Homeless Management Information System (HMIS)

Policies and Procedures Manual

December 20, 2019

Table of Contents

Contact Information

The Alliance to End Homelessness in Suburban Cook County

4415 Harrison St, Suite 228
Hillside, IL 60162
Phone: 708-236-3261
Fax: 708-236-3299
Web: www.suburbancook.org

HMIS Staff

Peggy Troyer

Director of Information Services
Phone: 708-236-3261 x2#
Email: peggy@suburbancook.org

Jeremy Heyboer

Senior Data Analyst
Phone: 708-236-3261 x3#
Email: jeremy@suburbancook.org

Lynn Suchwalko

System Implementation Manager
Phone: 708-236-3261 x7#
Email: lynn@suburbancook.org

Erin Matheny

HMIS Policy and Training Manager
Phone: 708-236-3261 x10#
Email: erin@suburbancook.org

For HMIS technical support, please submit a request through the NIL HMIS Support Ticketing system or *directly contact a member of the HMIS Team.*

Homelessness Management Information System
Policies and Procedures Manual

This manual is developed by the HMIS Committee and authorized by the Board of Directors of the Alliance to End Homelessness in Suburban Cook County

HMIS Governance Charter

Introduction

The Alliance to End Homelessness in Suburban Cook County (Alliance) is the lead agency and Collaborative Applicant for the Cook County Continuum of Care (CoC, IL-511) as well as the designated lead agency for the Cook County Homeless Management Information System (HMIS). The coverage area for both the CoC and the HMIS includes all municipalities in Cook County, Illinois except for the City of Chicago. The Alliance has primary responsibility for all HMIS activities.

The HMIS Governance Charter serves to delineate the roles and responsibilities related to key aspects of the governance and operations of the Cook County HMIS and includes the most recent *HMIS Policies and Procedures Manual* (Policy) approved and adopted by the Alliance, which is incorporated into this charter by reference. The Policy includes privacy, security, client consent and data entry requirements and may be modified from time to time at the Alliance's discretion.

Beginning with the 2003 Continuum of Care (CoC) grants and continuing with the Emergency Solutions Grants (ESG), 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. 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.

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 reporting requirements. Aggregate data taken from the HMIS is used to inform Strategic Planning activities and the Consolidated Plans of Cook County and other entitlement communities.

KEY SUPPORT ROLES & RESPONSIBILITIES

Alliance to End Homelessness in Suburban Cook County (Alliance) – Board of Directors

As lead agency for the Cook County Continuum of Care (CoC):

- ⇨ Designates the HMIS lead agency, oversees the HMIS project and has primary responsibility for all HMIS activities
- ⇨ Ensures HMIS compliance with all HUD rules and regulations
- ⇨ Encourages and facilitates participation
- ⇨ Approves and facilitates enforcement of HMIS policies as set forth in the *HMIS Policies and Procedures Manual*
- ⇨ Appoints the HMIS committee
- ⇨ Designates software to be used for the HMIS in the geographic region
- ⇨ Selects, approves and executes annual contract(s) with HMIS vendor(s)

HMIS Committee

- ⇨ Guides the implementation of the Homeless Management Information System
- ⇨ Develops, informs and reviews HMIS policies and procedures
- ⇨ Advises and recommends to the CoC board changes to HMIS policies and procedures
- ⇨ Cultivates ways in which future data measurement can contribute to fulfillment of strategic goals
- ⇨ Is appointed by the Alliance board of directors

HMIS Management Team

- ⇨ Consists of the HMIS Lead Agency staff, including the Director of Information Services and system support staff
- ⇨ Authorizes/makes decisions regarding day-to-day operations
- ⇨ Ensures compliance with HMIS policies and HUD requirements, including conditions identified by the Security, Privacy, and Data Quality Plans of the *HMIS Policies and Procedures Manual*
- ⇨ Acts as liaison between the Alliance and regional or national HMIS related organizations and participates in related activities
- ⇨ Supervises contract(s) with vendor(s)
- ⇨ Provides training and support to partner agency users
- ⇨ Cross-trains staff and develops process documentation for improving knowledge transfer and support of HMIS

- ⇨ Facilitates continuing quality improvement via data analyses and knowledge of best practices
- ⇨ Supports data collection and management protocol, reporting, and security structures for the CoC's Coordinated Entry system

HMIS Partner Agencies

- ⇨ Execute an *HMIS Agency Partner Agreement* and an *Inter-Agency Data Sharing Memorandum of Agreement ("MOA") for Housing and Service Coordination*
- ⇨ Agree to abide by the most current *HMIS Policies and Procedures Manual* approved and adopted by the CoC
- ⇨ Ensure that all employees and agents comply with the most current *HMIS Policies and Procedures Manual*
- ⇨ Ensure staffing and equipment necessary to implement and ensure HMIS participation, in accordance with the *HMIS Policies and Procedures Manual*

HMIS Primary Point Persons/Agency Administrators

- ⇨ Are the main communicators and the liaison between the HMIS Management Team and their respective agency's users
- ⇨ Ensure compliance with HMIS policies within their agency
- ⇨ Provide support for HMIS use within their agency, including development of site-specific documentation and planning for HMIS knowledge transfer for staff turnover

