Chicago Homeless Management Information System (HMIS)

Standard Operating Procedures for Implementation

Approved by the Planning Council on Homelessness:

Date: January 2014

Current Version #: 1.01

all Chicago
making homelessness history

Table of Contents

INTRODUCTION

SECTION 1

SECTION 2

SECTION 3

SECTION 4

SECTION 5

SECTION 6

Introduction

HMIS Objectives and Expectations

The HMIS implementation is led by All Chicago Making Homelessness History (All Chicago) in close collaboration with the Chicago Planning Council on Homelessness (Planning Council). In turn, the Planning Council relies on a number of committees and task groups to develop policy recommendations and provide guidance on implementation activities. These groups are committed to balancing the interests and needs of all stakeholders involved, including but not limited to homeless men, women, and children; service providers; funders; and policy makers.
The Bowman Systems software product, ServicePoint, has been adopted by the Chicago Continuum of Care (CoC) as the official Homeless Management Information System (HMIS) for CoC providers. The primary goal of the HMIS is to provide a data collection and reporting tool to aid the Continuum in its efforts to end homelessness in Chicago. The HMIS provides a critically important vehicle to collect client-level and data on the provision of housing and services to homeless individuals and families and persons at risk of homelessness. The HMIS facilitates the analysis of information that is gathered from consumers throughout the service provision process to generate an unduplicated count and other aggregate information (stripped of any identifying client level information) that can be made available to policy makers, service providers, advocates, and consumer representatives.

This document describes the policies, procedures, guidelines, and standards -- collectively referred to as the Standard Operating Procedures (SOPs) -- that govern HMIS operations and the respective roles and responsibilities of the HMIS Lead and agencies contributing HMIS data (identified by HUD and hereafter as Contributing HMIS Organizations or CHOs), whether such contribution of data is voluntary or required as a condition of funding. The SOP is 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.

SECTION 1

Contractual Requirements & Roles

SOP#: 01-010
Revised#: 01-010 Revised Date: 01/14/2015 Revised by: HMIS Lead
Planning Council Responsibilities

Policy: The Planning Council must review and approve all HMIS policy decisions.

Standard: The HMIS related responsibilities of the Planning Council will be apportioned according to the information provided below.

Purpose: To define the roles and responsibilities of the Planning Council with respect to HMIS activities.

Responsibilities:

As required by the CoC Interim Rule, the Planning Council, acting on behalf of the Continuum of Care, is responsible for:

- Designating a single HMIS for the geographic area;
- Designating an HMIS Lead to manage the Continuum's HMIS;
- Reviewing, revising, and approving a privacy plan, security plan, and data quality plan that is in compliance with HUD HMIS regulations and notices;
- Ensuring consistent participation of recipients and sub recipients in the HMIS; and
- Ensuring the HMIS is administered in compliance with requirements prescribed by HUD.

The Planning Council is responsible to review and approve any HMIS-related decisions. The Planning Council may designate a committee or task group to develop and help enforce the implementation of HMIS policies.

The Planning Council will provide guidance on the following HMIS-related key issues:

- The guiding principles that should underlie the HMIS implementation activities of participating organizations and service programs.
- Approving data quality standards, policies and procedures for ensuring adherence to data quality standards for the CoC as stated by HUD
- Encouraging Continuum-wide provider participation.
- Defining criteria, standards, and parameters for the use and release of all data collected as part of the HMIS.
- Documenting, approving, and regularly reviewing the policies herein the "Chicago Homeless Management Information System Operating Procedures for Implementation" (commonly referred to as the SOPs);
- Establishing Continuum-level mechanisms for monitoring and/or enforcing compliance with the approved SOPs; and

Any CoC stakeholder or Planning Council committee/workgroup may raise concerns or make recommendations for revising a specific HMIS SOP. To the extent that such a concern or recommendation is brought to the attention of the Planning Council, or if an SOP appears to conflict with applicable local, state or federal laws, or contractual obligations, the Planning Council will work with the HMIS Lead to amend the policy or procedure to address the matter. The Planning Council may also identify procedures that need to be amended based on the initial implementation and/or ongoing operation of the system. The Planning Council's process for addressing such matters shall be as follows:

- The Planning Council shall designate a specific committee or workgroup to explore the concern and to develop a recommendation for full Planning Council consideration. While a single committee may be identified as the primary entity generally responsible for overseeing the SOPs, another committee may be designated as the lead to explore a specific concern/recommendation.
- Proposed revisions must be presented and approved by the full Planning Council.
- After approval, a list of all revisions, the date revised, and a brief description of the change should be incorporated as part of the Table of Contents in the SOP documentation. The most current revision date should also be noted at the top of each individual policy.

SOP#: 01-020
Revised#:01-020 Revised Date: 01/14/2015 Revised by: HMIS Lead
HMIS Lead Responsibilities

Policy: An HMIS Lead Agency (hereinafter HMIS Lead) will be designated to support the operations of the HMIS according to the policies and procedures described in this document. Effective May 1, 2012, by agreement of the Planning Council on behalf of the Continuum of Care, the City of Chicago, and HUD, All Chicago Making Homelessness History (All Chicago) will serve in the role of HMIS Lead.

Standard: The responsibilities of the HMIS Lead are described herein.

Purpose: To define the roles and responsibilities of the HMIS Lead organization and staff.

Responsibilities:

The HMIS Lead is responsible for:

(a) Overseeing the operation of the Continuum-wide HMIS, to ensure that implementation is in compliance with HUD requirements.
(b) Developing and recommending periodically necessary revisions to, and implementing the privacy plan, security plan, and data quality plan which the Planning Council is charged with approving.
(c) Overseeing the participation by recipients and sub recipients and other Contributing HMIS Organizations (hereinafter CHOs) in the Continuum-wide HMIS.
(d) Developing, recommending periodically necessary revisions to, and overseeing compliance with the Chicago HMIS System Operating Procedures (hereinafter SOPs) adopted by the Planning Council on behalf of the Continuum.
(e) Executing and overseeing compliance with written HMIS Participation Agreements with each CHO, in accordance with HUD requirements and these SOPs.
(f) Serving as the applicant to HUD for grant funds to be used for HMIS activities for the Continuum-wide HMIS and, if selected for an award by HUD, entering into a grant agreement with HUD to carry out the HUD-approved activities.
(g) Supervising the contractual relationship with the HMIS Vendor.
(h) Working with the Planning Council to ensure the adequacy of funding to support the cost of the HMIS implementation, including the cost of staff and operations required by the HMIS Lead to comply with its responsibilities as defined herein and by HUD.

