first be processed to destroy any data residing on that media. Degaussing and overwriting are acceptable methods of destroying data. HMIS information in hardcopy format should be disposed of properly. This could include shredding finely enough to ensure that the information is unrecoverable.

HMIS De-Duplication Policies and Procedures

De-duplication Data Elements

The HMIS application will use the following data elements to create unduplicated client records:

- Name (first, middle, last, suffix; aliases or nicknames should be avoided);
- Social Security Number;
- Date of Birth (actual or estimated);
- Race and Ethnicity.

User-mediated Look-up

The primary way to achieve de-duplication will be a user-mediated search of the client database prior to creating a new client record. The user will be prompted to enter a minimum number of the data elements into the HMIS application and a list of similar client records will be displayed. Based on the results, the user will be asked to select a matching record if the other identifying fields match correctly.

If the user is unsure of a match (either because some data elements differ or because of blank information), the user should query the client for more information and continue evaluating possible matches or create a new client record.

The user will not be able to view sensitive client information, or program-specific information, during the de-duplication process. After the client record is selected, the user will be able to view previously existing portions of the client record only if they have explicit authorization to view that client's record.

Back-end Central Server Matching Based on Identifiable Information: When Primary Identifiers are not shared across agencies for de-duplication purposes, the Alliance System Administrator with the assistance of the Agency Administrator will manage a process for matching a client's personal identifying information based on a unique client identifier that is assigned by the HMIS to each client. The unique client identifier provides an unduplicated internal count of clients served by the Agency, and provides the HMIS Management Team the means of conducting longitudinal analysis of services provided to each client.

This scenario will be used to de-duplicate hidden client records. The process will also be used to validate data received from all users, as human decisions and misjudgments may introduce error to the provider-mediated look-up process.

HMIS Data Ownership Policies

The client ultimately retains ownership of any identifiable client-level information that is stored within the HMIS. If the client consents to share data, the client, or agency on behalf of the client, has the right to later revoke permission to share data without affecting the client's right to service.

In the event that the relationship between the Alliance HMIS and a Partner Agency is terminated, the agency will retain ownership of the identifiable client-level data that has been submitted to the HMIS. In this circumstance, any agency-entered client-level data must be de-identified in order to remain in the HMIS database. This de-identified information shall remain available to the Alliance for analytical purposes.

For the purposes of de-identification, the personal identification number shall not be considered an identifying data element if it is not stored with any other personal identifiers.

The HMIS Management Team shall make reasonable accommodations to assist a Partner Agency to export their data in a format that is usable in their alternative database.

HMIS Data Use and Disclosure Policies and Procedures

Each of the HMIS Partner Agencies must comply with the following uses and disclosures, as outlined in the *HUD Data and Technical Standards: Notice for Uses and Disclosures for Protected Personal Information (PPI)*. A Partner Agency has the right to establish additional uses and disclosures as long as they do not conflict with the Alliance approved uses and disclosures.

Privacy Notice Requirement

Each Partner Agency must publish a privacy notice that incorporates the content of the *HUD Data and Technical Standards Notice* as described below. Agencies that develop their own privacy and security policies must allow for the de-duplication of homeless clients at the Continuum level.

Each agency must post the privacy notice and provide a copy of the privacy notice to any client upon request. If an agency maintains a public web page, the agency must post the current version of its privacy notice on its web page.

An agency's privacy notice must:

- ⇒ Specify all potential uses and disclosures of a client's personal information;
- ⇒ Specify the purpose for collecting the information;
- ⇒ Specify the time period for which a client's personal information will be retained at the agency;
- ⇒ Specify the method for disposing of a client's personal information or removing identifiers from personal information that is not in current use seven years after it was created or last changed;
- ⇒ State the process and applicability of amendments, and commit to documenting all privacy notice amendments;
- ⇒ Offer reasonable accommodations for persons with disabilities and/or language barriers throughout the data collection process;
- ⇒ Allow the individual the right to inspect and to have a copy of their client record and offer to explain any information that the individual may not understand; and

- ⇒ Specify a procedure for accepting and considering questions or complaints about the privacy and security policies and practices.

Alliance Approved Uses and Disclosures

Identifiable HMIS client data may be used or disclosed for case management, billing, administrative and analytical purposes.

- ⇒ Case management purposes include uses associated with providing or coordinating services for a client. As part of case management, the agency will only share client information with other agencies based on written client consent, or in the case of the Homelessness Prevention Call Center, explicit oral consent.
- ⇒ Billing uses include functions related to payment or reimbursement for services. An example might include generating reports for fund raising purposes.
- ⇒ Administrative purposes are uses required to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions. An example would be analyzing client outcomes to evaluate program effectiveness.
- ⇒ Analytical purposes are functions that are related to analyzing client data to understand homelessness, including but not limited to creating de-identified protected personal information, understanding trends in homelessness and the needs of persons who are homeless, and assessing the implementation of the Continuum's 10-Year Plan to End Homelessness.

Unless a client requests that his/her record remains hidden, his/her primary identifiers will be disclosed to other HMIS agencies. This will allow agencies to locate the client within the HMIS system when the client comes to them for services. This will allow the Alliance to determine how many people are homeless in suburban Cook County during any specified timeframe.