HMIS User Group

- ⇨ Meets at least twice annually
- ⇨ Includes representatives of all HMIS participating projects
- ⇨ Provides feedback on system performance and the need for system enhancements
- ⇨ Provides input and support for policy enforcement
- ⇨ Provides information link between agency users and the HMIS Management Team

HMIS Agency Implementation Policies and Procedures

HMIS Participation Policy

Mandated Participation

All projects that are authorized under HUD's McKinney-Vento Act as amended by the HEARTH Act to provide homeless services, designated Federal Partners, and projects receiving Illinois Department of Human Services homelessness prevention funding must meet the minimum HMIS participation standards as defined by this Policies and Procedures manual. In addition, all homeless services and housing providers within the CoC that participate in Coordinated Entry, and not statutorily disallowed from participating in HMIS, shall use the HMIS for data collection and sharing. In addition, all homeless services and housing providers within the CoC that participate in Coordinated Entry, and not statutorily disallowed from participating in HMIS, shall use the HMIS for data collection and sharing. 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 required to meet only 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

- ⇨ Each participating agency shall execute an *HMIS Agency Partner Agreement* and an *Inter-Agency Data Sharing Memorandum of Agreement ("MOA") for Housing and Service Coordination*
- ⇨ Agency staff shall collect the universal and program-specific data elements as defined by HUD and other data elements as determined by the HMIS Committee for all clients served by programs participating in HMIS; data may be shared with other agencies subject to appropriate client consent and data sharing agreements.
- ⇨ Agency staff shall enter client-level data into the HMIS within three working days of client interaction.
- ⇨ Participating agencies shall comply with all HUD regulations for HMIS participation.
- ⇨ Each agency shall designate at least one HMIS Primary Point Person. This person may or may not also be the Agency Administrator (see below). The HMIS Primary Point

Person functions as the main liaison with the HMIS Management Team and is responsible for organizing their 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.

- Each agency having five or more users must designate at least one user to function as an Agency Administrator. Agencies with fewer than five users have the option of designating an Agency Administrator. The Agency Administrator is expected to provide on-site support to the agency's end-users, run agency reports, monitor the agency's data quality and work with the HMIS Management Team to troubleshoot HMIS issues. Agency Administrators are expected to attend HMIS User Group meetings.
- Each HMIS participating <u>project</u> within an agency is required to have a representative at each HMIS User Group meeting <u>who can effectively communicate</u> what is covered in the meeting to the rest of the project's HMIS users.

HMIS Partnership Termination - Data Transfer Policies

In the event that the relationship between the Alliance HMIS and a Partner Agency is terminated, the Partner Agency will no longer have access to the HMIS. The HMIS Management Team shall make reasonable accommodations to assist a Partner Agency to export its data in a format that is usable in its alternative database. Any costs associated with exporting the data will be the sole responsibility of the Partner Agency.

HMIS Security Plan

The Continuum has defined a security plan that:

- ⇨ Ensures the confidentiality, integrity and availability of all HMIS information
- ⇨ Protects against any reasonably anticipated threats or hazards to security
- ⇨ Ensures compliance by end-users

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; dual core recommended
- ⇨ Memory: 4gb recommended (2gb minimum)
- ⇨ Hard Drive: 40 MB available space
- ⇨ Web Browsers: The most current version of MS Internet Explorer, Chrome, Edge, Safari, 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.

Any network that has a Wi-Fi component must employ at least WPA2 level security.

Security Hardware/Software

All workstations accessing the HMIS need to be protected by a securely configured firewall 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. Each Partner Agency will determine the physical access controls appropriate for their organizational setting based on HMIS security policies, standards and guidelines. All workstations must be password protected with the "Screen Timeout" setting, or equivalent, implemented, and they may not be located where screens are visible to non-authorized persons. Any workstation used off-site, including laptops and other mobile devices, should have appropriate and current firewall and virus protection as specified above under *Security Hardware/Software* and must be approved by HMIS staff. Tablets and cell phones must have the ability to be wiped remotely, and it is preferred for laptops to have the ability. Any laptops storing clients' personally identifying information must have the ability to be wiped remotely.

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, in consultation of the HMIS Team, must:

- ⇨ Determine the access level of the proposed HMIS user
- ⇨ Review HMIS records about previous users to ensure that the individual does not have previous violations with the *HMIS Policies and Procedures Manual* that prohibit their access to the HMIS

- ⇨ Verify that an *HMIS End User Policy and Code of Ethics* has been correctly executed
- ⇨ Verify that appropriate and sufficient training has been successfully completed
- ⇨ Create the new user ID and password in Community Services (ServicePoint™)", if authorized, or submit request for creation to the HMIS Management Team

If any user leaves the agency or no longer needs access to the HMIS, the Partner Agency is responsible for immediately notifying the HMIS Management Team.