The HMIS Lead is responsible for oversight of all day-to-day operations including:

- Understanding all aspects of the HMIS implementation, and communicating significant application issues and/or system problems to the HMIS vendor

- Making, supporting, and/or requesting from the HMIS Vendor any application-level changes to setups and configurations, user interfaces, or system enhancements.
- Providing application, functionality, privacy protection, system security and agency-level system administration functionality.
- Supporting Agency Technical Administrators in fulfilling their HUD-related roles and responsibilities within their respective agencies, including generating all HUD- required reports, ensuring adherence to data quality standards, and supporting necessary data migration;
- Communicating system availability, planned outages, and other HMIS information to Agency Technical Administrators.
- Managing CHO agency and user system access based on execution of applicable agreements, training, and adherence to approved policies.
- Assigning user IDs to new users based on the approved licensing structure, authorized agency requests, and documentation of user training.
- Managing user accounts and application access control, in conjunction with the Agency Technical Administrators.
- Supporting CoC participation in the Annual Homeless Assessment Report;
- Providing technical support and application training to users; except that the HMIS Lead may delegate responsibility for application training to Technical Administrators at the various partnering agencies, or to other appropriately qualified agency staff, upon demonstration that said staff are sufficiently skilled and knowledgeable to effectively deliver such training.
- Monitoring compliance by CHOs with the provisions of the privacy, data security, and data quality plans, including periodically site visits to assess agency and staff adherence to data security policies and procedures;
- Developing a reasonable number of reports for use by CHOs to enable them to meet funding requirements, to support their efforts to ensure data quality (e.g., to identify missing data, inconsistent data, excessive use of "unknown" and "refused" responses, etc.), to facilitate caseload management, to support performance measurement, and to support participation in a CoC-wide coordinated intake and assessment system, when such system is implemented.
- To enter into an agreement with approved CHOs that enter HMIS data into their own systems (hereinafter "Interface Agencies") to upload their HMIS data into the CoC-wide HMIS. In conjunction with this responsibility, the HMIS Lead will assist in troubleshooting problems with such uploads, and will work with the HMIS Vendor and the Interface Agency to help resolve any such problems.
- Administering other system functions, as needed and appropriate.

The HMIS Lead shall specify within the written HMIS Participation Agreements executed with each CHO the nature and circumstances under which persons employed by or contracting with the HMIS Lead may have access to client-level data as part of their system administration responsibilities. All such employees and contractors must execute computer security and data confidentiality agreements as a precondition of access to client-level data. The HMIS Lead shall likewise ensure in its agreement with the HMIS Vendor that the vendor's employees and subcontractors are bound by similar requirements.

SOP#: 01-030
Revised#: 01-030 Revised Date: 01/14/2015 Revised by: HMIS Lead

Responsibilities of Contributing HMIS Organizations (CHOs)

Policy: The CEO or the Executive Director of every CHO will be responsible for oversight of all agency staff members who generate or have access to client- level data stored in the system software to ensure adherence to the HMIS standard operating procedures outlined in this document.

Standard: The CEO or the Executive Director holds final responsibility for the adherence of his/her agency's personnel to the HMIS Guiding Principles and Standard Operating Procedures outlined in this document.

Purpose: To outline the role of the agency CEO or the Executive Director with respect to oversight of CHO personnel in the protection of client data within the HMIS application.

Responsibilities:

The CHO’s CEO or the Executive Director is ultimately responsible for all activity associated with agency staff access to and use of the HMIS. The CEO or the Executive Director is responsible for establishing and monitoring compliance with agency procedures that adhere to the Standard Operating Procedures (SOPs) outlined in this document. The CEO or the Executive Director is ultimately responsible for any misuse of the HMIS by his/her designated staff. The CEO or the Executive Director agrees to only allow access to the HMIS based upon need. Need exists only for those program staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients and/or have data entry, analysis, or reporting or other administrative responsibilities which require access to the HMIS.

The CEO or the Executive Director will sign an Agency Partnership Agreement with the HMIS Lead to oversee the implementation and:

- Assumes ultimate responsibility for completeness, accuracy, and protection of client-level data entered into the HMIS system;
- Must oversee the implementation of data security policies and standards;
- Must establish business controls and practices to ensure organizational adherence to the HMIS SOPs;
- Must designate an Agency Technical Administrator (ATA) to manage HMIS related technical tasks; the ATA may be an employee of the agency, a paid consultant to the agency, a paid consultant or employee of a second agency whose service as an ATA is contractually shared by the two (or more) agencies.
- Must communicate data privacy, confidentiality, and security requirements to agency data custodians and users;

- Designates the staff that is authorized to access the data and/or have responsibility for custody of the data.
- Is responsible for monitoring compliance and for periodically reviewing agency data access, management, and custody policies and procedures.

SOP#: 01-040
Revised#: 01- 040 Revised Date:01/14/2015 Revised by: HMIS Lead
HMIS Agency Technical Administrators (ATA) Responsibilities

Policy: The CEO or the Executive Director of every CHO must designate one person to be the ATA

Standard: The designated ATA has responsibility for the administration of the system software in his/her agency.

Purpose: To outline the role of the ATA

Responsibilities:

The ATA is:

- The point person for the HMIS Lead team.
- The go to person for all HMIS users within the CHO
- To understand the system and the data and to be able to generate reports; frequently logging into the system.
- Responsible for CHO's data quality and reports
- Responsible for ongoing training and support for all staff apart from the trainings offered by the HMIS Lead team
- To be in compliance with the License Management Policy (Appendix B)
- Ensure all agency information is up to date with the Lead team
- Source for all HMIS related forms and consents.
- Leader in ensuring that the agency and programs are in compliance with all other HMIS requirements as specified by the HMIS Lead Team

Access for ATA's in the system allows:

- The ability to be in shadow mode
- Deletion of records
- Viewing of all their agency and program data
- Ability to view and generate data reports using Advanced Reporting Tool (ART)

SOP#: 01-050
Revised#:01-050 Revised Date: 01/14/2015 Revised by: HMIS Lead

HMIS Interface Agency Responsibilities

Policy: Agencies that have received approval prior to September 19, 2012 may continue to contribute data to HMIS as an interface agency and are required to comply with the Interface policy. The agency is responsible for ensuring the timeliness, accuracy and all costs associated with data uploaded to the CoC's designated HMIS.