Identifiable client information may also be used, or disclosed, in accordance with the *HUD Data and Technical Standards* for:

- Uses and disclosures required by law
- Aversion of a serious threat to health or safety
- Uses and disclosures about victims of abuse, neglect or domestic violence
- Uses and disclosures for academic research purposes
- Disclosures for law enforcement purposes in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial office or a grand jury subpoena.

Aside from the disclosures specified above, a client's protected personal information will be disclosed only with their written consent.

Client information will be stored with personal identifiers for a period of seven years from the time it was last modified. Beyond that point, client information will be retained only in a de-identified format.

HMIS Data Release Policies and Procedures

Client Identifying Data

No identifiable client data will be released to any person, agency, or organization that is not the owner of said data for any purpose other than those specified in the *HMIS Data Uses and Disclosure Policies and Procedures* section without the written permission of the owner.

Data Release Criteria

HMIS client data will be released only in aggregate, or in anonymous client-level data formats, for any purpose beyond those specified in the *HMIS Data Uses and Disclosures Policies and Procedures* section, according to the criteria specified below,

Aggregate Data Release Criteria

All data must be anonymous, either by removal of all identifiers and/or all information that could be used to infer an individual or household identity. Aggregate data must represent sixty percent (60%) of the total clients being served by the Alliance (program, agency, subpopulation, geographic area, etc.), unless otherwise required for the Congressional Annual Homeless Assessment Report (AHAR).

Only Partner Agencies can authorize release of aggregate program-specific information beyond the standard reports compiled by the Alliance for funding purposes. There will be full access to aggregate data for all participating agencies.

Parameters of the release of aggregate data (i.e., where the data comes from, what it includes and what it does not include) will be presented to each requestor of aggregate data.

Released aggregate data will be made available in the form of an aggregate report, and/or a raw dataset.

Data Release Process

Beyond individual agency reports, or Alliance reports on its funded programs, the Director of the Alliance to End Homelessness in Suburban Cook County must approve all data for public classification and release.

Technical Support

HMIS Technical Support Policies and Procedures

HMIS Application Support

As unanticipated technical support questions on the use of the HMIS application arise, users will follow this procedure to resolve those questions:

During the normal business hours of the Alliance:

- ⇒ Begin with utilization of the on-line help and/or training materials;
- ⇒ If the question is still unresolved, direct the technical support question to the Agency Administrator;
- ⇒ If the question is still unresolved, the Agency Administrator can direct the question to the Alliance HMIS System Administrator; and
- ⇒ If the question is still unresolved, the Alliance HMIS System Administrator will direct the question to Bowman Systems technical support staff.

After the normal business hours of the Alliance:

- ⇒ Begin with utilization of the on-line help and/or training materials;
- ⇒ If the question can wait to be addressed during the following business day, wait and follow the normal business hours procedure outlined above;
- ⇒ If the question cannot wait, direct the technical support question to the Agency Administrator, if available; and
- ⇒ If unavailable, and the question is still unresolved, contact the Alliance HMIS Technical Administrator, or the duly appointed representative. They will determine the appropriate procedure to be followed.

If it is determined that the issue needs immediate attention, the user's request will be forwarded to an appropriate Bowman Systems HMIS technical support representative. Otherwise, the user will be instructed to pursue assistance through normal channels on the following business day.

User Training

The HMIS Management Team will provide HMIS application training periodically throughout the year. If additional, or specific, training needs arise, the HMIS Coordinator may arrange for special training sessions.

Agency/User Forms

All Agency Administrators will be trained in the appropriate on-line and hardcopy forms. If the Agency Administrator has questions on how to complete HMIS forms, they shall contact the HMIS System Administrator.

Report Generation

Each Agency may send its Agency Administrator to receive training on how to develop agency-specific reports using the HMIS application. The HMIS System Administrator will be a resource to agency users as they develop reports but will be available only to provide a limited, reasonable level of support to each Agency.

The HMIS User Group will be the primary body to query Partner Agencies on their reporting needs and to prioritize a list of reports to be developed by the Alliance for use by all Partner Agencies.

Programming Related Service Requests

If a user encounters programming issues within the HMIS application that need to be addressed, that user should identify the error, or suggest an improvement, to their Agency Administrator. The Agency Administrator will forward this information to the HMIS System Administrator, identifying the specific nature of the issue or recommended improvement, along with the immediacy of the request.

The HMIS System Administrator will review all application service requests and determine the action to be taken. Requests to fix programming errors will be prioritized and forwarded to the HMIS Management Team. Suggested application improvements will be compiled and periodically discussed by the HMIS Committee and the HMIS User Group. A prioritized list of improvements will be submitted to the HMIS Management Team for review. Approved recommendations will be submitted to Bowman Systems.

HMIS System Availability Policies

There are times that ServicePoint is unavailable because Bowman Systems is performing necessary backup and maintenance of the HMIS database. These are usually in the late evenings when as few people as possible need access to the system. However, when the Alliance receives notice of a planned interruption of service for other reasons or for an abnormal amount of time, the HMIS Management Team will notify Agency Administrators via email. If there is an unplanned interruption to service, the HMIS System Administrator will communicate with Bowman Systems, and Agency Administrators will be notified of any information regarding the interruption as it is made available.