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

Adding Partner Agencies

Prior to setting up a new Partner Agency within the HMIS database, the HMIS Management Team shall:

- ⇨ Review HMIS records to ensure that the agency does not have previous violations
- ⇨ Verify that the required documentation has been correctly executed and submitted or viewed on site, including:
    - Partner Agreement
    - Additional Documentation on Agency and Project(s)
    - Designation of HMIS Primary Point Person/Agency Administrator
    - Fee Payment, if applicable
- ⇨ Request and receive approval from the HMIS Management Team to set up a new agency in the HMIS

- ⇨ Work with the Partner Agency to input applicable agency and program information
- ⇨ Work with the HMIS Management Team to migrate legacy data, if applicable

Agency Information Security Protocol Requirements

At a minimum, Partner Agencies must develop security rules, protocols or procedures based on the current *HUD Data and Technical Standards* including but not limited to 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
- ⇨ Physical protection of workstations where employees are accessing HMIS via password protected computers with the "Screen Timeout", or equivalent, setting enabled and restrict viewing of screens to only those persons authorized to see specific content
- ⇨ 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
- ⇨ Procedures for regularly auditing compliance with the agency's information security protocol

The HMIS Management Team conducts annual site visits to monitor compliance with HMIS policies, at which time agencies may need to demonstrate their procedures for securing client data.

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. Users will have access to client-level data that is collected by their own agency. In some cases, the user may have access to data collected by another agency when that agency shares that data, subject to appropriate client consent.

DATA ACCESS CONTROL POLICIES

User Accounts

Partner Agencies are responsible for managing user accounts following the procedures documented in the *HMIS User Implementation* section of this manual 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 Partner Agencies must regularly review user access privileges.

Partner Agencies are responsible for inactivating and/or removing users from the system by contacting the HMIS Management Team. 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), their account should be temporarily suspended within 5 business days from the start of the leave. Suspended accounts may be reactivated only with the authorization of the user's supervisor.

User Passwords

Each user will be assigned a unique identification code (User ID), preferably the first initial and last name of the user. In the event a username that fits these parameters is unavailable, a number will be added to the end of the username, starting with "1", in ascending order

A temporary password will be assigned when a new user is created. The user will be required to establish a new password upon 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 must be between 8 and 50 characters long, contain at least one uppercase letter, one lowercase letter, one number, and one symbol. The password is case-sensitive and should not be easily guessed or found in a dictionary. The same log-in credentials cannot be used on more than one open session of Community Services (ServicePoint™) concurrently.

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

Community Services (ServicePoint™) will prompt a user to reset an expired password upon their next valid log-in attempt. In addition, a self-service password reset is available to users, who have an agency-specific and user -specific email address registered with their HMIS access credentials. The HMIS Management Team, and in some cases the Agency Administrator, also can temporarily reset a password. All requests for password resets by the HMIS Team should be submitted through NIL HMIS Support Ticketing system.

Temporary Suspension of User Access to HMIS

System Inactivity

Users must log off from the HMIS application and either lock or log off their respective workstation if they leave the workstation. Also, password protected screen-savers or automatic network log-off should be implemented on each workstation. If the user is logged into HMIS and the period of inactivity in HMIS exceeds 30 minutes, the user will be logged off the HMIS system automatically.

Unsuccessful Log-in

If a user attempts 3 unsuccessful log ins, the User ID will be temporarily deactivated. To regain access, the user will need to follow the password reset procedure, using the self-service password reset tool on the Community Services (ServicePoint™) log-in page. If the user does not have an agency-specific and user -specific email address registered with their HMIS access credentials or a current user ID, the user will need to be reactivated. All requests for reactivation by the HMIS Team should be submitted through NIL HMIS Support Ticketing system.

Electronic Data Control

Agency Policies Restricting Access to Data

Partner agencies must establish protocols limiting internal access to data based on the current *HUD Data and Technical Standards*. Only persons who have been granted explicit access by the partner agency or HMIS Team are permitted to view personally identifying information or other data that could be used for de-anonymization.

Downloaded Data

Users have the ability to download and save client-level data. Once this information has been downloaded from the HMIS server, the security of this data then becomes the responsibility of the user and the agency. The protocol must address secure data storage, transmission, and disposal.

Correspondence

On occasions when a user must communicate with the Alliance staff or other internal/external agency staff regarding a specific client record, no identifiable information should be shared through unencrypted email. The preferred method for communicating with the HMIS Team about client data is through the NIL HMIS Support Ticketing system. When communicating with the HMIS Team via email, a client ID may be stated in the email body, but not the email subject line. No PII should be stated in either form of correspondence.

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, and the establishment of protocols for secure data storage, transmission, and disposal.

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 Privacy Plan

The Continuum has defined a privacy plan that includes:

- Data collection limitation
- Purpose and use limitations
- Allowable uses and disclosures
- Access and correction standards
- Protection for victims of domestic violence, dating violence, sexual assault and stalking

Data Collection Limitation Policy

Partner Agencies will solicit or enter information about clients into the HMIS database only in order to provide services or conduct evaluation or research. Partner Agency management, in consultation with the Alliance, will make a determination of what qualifies as essential for services or research.

Client Notification Policies and Procedures

The Alliance has prepared standard documents for *HMIS Notice of Privacy Practices* and *Client Consent to Release Information*, which are available on the Alliance web site (www.suburbancook.org) and should be modified to include agency-specific information. Partner Agencies may either use these forms or incorporate the content of the HMIS documents into the agency's own documentation. All written consent forms must be stored in each 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.