Standard: Agencies participating in HMIS as interface agencies will sign an agreement with the HMIS Lead and provide their own technical support and funding for interface/upload capabilities, and will ensure their data is transmitted in a manner that is timely, complete and accurate.

Purpose: To outline the responsibilities for interface agencies and comply with the Interface Policy (Appendix D)

Procedures Pertaining to Interface Agencies:

Agencies that upload data from their own database into the CoC's HMIS will follow the steps outlined below:

1. Enter into a yearly contract/agreement with the HMIS Lead for technical support, charges incurred due to customizations, to ensure a license allowing uploading of the data and naming the specific staff that will oversee such uploading.

2. The ATA or the interface designated staff must validate and test data uploads to ensure accuracy with HMIS Software Provider before officially submitting data, and monitor data uploads on a regular basis to ensure accuracy.

3. Periodically modify data import format as changes are made to the HUD data standard, or database and CoC workflow changes.

4. Upload all required data at least monthly, or more often, as instructed and required by the HMIS Lead, provided, however, that the HMIS Lead may from time to time direct interface agencies to complete special supplementary uploads to ensure data completeness or to correct data problems, as described below.

Responsibilities of Interface Agency:

The Interface Agency is financial held responsible to ensure that all required data is uploaded in a timely and accurate manner, and that the data is collected and handled in compliance with CoC's established data privacy, data security, and data quality plans, and in compliance with HUD requirements and any other applicable laws or regulations.

The Interface agency will be held responsible for ensuring that data is in the appropriate format. To the extent that the HMIS Lead identifies data quality problems with the uploaded data, it will be the Interface Agency's responsibility to address those data quality problems, including making any necessary corrections in the source data for a subsequent upload, within an agreed upon timeframe. Interface Agencies must upload data at least monthly, and should anticipate a requirement for more frequent upload as the Continuum moves to implement the coordinated intake and assessment system required by HUD.

If the Interface Agency determines that properly formatted data was not correctly uploaded into the HMIS, the Interface Agency shall contact the HMIS Lead to request help in addressing the problem and incur the charges for the changes appropriately. The agency is responsible for all costs incurred to implement, operate, and modify their side of the interface process.

SECTION 2

Operational Policies and Procedures

SOP#: 02-010
Revised#: 02-010 Revised Date: 01/14/2015 Revised by: HMIS Lead
HMIS Participation Policy

Policy: Agencies that are funded by the City or HUD to provide client level services to prevent or address homelessness in Chicago are required to participate in the HMIS. All other providers operating client-level programs to prevent or address homelessness in Chicago are strongly encouraged to participate in the HMIS.

Standard: The HMIS Lead will provide quality HMIS services to all participating agencies.

Purpose: To outline which agencies are expected to participate in the HMIS, the extent to which their participation is mandated or voluntary, and a definition of participation.

Procedure:

Beginning with the 2012 City of Chicago and HUD Emergency Solutions Grants (ESG), all recipients and sub recipients must participate in HMIS. All recipients and sub recipients of HUD Continuum of Care grants, including recipients of legacy Supportive Housing Program (SHP) grants, Section 8 Moderate Rehabilitation SRO grants, and Shelter plus Care grants must participate in the HMIS. Congress and HUD have established that victim services providers and legal assistance providers may satisfy this requirement through use of a comparable data base as described in the applicable HUD regulations.

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 promulgated HUD Data and Technical Standards Final Notice. Recognizing that certain agencies may be further constrained by HIPAA and other Federal, State and local laws, the HMIS Lead shall work with such agencies to develop recommendations to the Planning Council regarding the appropriate level and parameters of their HMIS participation, and shall tailor its agreements with such agencies pursuant to the policies and procedures adopted by the Planning Council, so that those agencies may remain in compliance with applicable laws.

Participation Requirements

Mandated Participation

All providers that are funded by the City or HUD to provide client-level services to prevent or address homelessness in the City of Chicago must meet the Minimum Participation Standards of the HMIS, as defined by this SOP. 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 only HUD and City-funded programs are ***required*** to participate in the HMIS, the HMIS Lead and the Planning Council will strongly encourage an appropriate level of HMIS participation by all programs targeting assistance to homeless persons (e.g., universal fields only for overnight emergency shelters, program fields for programs offering more extended assistance, etc.). While neither the Planning Council nor the HMIS Lead can require non- HUD-funded and non-City-funded providers to participate in the HMIS, they will work to persuasively articulate the benefits of HMIS participation in order to achieve a more comprehensive and accurate understanding of homelessness in Chicago.

Minimum Participation Standards

A client has the right to refuse to have his/her data entered into the HMIS database. The client's individual choice regarding participation will not affect his/her right to services. The only exception to this Standard is for clients who call the Homeless Prevention Call Center (HPCC); as stated under the policy and procedures section.

Minimum participation means:

- Each participating agency shall execute an HMIS Agency Partner Agreement and, if applicable, a Data Sharing Agreement.
- Collecting the universal data elements: Data Collection Requirements, for all programs operated by the agency that primarily serve persons who are homeless or formerly homeless, or that provide client-level ESG-funded homelessness prevention assistance;
- Collecting program-specific data elements: Data Collection Requirements, for all clients served by programs funded under HUD's Continuum of Care program and for some designated programs funded by the City of Chicago; and
- Submitting data to the HMIS using one of the following options:
    - Option 1: Entering client-level data into the HMIS while being in compliance with Data Quality and Monitoring Plan
    - Option 2: Interface agency will be responsible to abide by the Interface policy and for ensuring that the data is in the appropriate format for uploads and being responsible for all costs associated with formatting and uploading data correctly. Upload of data is expected to be in compliance with Data Quality and Monitoring Plan

  - Option 3: In accordance with requirements outlined in HUD regulations, victim services providers and providers of legal assistance shall be deemed in compliance with this requirement by virtue of entering their data into a comparable data base.

- Each CHO shall designate an ATA. The main role of this person is to serve as a liaison between the Agency and the HMIS Lead and is responsible for organizing its agency user's, 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.

Initial HMIS Participation Requirements

Policy: Each CHO must meet all initial participation requirements in order to receive access to the HMIS.

Standard: HMIS Lead will certify that the CHO has met the participation requirements prior to initiating the HMIS.

Purpose: To provide Agencies with clear expectations for their participation in the HMIS.

Requirements:

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

— Call on a meeting to discuss HMIS goals and objectives, requirements, site considerations, and documentation.

— *Agency Partnership Agreement:* An authorized Agency representative is required to execute a Partner Agreement stating the organization's commitment to uphold the policies and procedures for effective use of the HMIS and proper collaboration with the HMIS Lead. An executed Partner Agency Agreement must be in the possession of the HMIS Lead as a precondition for HMIS access.

— *Verification and Documentation, including:*

- All documentation on agency and program information must be submitted to ensure that complete and accurate CHO information is entered within the HMIS. All forms must be in the possession of the HMIS Lead’s as a precondition for HMIS access.
- Agency Technical Administrator: One key staff person or contractor must be designated to serve as the Agency Technical Administrator (ATA) for each CHO.
- Fee payment, if applicable. Each CHO is responsible for individual agency costs related to equipment purchase, equipment maintenance, internet connectivity, and related personnel expenses.

Site Hardware & Connectivity Requirement: Any computer being used to access the HMIS must meet the minimum hardware and recommended connectivity requirements.

Data Migration: All legacy data that will be migrated from a CHO's existing database to the HMIS database must be cleaned, updated, and formatted according to HMIS data specifications prior to migration. The specific requirements for cleaning, updating, formatting, and uploading that data must be individually discussed in advance of uploading with the HMIS Lead.

SOP#: 02-030
Revised#: 02-030 Revised Date: 01/14/2015 Revised by: HMIS Lead
HMIS User Set-Up Procedure

Policy: The HMIS Lead may create a new User ID for eligible individuals based on the following procedure.

Standard: The HMIS Lead must ensure that the following set-up procedure has occurred prior to setting up a new user.

Purpose: To inform all parties involved with the HMIS of the requirements to become an HMIS user.

Responsibilities:

User Requirements

Prior to being granted a username and password, users must:

- Successfully complete all HMIS policy and application training required for assigned user level.
- Execute an HMIS End User Policy and Code of Ethics (Appendix C)

Users must be aware of the sensitivity of client-level data and take appropriate measures to prevent unauthorized disclosure of it. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with the all policy and standards described in these Standard Operating Procedures. Users are accountable for their actions and for any actions undertaken with their usernames and passwords.

The HMIS Lead shall:

- Review HMIS records about previous users to ensure that the individual does not have previous violations with the HMIS SOPs that prohibit access to the HMIS.
- Verify that required training has been successfully completed.
  Note: A new user login with credentials will be created for the user if the user attended the training
- Verify that the required documentation have been correctly executed and submitted.

Once the user ID is established, the ATA is responsible for maintaining the user account. The ATA is responsible for immediately terminating user access if any user leaves employment with the agency, or otherwise no longer needs access to the HMIS and must notify the HMIS Lead team.

If an ATA leaves the agency or deemed no access to the HMIS, it will be the responsibility of the immediate supervisor or CEO/Executive Director to notify the HMIS Lead team immediately.

Volunteers and Interns have the same user requirements as that of a paid staff. 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 CEO or the Executive Director is responsible for ensuring that the user understands and complies with all applicable HMIS SOPs.

Enforcement Mechanisms:

The HMIS Lead team has the right to 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 or Revocation of system privileges

A user may also be subjected to disciplinary action leading to termination of employment is serious or repeated violation(s) of HMIS Policies and Procedures.

SOP#: 02-040
Revised#: 02-040 Revised Date: 01/14/2015 Revised by: HMIS Lead

Homelessness Prevention Call Center Protocol

Policy: The Homelessness Prevention Call Center will utilize HMIS to capture and report data with the exception of the client notification policy that is contrary to their operations and functions as a program that delivers services via telephone or other electronic referral.

Standard: Homelessness Prevention Call Center that delivers services primarily through telephonic or other electronic means is responsible for ensuring that the appropriate procedures are implemented to enforce the client notification and consent policy.

Purpose: To outline the operating procedures for the Homeless Prevention Call Center to contribute data to HMIS.

Responsibilities:

All clients must be informed of their right to participate in HMIS. Clients will be read the privacy notice and given the opportunity to view it on the agency website or pick up a copy at the agency. Callers who do not want their information shared will have their records closed and/or maybe limited in their ability to obtain an agency referral.

SECTION 3

Security and Privacy Policies and Procedures

SOP#: 03-010
Revised#: 03-010 Revised Date: 01/14/2015 Revised by: HMIS Lead

HMIS Client Notification Policy and Procedures

Policy: CHOs shall use the Client Notification and/or consent procedure prior to entering any client-level data into the HMIS.

Standard: The CEO or the Executive Director of each CHO is responsible for ensuring that the agency has implemented appropriate procedures to enforce the client notification and consent procedures.

Purpose: To give client's control of their personal information.

Responsibilities:

The HMIS Lead team with approval from the PC and HMIS Committee has prepared standard documents for HMIS Notice of Privacy Practices and Client Consent to Release Information. CHOs may either use these forms or incorporate the content of these 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 recordkeeping and auditing purposes. The forms that are a part of the privacy packet are:

- HMIS Privacy documents Instructions and Index
- Standard Agency Privacy Posting
- Standard Agency Privacy Practices Notice
- Client Consent Form
- DV Form
- Client Revocation Form

CHOs 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.

CHOs 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.

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.

Client Authorization:

HMIS users may share client information only if the client authorizes that sharing with a valid Client Release of Information form (see exception below for the call center operations).

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 ensure that this data sharing procedure is followed. Specific monitoring procedures around program enrollment will be implemented to ensure appropriate client information access.

Client Revocation:

The client maintains a right to revoke written authorization at any time (except if that policy is over-ridden 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.

Applicability

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

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

Client Data Elements	**Summary of Notification/Consent and Data Sharing Procedures**
Primary Identifying Information: • Name and Aliases • Date of Birth • Gender • Social Security Number • Veteran Status Along with: • Household/Relationship information	*Open Client Record*: If the client does not ask to hide his/her identifiers, the primary identifiers along with Household information under the Summary Tab will be available to all HMIS users in the Client Search to locate an existing client. None of the other client information will be accessible. *Closed Client Record:* If a client disagrees to share his/her primary identifiers, the record must be locked and will appear on the Client Search List only for the originating agency. It will be hidden to all other agencies and searches with the exception of Systems Administrators (HMIS Lead team)
All other Client Information: • Entry/Exit • Service Provided/Transactions Protected Information: • Housing History • Disability • Mental Health • Substance Abuse • HIV/AIDS • Domestic Violence Information • Health Insurance Information	*Closed Client Records:* Client information is available only within the originating service provider to users that have an authorized access level and to authorized, System Administrators for system administration purposes. Any other sharing of this data should be limited to specific partner service providers as a closed exception and requires signed consent from the client.
Program Exceptions: • Primary Identifying Information • HUD COC and ESG Entry Assessment • Homeless Status • Income • Additional resources that could help with housing • Current contact information • Case Manager's contact information	Sharing of data elements for specific programs and/or projects are funding requirements based. *Open Client Records:* The client must agree to provide a written consent before sharing data. *Closed Client Records:* All Client records will remain locked and Clients are made aware that lack of sharing will impact their ability to be screened as eligible for the Rapid Re-housing program

Specific Call Center 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. 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/or may be limited in their ability to obtain an agency referral.