The HMIS Management Team conducts annual site visits to monitor compliance with HMIS policies, at which time agencies may need to provide examples of the above-mentioned privacy documents and their procedures for protecting the privacy of client data.

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 their information and where it is stored. A public notice of privacy practices that explains the purpose of HMIS and the client's rights as they relate to data-sharing policies must be posted or viewable wherever data is collected from a client. 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 how much of their data may be shared and to view a copy of their 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 the content of the standard HMIS Notice. If the agency has a web site, the adopted Notice of Privacy Practices or equivalent privacy notice must also be posted on the website.

Locked Client Record

After learning about the HMIS, if a client does not wish to have their Primary Identifiers accessible to all HMIS users, the originating HMIS user should change the visibility settings on the client record. Locking a client record will allow the agency to access the client's information for agency purposes. This action will allow the HMIS Management Team 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 their Information within the Alliance HMIS.

If a client is willing to share their information within the HMIS, he/she must provide written consent (see exception below for call center and telephone intake operations). The consent must be specific regarding:

- ⇨ Purpose
- ⇨ The expiration of the sharing
- ⇨ Affected data elements
- ⇨ Function
- ⇨ Involved parties

The client maintains a right to revoke written authorization at any time (except if that policy is overridden by agency policy or if the information is required to be shared as a condition of a provider agreement). Note that any such revocation will not be retroactive to any information that has already been released. 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 data-sharing that is in accordance with a valid Client Consent to Release information form, or in the case of call center and telephone intake operations, explicit oral consent (see p. 22).

Authorized users will be able to grant permission based on appropriate client consent to share individual client information with another agency's users. To document a client's authorization, the signed *Client Release of Information* form must be uploaded to the client's HMIS record. In addition, audit trails and other monitoring tools may be used to ensure that this data sharing procedure is followed.

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.

Summary of Notification/Consent and Data Sharing Procedures

The table below summarizes the general procedures for sharing client information in HMIS, and the related notification rules that relate to each level, as stated on the *Client Consent to Release Information* (ROI). These minimum procedures should not imply that all providers would perform all of these functions. Notably, sharing of client information for the purposes of Coordinated Entry is defined by the *Inter-Agency Data Sharing Agreement for Housing and Service Coordination* and through allowances determined by the *VI-SPDAT Survey and Entry Point Assessment Consent* (CE VI-SPDAT Consent).

<table>
<tr><th>Client Information Sharing Categories</th><th>Summary of Notification/Consent and Information Sharing Procedures</th></tr>
<tr><td>Primary Identifiers:
Name and Alias
Date of Birth
Gender
Social Security Number
Household Relationships
Housing Status
Client Veteran Status
Client Photo (where applicable)</td><td><u>When a client selects Profile Only or Profile Plus on the ROI,</u> the Name and Alias, Date of Birth, Gender, Social Security Number, and Household Status will be available to all HMIS users in the Client Search to locate an existing client. In addition, Veteran Status and the Housing Status will be available within the client record. None of the other client information will be viewable, except as described below.

<u>When a client selects to not share information on the ROI, the record must be “locked”.</u> 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 records for system administration purposes.</td></tr>
<tr><td>General Client Information:
Race/Ethnicity
Services Provided
Project Enrollment (Entry/Exit)
Income/Benefits</td><td><u>When a client selects Profile Plus on the ROI</u>, this information can be shared with HMIS users from partner agencies by unlocking the relevant demographic assessments, Entry/Exit, and Service Transactions.

<u>When a client selects Profile Only or chooses not to share information</u>, this information is accessible only within the originating agency and some system-level users for system administration purposes.</td></tr>
<tr><td>Protected Information:
Disability Information
Mental Health Assessment
Substance Use Assessment
HIV/AIDS Information
Vulnerability Assessment
Domestic Violence Information</td><td><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 information requires signed consent from the client. The CE VI-SPDAT Consent permits sharing of this information.</td></tr>
</table>

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

The Alliance provides an *HMIS Notice of Privacy Practices* template which can be found on the Alliance HMIS web site (www.suburbancook.org) . Before use, the template should be modified to include agency-specific information as indicated in the template. In addition, the Alliance provides a sample Domestic Violence Notice as part of the Privacy Document Packet on the Alliance website.

Each agency must post their public notice of privacy practices wherever client data is collected and provide a copy of the full 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.

The *Privacy Notice* includes:

- ⇨ All potential uses and disclosures of a client's personal information
- ⇨ The purpose for collecting the information
- ⇨ The time period for which a client's personal information will be retained at the agency
- ⇨ 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
- ⇨ The process and applicability of amendments, and the commitment to documenting all privacy notice amendments
- ⇨ An offer for reasonable accommodations for persons with disabilities and/or language barriers throughout the data collection process
- ⇨ An individual's right to inspect and to have a copy of their client record and offer to explain any information that the individual may not understand
- ⇨ Procedures 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 share client information with other agencies based only on written client consent, or in the case of call center operations, explicit oral consent (see p. 22)
- ⇨ Billing uses include functions related to payment or reimbursement for services. An example might include generating reports for fundraising 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 *Strategic Plan to End Homelessness*.

Unless a client requests that their record be locked, their 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.

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.

HMIS Data Release Policies and Procedures

Client-identifying Data

No identifiable client data will be released to any person, agency, or organization for any purpose other than those specified in the *HMIS Data Use and Disclosure Policies and Procedures* section of this manual without the written permission of the client.

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 Use and Disclosure Policies and Procedures* section of this manual, such that the identity of any individual or household cannot be determined.

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.

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.

Specific Coordinated Entry Consent Requirement

Client information collected for the purposes of Coordinated Entry (CE) will be recorded in the HMIS. To better ensure that that housing availability is equitable and appropriate based on prioritized need, additional data-sharing beyond the standard HMIS consent is necessary. Disclosures, consents for sharing information, and policies specific to CE are maintained separately by the CE lead body. All participants in CE who use HMIS are also subject to the HMIS policies and procedures.

Specific Call Center and Telephone Intake Exception to Written Consent Requirement

Call center operations 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 rights regarding HMIS participation, and written consent is required for sharing of Protected Information (as defined on page 19). Clients will be read the call center or telephone intake consent and notifications script. Clients can view the Privacy Notice on the Alliance website or pick up a copy at the Alliance office. Callers who do not want their information shared in HMIS will have their records locked and/or may be limited in their ability to obtain an agency referral.

Specific Client Notification Procedures for Victims of Domestic Violence, Dating Violence, Sexual Assault and Stalking

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

The Alliance provides a sample Domestic Violence Notice as part of the Privacy Document Packet on the Alliance website (www.suburbancook.org).

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.

Clients shall have the right to an independent, impartial review of any complaints they may have regarding HMIS data collection, explanations offered for that collection, and policies surrounding the collection. They also have a right to know about this opportunity. Participating providers must apprise clients of their rights to file a formal grievance with the Alliance should they suspect their HMIS data privacy rights have been compromised and inadequately addressed by the agency, in accordance with the *Privacy Notice*. It is the responsibility of the Agency to ensure that the client is informed of their rights and that the *Privacy Notice* is readily accessible to clients.

HMIS Data Quality Plan

The Continuum has defined a data quality plan that:

- ⇨ Based on current HMIS data standards and CoC data requirements, specifies the data quality standard to be used by all participating agencies
- ⇨ Ensures a system that is fortified by data accuracy, integrity, and timeliness.
- ⇨ Provides a mechanism for monitoring adherence to the standard
- ⇨ Provides the necessary tools and training to ensure compliance with the standard
- ⇨ Includes strategies for working with agencies that are not in compliance with the standard

HMIS Data Collection

Data Quality Standard

- ⇨ All data entered will be accurate
- ⇨ Per HUD data standards, blank entries in required data fields will not exceed 5% per month
- ⇨ All services provided will be compatible with providing program
- ⇨ Data entry, including project Entry and Exit transactions, must be complete within three working days of data collection, with a push towards real time data collection where feasible.

Data Quality Monitoring

The HMIS Management Team will perform regular data integrity checks on the HMIS data, as well as conduct an annual review of the Project Descriptor Data Elements (PDDEs) as defined by the current *HUD Data and Technical Standards*. Any patterns of error at a Partner Agency will be reported to the Agency Administrator and/or Primary Point Person. When patterns of error have been discovered, users will be required to correct data entry techniques and will be monitored for compliance.

Partner Agencies are expected to:

- ⇨ Run and submit data completeness reports, data incongruities reports and other data quality reports as required by HMIS Lead staff
- ⇨ Review monthly Point in Time (PIT) reports to confirm accurate program entry and exit data
- ⇨ Notify HMIS Lead staff of findings and timelines for correction
- ⇨ Rerun reports for errant agencies/programs to confirm data correction

Data Collection Requirements

Required Data Elements – HMIS Management Team

The HMIS Management Team is responsible for ensuring that the Project Descriptor Data Elements (PDDEs), which identify and define the individual projects within the HMIS, are complete. The PDDEs are determined by the current *HMIS Data Standards* and are recorded at the point of project set-up and annual intervals. Thus, the PDDEs for every project must be reviewed and updated on a yearly basis by the HMIS Management Team, in accordance with the current *HMIS Data Standards*. It is the responsibility of Partner Agencies to provide HMIS staff with accurate information, as best understood, to record and maintain valid PDDEs at the appropriate intervals.

Required Data Elements – Partner Agency

A Partner Agency is responsible for ensuring that a minimum set of data elements, referred to as the Universal Data Elements (UDEs) and Program-specific Data Elements (PSDEs)as defined by the *current HMIS Data Standards*, and other data elements as determined by the HMIS Committee, will be collected and/or verified from all clients at their initial project enrollment or as soon as possible thereafter. Partner Agencies are required to enter data into the HMIS within three business days of collecting the information.

Partner Agencies will strive to collect complete data on all applicable clients and must report client-level UDEs and PSDEs using the required response categories detailed in the current *HMIS Data Standards.* These standards are already incorporated into the HMIS.