Special Notice and Consent for Persons who May be 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:

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.

SOP#: 03-020
Revised#: 03-020 Revised Date: 01/14/2015 Revised by: HMIS Lead

Data Access Control Policies and Procedures

Policy: HMIS Lead must reasonably secure the HMIS data from access from unauthorized users.

Standard: HMIS Lead or its designee should employ access prevention control measures to secure HMIS database resources.

Purpose: To protect the security of the HMIS database(s).

Guidelines:

User Accounts

Each user's access to data should be defined by their user type and specific agency data-sharing agreements, if any, Agency Technical Administrators must regularly review user access privileges and terminate user IDs and passwords from their systems when users no longer require access.

Users should only be logged into the HMIS from one workstation at any given time.

User Passwords

Each user must have a unique identification code (user ID). Each user's identity will be authenticated using a user password. Passwords are the individual's responsibility. Users are prohibited from sharing user IDs or passwords. Sanctions will be imposed on the user and/or agency if user account sharing occurs.

A temporary password will be automatically generated from the system when a new user is created. Agency Technical Administrators or HMIS Lead will communicate the system-generated password to the user. The user will be asked to establish a permanent password at initial log-in.

The system will force the users to change the passwords once every 45 days. Users at that time will be able select and change their own passwords. A password cannot be re-used until 2 password selections have expired.

Passwords should be between eight and sixteen characters long and not easily guessed or found in a dictionary. The password format is alphanumeric.

Any passwords written down must be securely stored and inaccessible to other persons. Users should not save passwords on a personal computer for easier log on.

Password Reset

Except when prompted by ServicePoint to change an expired password, users cannot reset their own password. The HMIS Lead and in some cases, the Agency Administrator, have the ability to temporarily reset a password. If an Agency Administrator needs to have his/her password set, a member of the HMIS Lead will need to reset that password.

Temporary Suspension of User Access to Database Resources

System Inactivity: Users must logoff from the HMIS and workstation if they leave their workstation. If a user is logged onto a workstation, and the period of inactivity on the workstation exceeds the designated inactivity time period. The user will be automatically logged off of the system. By default the inactivity period is set to 30 minutes – if a user is inactive for 30 minutes, then the user is logged off and must reenter his/her user ID and password in order to resume work.

Unsuccessful logon: If a User unsuccessfully attempts to log on 3 consecutive times, the User ID will be "locked out", access permission revoked and unable to gain access until their password is reset by the HMIS helpdesk or ATA.

Electronic Data Controls

Agency Policies Restricting Access to Data: The CHOs must establish internal access to data protocols based on the final HUD Data and Technical Standards.

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.

Ability to export Agency specific Database from HMIS:

CHOs 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 and Digital Data Controls

Printed versions (hardcopy) of confidential data should not be copied or left unattended and open to compromise. Media containing HMIS client identified data may not be shared with any person or agency other than the owner of the data for any reason not disclosed within the Client Notice.

Agencies policies, consistent with applicable state and federal laws, should be established regarding appropriate locations for storage, transmission, use and disposal of HMIS generated hardcopy or digital data. HMIS data may be transported by authorized employees using methods deemed appropriate by the participating agency that meet the above standard.
Reasonable care should be used, and media should be secured when left unattended. Magnetic media containing HMIS data which is released and/or disposed of from the participating organization and 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 may include shredding finely enough to ensure that the information is unrecoverable.

SOP#: 03-030
Revised#: 03-030 Revised Date: 01/14/2015 Revised by: HMIS Lead

HMIS Agency Hardware, Connectivity and Security Requirements

Policy: Any computer, tablet, smartphone or other such device used to enter data into the HMIS or to access data already in the HMIS must meet the minimum technical and connectivity specifications and comply with applicable data security and privacy requirements established in these SOPs.

Standard: The CHO must certify that they have adequate hardware, connectivity, and data privacy and security protections in place, in order to be granted HMIS access.

Purpose: To provide agencies with minimum requirements for hardware and connectivity.

Requirements:

Workstation Specifications:

Computers using HMIS must meet the minimum specifications below or newer as prescribed by Bowman Systems.

- Operating System: Microsoft Windows XP or better
- Processor: 2 Gigahertz or higher processor (a Dual-Core processor is recommended);
- Memory: 512 MB RAM; for Windows XP: 4Gig recommended (2 Gig minimum); for Windows Vista: 2Gig recommended (1 Gig minimum)
- Web Browser: The latest versions of either Firefox, Internet Explorer, or Chrome are recommended. No additional plugin is required

Internet Specifications:

Agencies directly entering data must have internet connectivity for each workstation that will be accessing the HMIS. To optimize performance, all agencies are encouraged to secure a high speed internet connection with a cable modem or DSL/ISDN or T1 line.

Agencies considering or using a wireless internet configuration must employ higher security measures. A secure internet connection is required and wireless settings must be documented as part of the information security protocol created by each CHO.

Security Specifications:

All workstations directly accessing the HMIS and any workstation that is on a network that has a workstation(s) directly accessing the HMIS must have:

- Operating System Updates. Operating system updates must be downloaded and applied automatically or on a regular basis.
- Adequate firewall protection and apply all critical virus and system updates automatically.

- Virus protection software. Virus definitions must be updated automatically.
- Anti-spyware software. Spyware definitions must be updated automatically.
- Anti-Phishing software. Phishing definitions must be updated automatically.

Agency Workstation Access Control:

Access to the HMIS will be allowed only from computers specifically identified by the CHO's CEO or Executive Director or authorized designee and the ATA. Each agency's ATA will determine the physical access controls appropriate for their organizational settings. Each workstation, including laptops used off-site, should have appropriate and current firewall and virus protection.