Entry/Exit Data

The Project Start Date and Exit Date should be recorded upon any project enrollment or project separation on all participants. The Start Date should be recorded for the first day of service or project enrollment, with a new project Start Date for each period/episode of service. The appropriate Project Start Date is informed by the type of project in which the client is enrolled, in accordance with the current HMIS Data Standards. The Exit Date should be recorded for the date in which the client is no longer considered to be participating in the project, such as the last day of residence in a project's housing before the participant leaves the shelter or the last day a service was provided. The appropriate Project Exit Date is informed by the type of project in which the client is enrolled, in accordance with the current HMIS Data Standards. In the case where a client has not been in contact with, or received services from, a project for an extended period, the service provider must apply an Exit Date to the client's record, using the standard set by the CoC. The current period is 90 days from the last contact or service transaction, although this is subject to change.

Data Quality Training Requirements

End User Training

Each end user of the HMIS system must complete Alliance approved HMIS training before being given HMIS log-in credentials. Trainings are offered on regular basis, and users are able to register from the Alliance website. It is recommended they also receive training from their Agency Administrator in order to understand agency-specific nuances in how they enter data. HMIS Primary Point Persons and Agency Administrators should notify the Alliance when they have specific training needs for their end users.

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 Provider Reports in ServicePoint™, how to use ReportWriter to create simple reports, how to run existing reports in the Advanced Reporting Tool (ART) and may include opportunities for training in report creation using ART. (Note: Use of ART requires a separate Report Viewer or Ad-hoc Report Creation license.)

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

HMIS De-duplication of Data

De-duplicating Data Elements

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

- Name (first, middle, last; aliases or nicknames should be avoided)
- Date of Birth (actual or estimated)
- Gender

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 he/she has explicit authorization to view that client's record.

In the event a duplicate client record is identified, the user should submit a case to the HMIS Management Team through the NIL HMIS Support Ticketing system.

Back-end Central Server Matching Based on Identifiable Information

When Primary Identifiers are not shared across agencies for de-duplication purposes, the HMIS Management Team 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 locked 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.

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 or Primary Point Person
- ⇨ If the question is still unresolved, the Agency Administrator or Primary Point Person can direct the question to the HMIS Management Team through the NIL HMIS Support Ticketing system
- ⇨ If the question is still unresolved, the HMIS Management Team will direct the question to WellSky 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 or Primary Point Person, if available
- ⇨ If unavailable, and the question is still unresolved, contact the HMIS Management Team through the NIL HMIS Support Ticketing system, 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 WellSky 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 at least 6 times per year. If additional, or specific, training needs arise, the HMIS Management Team may arrange for special training sessions. The training calendar is published on the Alliance website.

Agency/User Forms

All Agency Administrators and Primary Point Persons will be trained in the appropriate on-line and hardcopy forms. If the Agency Administrator or Primary Point Person has questions on how to complete HMIS forms, he/she shall contact the HMIS Management Team.

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 Management Team will be a resource to agency users as they develop reports but will be available to provide only 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 the Agency Administrator. The Agency Administrator should submit the request to the HMIS Management Team through the NIL HMIS Support Ticketing system, identifying the specific nature of the issue or recommended improvement, along with the immediacy of the request.

The HMIS Management Team will review all application service requests and determine the action to be taken. Requests to fix programming errors will be prioritized and forwarded to WellSky. Suggested application improvements will be compiled and periodically discussed by the HMIS Committee and the HMIS User Group.

HMIS System Availability Policies

There are times that Community Services (ServicePoint™)"is unavailable because WellSky 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 Management Team will communicate with WellSky, and Agency Administrators will be notified of any information regarding the interruption as it is made available.

Appendix A: Glossary of HMIS Acronyms and Terms

Adapted from http://www.hmis.info/Resources/742/HMIS-Acronyms-and-Definitions.aspx

Acronyms

Provider Project Types

ES – Emergency Shelter

EE – Entry Exit (extended stay)
NbN – Night by Night

HP – Homelessness Prevention

PSH – Permanent Supportive Housing

PH – Permanent Housing

RRH – Rapid Rehousing

SH – Safe Haven

SO – Street Outreach

SSO – Support Services Only

STSS – Short Term Stabilization Services

TH – Transitional Housing

AIRS - Alliance of Information & Referral Systems

AHAR - Annual Homeless Assessment Report

APR - Annual Performance Report

ART – Advanced Reporting Tool in Community Services (ServicePoint™)

BNL – By-Name List (for coordinated entry)

CE – Coordinated Entry

CHO – Contributing HMIS Organization

CoC - Continuum of Care

DOB - Date of Birth

DV - Domestic Violence

ESG - Emergency Solutions Grants

FIPS - Federal Information Processing Standards Codes for states, counties, and named populated places.