SOP#: 03-040
Revised#: 03-040 Revised Date: 01/14/2015 Revised by: HMIS Lead

System Availability

Policy: The HMIS application will be available to users in a manner consistent with the agencies' reasonable usage requirements.

Standard: HMIS Lead staff will operate the system and respond immediately in the event of an interruption to service

Purpose: To define system availability.

Guidelines:

Staff from the HMIS Lead will be available during normal business hours 8:00 – 5:00PM.

Interruption to Service

The HMIS Lead staff will ensure that all users are informed via HMIS email, helpdesk and/or newsletter of any planned interruption to service. An explanation of the need for the interruption, expected duration, and benefits or consequences will be provided.

When an event occurs that makes the system inaccessible and the interruption is expected to exceed two hours, the HMIS lead team will communicate with Bowman Systems, and Agency Administrators will be notified of any information regarding the interruption as it is made available.

SECTION 4

Training and Technical Support

SOP#: 04-010
Revised#: 04-010 Revised Date: 01/14/2015 Revised by: HMIS Lead

HMIS Lead Technical Support

Policy: The HMIS Lead will offer standard technical support services to all CHOs and users.

Standard: Users needing technical support on the HMIS application should access standard technical support services using the guidelines articulated in this policy.

Purpose: To define technical support services.

Guidelines:

As unanticipated technical support questions on the use of the HMIS application arise, users should follow the following procedure to resolve their questions.

ATA's or any HMIS user can:

- Submit any HMIS technical questions through the HMIS portal
    - If question remains unresolved, the HMIS Lead team will further direct the question to Bowman technical support staff.
- ATA's can also access the knowledge base through the HMIS portal at any time to commonly asked questions and issues.

User Training

The HMIS Lead will provide ongoing HMIS software training as stated in the training protocol. The details of the protocol is outlined in this document is also accessible on the HMIS portal.

Agency/User Forms

All Agency Technical Administrators will be trained in the appropriate on-line and hardcopy forms. If the Agency Technical Administrator has questions on how to complete HMIS forms, he/she should contact the HMIS Lead through the portal.

Report Generation

Each CHO may send its ATA to receive training on how to develop agency-specific reports using the advanced reporting tools. The HMIS Lead will be a resource to agency users as they develop reports, but will be available to provide only a limited and deemed reasonable by the team to offer support to each CHO.

SOP#: 04-020
Revised#: 04-020 Revised Date: 01/14/2015 Revised by: HMIS Lead

HMIS User Training Protocol

Policy: HMIS users follow the Training Protocol and must successfully complete training for access to ServicePoint.

Standard: The HMIS Lead will not create a user ID until successful completion of required training is attended.

Purpose: To inform users of the training requirements to access the HMIS.

Responsibilities:

Training Protocol:

HMIS Training Protocol for New Users:

Training Calendar:

HMIS New User Trainings are offered on the first and third Thursdays of every month. In addition, the third Monday of each month is available for New User agency-specific on-site training as needed. These training dates are available on a shared Google document. ATAs have access to the link to this calendar and can view it for training details and updates regarding openings.

Registration:

New employees (or those new to using HMIS) can contact hmis@allchicago.org to request a link to the New User Training Registration Form. The link to the Google document will be sent to the New User.
The New User will be asked to specify their ServicePoint user role and the programs they will be entering data for within HMIS. In addition, the New User will specify the exact training date that they would like to attend. The registration form includes information about the need to attend the selected training and emphasizes this expectation. In addition, the form asks for the supervisor's contact information to ensure that he or she will be notified if the New User does not attend the selected training.

Once the registration is reviewed by the HMIS Team, a confirmation email will be sent to the New User via an Outlook meeting invitation. The invitation will include the date, time, and location of the selected training along with other helpful information. The New User is encouraged to "accept" this information to confirm its receipt.

Licensure of New Users:

HMIS New Users will participate in the specific training designed to familiarize them with the ServicePoint site and to train them in the Chicago HMIS Workflow. Following their successful completion of training, the New User will receive their user name and password. The New User will gain access to the ServicePoint site at the close of the in person training.

New Users are encouraged to remain active users within the HMIS ServicePoint site. They are asked to log into the site within two weeks following their training. The New Users are asked to remain engaged with the site and the data entry and review process to both ensure appropriate interface with it and the entry of quality information.

Ongoing Training and Support:

At the close of the HMIS New User Training, participants and provided with information regarding the HMIS New Users Forum. This New Users Forum is scheduled in approximately two to three weeks following their participation in their initial training. The meeting takes place via webinar and is structured to allow New Users to share feedback regarding their training experience and to highlight any challenges they are experiencing when attempting to independently enter data into or access ServicePoint. The New Users are encouraged to participate and to share their questions and challenges. This session's goal is to add one more means of supporting New Users as they navigate ServicePoint.

HMIS Specialized Training for Current Users:

Training Calendar and Announcements:

The ongoing trainings for Current HMIS Users are detailed on the HMIS Training calendar. The ATAs have access to this calendar and also receive training announcements via email from the HMIS team. ATAs are asked to communicate the training announcements and details to their programs.

Trainings may also be highlighted within the System News in the ServicePoint site. Current HMIS Users are encouraged to continue to access the site and to review the System News to ensure that they receive all of the related information.

Registration for In-Person Trainings:

Current Users can contact hmis@allchicago.org to request a link to the Training Registration Form. In addition, this link is emailed to the ATAs and can be received from their agency representative.

The Current User will be asked to complete the information on the Training Registration Form to participate in the selected training. Their attendance in the selected training is important and they are asked to register only if they can participate. The registration form asks for the supervisor's contact information to ensure that he or she will be notified if their Current User does not attend the selected training. Once the registration is reviewed by the HMIS Team, a confirmation email will be sent to the Current User via an Outlook meeting invitation. The invitation will include the date, time, and location of the selected training along with other helpful information. The Current User is encouraged to "accept" this information to confirm its receipt.

Registration for Online/Webinar-based Trainings:

Webinar-based Trainings allow Current Users to register for each session via a Go-To-Webinar link. Once they complete the registration process, they will receive an email that confirms their participation and provides a unique login to use to join the training. Webinar-based Trainings allow for a number of Current Users to participate in the presented session. It is important that the Current Users register only if they can attend the selected session. Their supervisors will also receive notification if they do not attend the scheduled session.

SECTION 5

Appendix A-C

Appendix A: Glossary of HMIS Acronyms and Terms

Acronyms

AIRS - Alliance of Information & Referral Systems
AHAR - Annual Homeless Assessment Report
APR - Annual Performance Report
CDBG – Community Development Block Grant
CoC - Continuum of Care
DOB - Date of Birth
DV - Domestic Violence
ESG - Emergency Solutions Grants
eHIC – electronic Housing Inventory Chart
FIPS - Federal Information Processing Standards Codes for states, counties, and named populated places.
HEARTH – Homeless Emergency Assistance and Rapid Transition to Housing
HIPAA - Health Insurance Portability and Accountability Act of 1996
HMIS - Homeless Management Information System
HUD - U.S. Department of Housing and Urban Development
I&R - Information and Referral
MH - Mental Health
NOFA - Notice of Funding Availability
PIT - Point in Time
PKI - Public Key Infrastructure
PPI - Personal Protected Information
S+C - Shelter Plus Care (McKinney-Vento Program)
SA - Substance Abuse
SHP - Supportive Housing Program
SRO - Single Room Occupancy
SSN - Social Security Number
SSI - Supplemental Security Income
SSO - Supportive Services Only
TA - Technical Assistance
TANF - Temporary Assistance for Needy Families
VAWA - Violence Against Women Act
XML - Extensible Markup Language

Glossary

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.

Chronic Homelessness
HUD defines a chronically homeless person as a homeless individual with a disabling condition who has either been continuously homeless for a year or more OR has had at least four (4) episodes of homelessness in the past three (3) years. To be considered chronically homeless, persons must have been sleeping in a place not meant for human habitation (e.g., living on the streets) and/or in an emergency homeless shelter during that time. Persons under the age of 18 are not counted as chronically homeless individuals.

Chronically Homeless Household
HUD defines a chronically household as a family that has at least one adult member (persons 18 or older) who has a disabling condition who has either been continuously homeless for a year or more OR has had at least four (4) episodes of homelessness in the past three (3) years. To be considered chronically homeless, persons must have been sleeping in a place not meant for human habitation (e.g., living on the streets) and/or in an emergency shelter/safe haven during that time.

Community Development Block Grant (CDBG)
A flexible program that provides communities with resources to address a wide range of unique community development needs. Beginning in 1974, the CDBG program is one of the longest continuously run programs at HUD. The CDBG program provides annual grants on a formula basis to 1,180 general units of local and State governments.

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

Consumer
An individual or family who has experienced or is currently experiencing 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.

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

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

Data Standards
See HMIS Data and Technical Standards Final Notice.

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 (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 his/her 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 his/her judgment not impaired at the time of consenting (by sleep, illness, intoxication, alcohol, drugs or other health problems, etc.).

Information and Referral
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.

Penetration Testing
The process of probing a computer system with the goal of identifying security vulnerabilities in a network and the extent to which outside parties might exploit them.

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

Public Keys
Public keys are included in digital certificates and contain information that a sender can use to encrypt information such that only a particular key can read it. The recipient can also verify the identity of the sender through the sender`s public key. 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.

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.

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.

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
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.

Appendix B: License Management Protocol

The purpose of the protocol is to ensure data security from a possible data breach and unwanted actions of unauthorized users. This outlines assignment and revocation of user licenses that provides access to Chicago's Homeless Management Information System (HMIS).

Access control to HMIS for users requires participation in the specific training designed to familiarize them with the ServicePoint site and to train them in the Chicago HMIS Workflow.

For New Users:

1) At the close of the New User Training, each user will be provided with a Username and a temporary Password.
2) It is anticipated that the new user will login in and begin using Service Point during the two week period following their training.
3) Failure to login within two weeks may result in the user account being "Inactivated"
4) Continued inactivity for a month, from the date of the training will result in license revocation. The user's account will be "Deleted" and will no longer have access to the HMIS.

For Current Users:

1) If a current user has been inactive in the system for more than 120 days, (from last login) the user account will be "Inactivated"
2) Continued inactivity for more than 180 days will result in license revocation and the account being "Deleted".

License Re-activation:

1) If the user's HMIS account has been "Inactivated", the user can send a request to the HMIS helpdesk to request reactivation.
2) If the user's HMIS account has been "Deleted", the user is required to attend training* before re-activation.

* Please note that trainings are subjected to availability and a user may have to wait a few weeks before being able to register again. There will be no priority for training scheduling.

Appendix C: HMIS End User Policy and Code of Ethics

HMIS User Name and Title (Please Print)

USER POLICY

Partner Agencies who uses Chicago Homeless Management Information System (HMIS) and each User within any Partner Agency is bound by various restrictions regarding Protected Personal Information **("PPI")**[1]. The employee, contractor, or volunteer whose name appears above is the **User**.

It is a **Client's** decision about what level of PPI information is to be shared with any Partner Agencies.

The **Client Consent Form** for data sharing shall be signed by the Client before any PPI is designated for sharing with any Partner Agencies, or in the case of the Homelessness Prevention Call Center, verbal consent shall be obtained as described in the HMIS Standard Operating Procedure. The User shall ensure that prior to obtaining Client's consent; the agency's HMIS Notice of Privacy Practices was fully reviewed with Client in a manner to ensure that Client fully understood the information.

USER PRINCIPLES

A User ID and Password gives you access to the Chicago HMIS. **You must initial each item below** to indicate your understanding and acceptance of the proper use of your ID and password. Failure to uphold the confidentiality standards set forth below is grounds for your immediate termination from HMIS.

(Initial each line below)

	I understand that I have an obligation to maintain Client privacy and to protect and safeguard the confidentiality of Client's PPI. PPI shall include, but not be limited to, the Client's name, address, telephone number, social security number, type of medical care provided, medical condition or diagnosis, veteran status, employment information, and any and all other information relating to the Client's programming.
	My User ID and Password are for my use only and **must not** be shared with anyone, including my supervisor(s). I must take all reasonable means to keep my Password physically secure.
	I understand that the only individuals who can view information in the HMIS are authorized users who need the information for legitimate business purposes of this Agency and the Clients to whom the information pertains.
	I may only view, obtain, disclose, or use information within the HMIS that is necessary to perform my job.
	If I am logged into the HMIS and must leave the work area where the computer is located, I **must secure the computer** before leaving the work area.
	Any hard copies of PPI printed from the HMIS must be kept in a secure file, and destroyed when no longer needed, in accordance with Agency's records retention policy. I will not leave hard copies of PPI in public view including, but not limited to on desks, or on a photocopier, printer, or fax machine.
	I will not discuss PPI with anyone in a public area.
	I have reviewed the Agency's HMIS Notice of Privacy Practices and the HMIS Standard Operating Procedures, understand each of those documents, and agree to abide by them.
	If I notice or suspect a security breach, I must immediately notify the Executive Director of the Agency and the HMIS System Administrator at hmis@allchicago.org
	I understand that any violation of this Agreement may also be considered a violation of my employment relationship with this Agency, and could result in disciplinary action, up to and including termination of my employment or affiliation with Agency, as well as potential personal civil and criminal legal fines and penalties.