HEARTH – Homeless Emergency Assistance and Rapid Transition to Housing

HIC – Housing Inventory Count

HIPAA - Health Insurance Portability and Accountability Act of 1996

HMIS - Homeless Management Information System

HOPWA – Housing Opportunities for Persons with AIDS

HUD - U.S. Department of Housing and Urban Development

I&R - Information and Referral

MH - Mental Health

NOFA - Notice of Funding Availability

PDDEs – Project Descriptor Data Elements

PIT - Point in Time

PII - Personally Identifiable Information

PPI - Personal Protected Information

PSDEs - Program-Specific Data Elements

RHY – Runaway and Homeless Youth

S+C - Shelter Plus Care (McKinney-Vento Program)

SA - Substance Abuse

SHP - Supportive Housing Program

SNAP – Supplemental Nutrition Assistance Program

SRO - Single Room Occupancy

SSN - Social Security Number

SSI - Supplemental Security Income

SSDI – Social Security Disability Insurance

SSO - Supportive Services Only

SSVF – Supportive Services for Veteran Families Program

TA - Technical Assistance

TANF - Temporary Assistance for Needy Families

UDE – Universal Data Element

VAWA - Violence Against Women Act

VI-SPDAT – Vulnerability Index and Service Prioritization Decision Assistance Tool

Terms

Alliance of Information and Referral Systems (AIRS)

The professional association for over 1,000 community information and referral (I&R) providers serving primarily the United States and Canada. AIRS maintains a taxonomy of human services.

Annual Performance Report (APR)

A report that tracks program progress and accomplishments in HUD`s competitive homeless assistance programs. The APR provides the grantee and HUD with information necessary to assess each grantee`s performance.

Audit Trail

A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Most database management systems include an audit trail component.

Bed Utilization

An indicator of whether shelter beds are occupied on a particular night or over a period of time.

Biometrics

Refers to the identification of a person by computerized images of a physical feature, usually a person's fingerprint.

By-Name List (BNL)

A by-name list is a real-time, up-to-date list of all people experiencing homelessness which can be filtered by categories and shared across agencies. This list is generated with data from outreach, HMIS, federal partners, and any other community shelters and providers working with the specific homeless subpopulation.

Chronic Homelessness

A homeless individual with a disability who lives either in a place not meant for human habitation, a safe haven, or in an emergency shelter, or in an institutional care facility if the individual has been living in the facility for fewer than 90 days and had been living in a place not meant for human habitation, a safe haven, or in an emergency shelter immediately before entering the institutional care facility. In order to meet the ''chronically homeless'' definition, the individual also must have been living as described above continuously for at least 12 months, or on at least four separate occasions in the last 3 years, where the combined occasions total a length of time of at least 12 months. Each period separating the occasions must include at least 7 nights of living in a situation other than a place not meant for human habitation, in an emergency shelter, or in a safe haven.

Chronically Homeless Household

A household that is comprised of one or more persons who are experiencing chronic homelessness, as defined by the HUD final rule, with the head of household (either an adult or a minor if there is no adult present) having the qualifying disability and meeting all other criteria required for chronicity

Client Intake

The process of collecting client information upon entrance into a program.

Consumer

An individual or family who has experienced homelessness, is currently experiencing homelessness, or is at-risk for homelessness

Continuum of Care (CoC)

A community with a unified plan to organize and deliver housing and services to meet the specific needs of people who are homeless as they move to stable housing and maximize self-sufficiency. HUD funds many homeless programs and HMIS implementations through Continuum of Care grants.

Coordinated Entry

The coordinated entry process is an approach to coordination and management of a crisis response system's resources that allows users to make consistent decisions from available information to efficiently and effectively connect people to interventions that will rapidly end their homelessness.

Coverage

A term commonly used by CoCs or homeless providers. It refers to the number of beds represented in an HMIS divided by the total number of beds available.

Contributing HMIS Organization (CHO)

Any organization (including its employees, volunteers, affiliates, contractors and associates) that records, uses or processes data on homeless clients for an HMIS. The requirements of the HMIS Final Notice apply to all Contributing HMIS Organizations.

Data Quality

The accuracy and completeness of all information collected and reported to the HMIS.

Data Standards

See current *HMIS Data Standards*.

De-identification

The process of removing or altering data in a client record that could be used to identify the person. This technique allows research, training or other non-clinical applications to use real data without violating client privacy.

Digital Certificate

An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be and to provide the receiver with the means to encode a reply.

Disabling Condition

A disabling condition in reference to chronic homelessness is defined by HUD as a diagnosable substance use disorder, serious mental illness, developmental disability or chronic physical illness or disability, including the co-occurrence of two or more of these conditions. A disabling condition limits an individual's ability to work or perform one or more activities of daily living.

Emergency Shelter

Any facility whose primary purpose is to provide temporary shelter for the homeless in general or for specific populations of the homeless.

Emergency Solutions Grant (ESG)

A federal grant program designed to help improve the quality of existing emergency shelters for the homeless, to make available additional shelters, to meet the costs of operating shelters, to provide essential social services to homeless individuals and to help prevent homelessness.

Encryption

Conversion of plain text into unreadable data by scrambling it using a code that masks the meaning of the data to any unauthorized viewer. Computers encrypt data by using algorithms or formulas. Encrypted data are not readable unless they are converted back into plain text via decryption.

Final Notice

See *HMIS Data and Technical Standards Final Notice*.

Hashing

The process of producing hashed values for accessing data or for security. A hashed value is a number or series of numbers generated from input data. The hash is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value or that data can be converted back to the original text. Hashing is often used to check whether two texts are identical. For the purposes of Homeless Management Information Systems, it can be used to compare whether client records contain the same information without identifying the clients.