USER CODE OF ETHICS

[1] Protected Personal Information is information about a client: (1) whose identity is apparent from the information or can reasonably be ascertained from the information; or (2) whose identity can be learned, taking into account any methods reasonably likely to be used, by linking the information with other available information or by otherwise manipulating the information.

A. Users must be prepared to answer Client questions regarding the HMIS.

B. Users must respect Client preferences with regard to the sharing of PPI within the HMIS. Users must accurately record Client's preferences by making the proper designations as to sharing of PPI and/or any restrictions on the sharing of PPI.

C. Users must allow Client to change his or her information sharing preferences at the Client's request (*i.e.*, to revoke consent) (except if that policy is over-ridden by Agency policy or if the information is required to be shared as a condition of a provider agreement).

D. The User has primary responsibility for information entered by the User. Information Users enter must be truthful, accurate and complete to the best of User's knowledge.

E. Users will not solicit from or enter information about Clients into the HMIS unless the information is required for a legitimate business purpose such as to provide services to the Client.

F. Users will not include profanity or offensive language in the HMIS; nor will Users use the HMIS database for any violation of any law, to defraud any entity or conduct any illegal activity.

PASSWORD PROCEDURES

By signing this Agreement, the User agrees to the following:

Passwords are the User's responsibility and the User may not share passwords. They should be securely stored and inaccessible to other persons—including your supervisor(s). Passwords should never be stored or displayed in any publicly accessible location without the HMIS Lead permission.

USER GRIEVANCE PROCEDURE

If a User has a grievance with this Code of Ethics, that User may send a written complaint to their HMIS Agency Technical Administrator (ATA). If the complaint is not resolved to the User's satisfaction, the User may send a written complaint to: All Chicago Making Homelessness History;
651, W. Washington, Suite 504, Chicago IL 60661

Attn: HMIS System Administrator.

I understand and agree to comply with the above User Policy, User Principles, User Responsibilities, Password Procedures, and User Grievance Procedure.

______________________________ HMIS User Signature

______________________________ Date

HMIS User Login (Username) ______________________________

Email Address ______________________________

______________________________ Supervisor Signature

______________________________ Date

Appendix D: HMIS Interface Policy

This Policy outlines the responsibilities and defines compliance for Interface Agencies.

Agencies that have received approval prior to September 19, 2012 may continue to contribute data to HMIS as an interface agency and will be responsible for ensuring the timeliness, accuracy and assume all costs associated with data uploaded to the CoC's designated HMIS.

Contributing HMIS Organizations (CHOs) will not receive authorization to transition from direct to interface data entry. It has been determined the quality and completeness of the HMIS will effectively be maintained through frequent and direct entry of data by the CHOs.

Standard: Agencies participating in HMIS as interface agencies will sign an agreement with the HMIS Lead and provide their own technical support and funding for interface capabilities, and will ensure their data is transmitted in a manner that is timely, complete and accurate per CoC requirements.

Procedures Pertaining to Interface Agencies:

Agencies that upload data from an external database into the CoC's HMIS will follow the steps outlined below:

1. Enter into a yearly agreement with the HMIS Lead Agency for technical support, charges incurred due to customization requests, licensing that allows uploading of the data and designate a staff who will oversee the uploading process.

2. The Agency Technical Administrator (ATA) or the interface designated staff must validate and test data uploads to ensure accuracy with the HMIS Software Provider before officially submitting data and monitor data uploads on a regular basis to ensure accuracy.

3. Periodically modify data import format as changes are made including, but not limited to the HUD Data Standards or CoC workflow changes.

4. Upload all required data at least monthly, or more often, if so instructed and required by the HMIS Lead, provided, however, the HMIS Lead may from time to time direct interface agencies to complete special supplementary uploads to ensure data completeness or to correct data problems, as described below.

Responsibilities of Interface Agency:

The Interface Agency is held financially responsible for ensuring all required data is uploaded in a timely and accurate manner, and the data is collected and handled in compliance with the HMIS established data privacy, data security, and data quality plans, and in compliance with HUD requirements and any other applicable laws or regulations.

The Interface agency will be held responsible for ensuring data is in the appropriate format. To the extent the HMIS Lead identifies data quality problems with the uploaded data, it will be the Interface Agency's responsibility to address those data quality problems, including making any necessary corrections in the source data for a subsequent upload, within an agreed upon timeframe. Interface Agencies must upload data at least monthly, and should anticipate a requirement for more frequent uploads as the Continuum moves to implement the Coordinated Access and Assessment System required by HUD.

If the Interface Agency determines properly formatted data was not correctly uploaded into the HMIS, the Interface Agency should contact the HMIS Lead within a week following the upload to request help in addressing the problem and incur the appropriate charges, if any.

Compliance:

It is the responsibility of the Interface Agency to ensure compliance with all uploading and data quality requirements.

In general, for all HUD funded programs, lack of compliance with data quality requirements may result in forfeiting points in the HMIS section of the local HUD NOFA Evaluation Instrument, as determined annually by HMV. Similar negative impact may occur on DFSS evaluations and grants which require the use of HMIS reporting.

Expectations:

- Interface agencies as of receipt of the policy will have three months to start uploading data.
- The HMIS Lead will continue to oversee all communication between the HMIS Software Provider and the interface agency to ensure all upload requirements are being met
- If for unforeseen reasons, the upload implementation extends beyond three months or if issues arise during important reporting periods (such as AHAR, CoC Competition etc.) it will be the agency’s responsibility to determine an alternative plan to ensure data is entered and corrected in the system to meet reporting deadlines and be in compliance.
- It will be the agency’s responsibility to incur all appropriate charges during the process.

SECTION 6

Version Control

Policy in effect as of: January 14, 2015

VERSION CONTROL

This document is to keep track of all changes made to this document:

SOP Section #:	Revised Section #	Revised Date:	Revised By:	Comments, if any