HEARTH Act

On May 20, 2009, President Obama signed the Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act of 2009. The HEARTH Act amends and reauthorizes the McKinney-Vento Homeless Assistance Act.

Homeless Management Information System (HMIS)

Computerized data collection tool designed to capture client-level information over time on the characteristics and service needs of men, women and children experiencing homelessness.

HMIS Data and Technical Standards Final Notice

Regulations issued by HUD via the Federal Register describing the requirements for implementing HMIS. The *HMIS Final Notice* contains rules about who needs to participate in HMIS, what data to collect and how to protect client information.

Housing Inventory Chart/Count (HIC)

A calculation of the numbers of beds and housing units in a region on one particular night, usually coinciding with the annual Point-in-Time count.

Inferred Consent

Once clients receive an oral explanation of HMIS, consent is assumed for data entry into HMIS. The client must be a person of age and in possession of all their faculties (for example, not mentally ill).

Informed Consent

A client is informed of options of participating in an HMIS system and then specifically asked to consent. The individual needs to be of age and in possession of all of his faculties (for example, not mentally ill) and their judgment not impaired at the time of consenting (by sleep, illness, intoxication, alcohol, drugs or other health problems, etc.).

Information and Referral (I & R)

A process for obtaining information about programs and services available and linking individuals to these services. These services can include emergency food pantries, rental assistance, public health clinics, childcare resources, support groups, legal aid and a variety of non-profit and governmental agencies. An HMIS usually includes features to facilitate information and referral.

McKinney-Vento Act

The McKinney-Vento Homeless Assistance Act was signed into law by President Ronald Reagan on July 22, 1987. The McKinney-Vento Act funds numerous programs providing a range of services to homeless people, including the Continuum of Care Programs: the Supportive Housing Program, the Shelter Plus Care Program and the Single Room Occupancy Program, as well as the Emergency Solutions Grant Program.

Notice of Funding Availability (NOFA)

An announcement of funding available for a particular program or activity.

Permanent Supportive Housing

Long term, community based housing that has supportive services for homeless persons with disabilities. This type of supportive housing enables special needs populations to live as independently as possible in a permanent setting. Permanent housing can be provided in one structure or in several structures at one site or in multiple structures at scattered sites.

Point-in-Time Count (PIT)

A snapshot of the homeless population taken on a given day. Since 2005, HUD requires all CoC applicants to complete this count every other year in the last week of January. This count includes a street count in addition to a count of all clients in emergency and transitional beds.

Privacy Notice

A written, public statement of an agency's privacy practices. A notice informs clients of how personal information is used and disclosed. According to the *HMIS Data and Technical Standards*, all covered homeless organizations must have a privacy notice.

Program-specific Data Elements (PSDEs)

Data elements required for programs that receive funding under the McKinney-Vento Homeless Assistance Act and complete the Annual Performance Reports (APRs).

Project Descriptor Data Elements (PDDEs)

Data elements that identify the individual projects within the HMIS System and are maintained by HMIS System Administration

Scan Cards

Some communities use ID cards with bar codes to reduce intake time by electronically scanning ID cards to register clients in a bed for a night. These ID cards are commonly referred to as scan cards.

Single Room Occupancy (SRO)

A residential property that includes multiple single room dwelling units. Each unit is for occupancy by a single eligible individual. The unit need not, but may, contain food preparation or sanitary facilities, or both. It provides rental assistance on behalf of homeless individuals in connection with moderate rehabilitation of SRO dwellings. This program type has been consolidated into the CoC Program by the HEARTH Act.

Shelter Plus Care Program

A program that provides grants for rental assistance for homeless persons with disabilities through four component programs: Tenant, Sponsor, Project and Single Room Occupancy (SRO) Rental Assistance. This program type has been consolidated into the CoC Program by the HEARTH Act.

Supportive Housing Program

A program that provides housing, including housing units and group quarters, that has a supportive environment and includes a planned service component. This program type has been consolidated into the CoC Program by the HEARTH Act.

Supportive Services

Services that may assist homeless participants in the transition from the streets or shelters into permanent or permanent supportive housing, and that assist persons with living successfully in housing.

Transitional Housing

A project that has as its purpose facilitating the movement of homeless individuals and families to permanent housing within a reasonable amount of time (usually 24 months)

Unduplicated Count

The number of people who are homeless within a specified location and time period. An unduplicated count ensures that individuals are counted only once regardless of the number of times they entered or exited the homeless system or the number of programs in which they participated. Congress directed HUD to develop a strategy for data collection on homelessness so that an unduplicated count of the homeless at the local level could be produced.

Universal Data Elements (UDEs)

Data required to be collected from all clients serviced by homeless assistance programs using an HMIS. These data elements include date of birth, gender, race, ethnicity, veteran's status, and Social Security Number (SSN). These elements are needed for CoCs to understand the basic dynamics of homelessness in their community and for HUD to meet the Congressional directive.

Written Consent

Written consent embodies the element of informed consent in a written form. A client completes and signs a form documenting the client's understanding of the options and risks of participating or sharing data in an HMIS system and consenting to such participation and data sharing. The signed document is then kept on file at the agency.