East Saint Louis/Belleville/Saint Clair County
Continuum of Care IL 508

Homeless Management Information System

(HMIS)

Policies and Procedures Manual

This manual has been reviewed by the East Saint Louis/Belleville/Saint Clair County Continuum of Care IL-508 Board of Directors.

IN WITNESS WHEREOF, the undersigned parties have caused this manual to take effect when the official's sign and date below.

Continuum of Care IL 508 Board Chairperson

By: _____

Title: _____

Date: _____

St. Clair County Intergovernmental Grants Department

By: _____

Title: _____

Date: _____

East Saint Louis/Belleville/Saint Clair County
Continuum of Care IL 508

Board Members

(June 2022)

Rick Stubblefield, Chairperson

Kesha Chatman, Vice Chairperson

Julie Poplstein, Secretary

James Kellerman, Assistant Secretary

Lisa Atkins, Member

Raeven Weaver, Member

Diane Bonner, Member

Susan Rehrig, Member

Kelly Clemmons, Member

Cara Moellenhoff, Member

Larry McLean, Member

Stacy Lautz, Member

Sandra Northern, Member

Darlene Jones, Member

Table of Contents

Attachments

Agency Partner Agreement

User Policy, Responsibility Statement and Code of Ethics

Privacy and Security Notice and HMIS Consumer Notice

Client HMIS Consent

Project Information Form

End User Access List and User Access Checklist

Background

Homeless Management Information System (HMIS)

HMIS Is a software application used to collect demographic information on people served. The purpose of HMIS is to record and store client-level information about the numbers, characteristics and needs of persons who use homeless housing and supportive services and about persons who receive assistance for persons at risk of homelessness over time to produce an unduplicated count of homeless persons for each Continuum of Care; to understand the extent and nature of homelessness locally, regionally and nationally; and to understand patterns of serv ice use and measure the effectiveness of programs.

Project Participation

The Homeless Emergency Assistance and Rapid Transition to Housing Act (HEARTH Act) address the homeless assistance and prevention programs that must utilize HMI S. HEARTH Act clarifies that all recipients of financial assistance under the Continuum of Care Program (CoC), the Rural Housing Stability Assistance programand HUD programs previously funded under the McKinney-Vento Act (the Supportive Housing Program, the Shelter Plus Care program and the Section 8 Single Room Occupancy Moderate Rehabilitation program) are required to use HMIS b collect client-level data on persons served. In addition, projects receiving funding under Emergency Solutions Grant (ESG) programs are required to participate in HMIS. Homeless and non-homeless projects not funded under any above listed programs may participate in the HMIS. Victim service providers are prohibited ed from entering data directly into the HMIS and legal service providers may choose not to use HMIS; however, victim service providers and legal service providers that are recipients of CoC Program or ESG Program funds must use a comparable database that meets HUD HMIS Standards.

HMIS Lead Agency

St. Clair County Intergovernmental Grants Department serves as the HMIS Lead agency forthe East Saint Louis/ Belleville/ Saint Clair County Continuum of Care IL 508. Designated through a governance agreement to manage and coordinate all HMIS operations and activities at the direction of the Coe Executive Committee. The responsibilities include executing written HMIS Participation Agreement with each Contributing HMIS Organization (CHO), conducting a training for CHO's on security and data quality standards with use of HMIS, compliance with HUD HMIS standards, and developing local HMIS operational policies and procedures.

HMIS Data Standards

The HMIS Project has adopted the HUD requirements whereby all agencies participating in HMIS are to collect a standard set of client information, known as the Universal Data Elements. Within the CoC, there are additional Program Specific

Data Elements that are also required in order to produce the necessary CoC level aggregate reports.

Agencies are responsible for knowing all the Universal and Program Specific Data Elements. These data elements can be found in HUD's "Homeless Management Information System Data Standards". These Standards may be accessed at www.hudexchange.info.

All participating agencies will collect HUD Universal Data Elements for baseline HMIS data-entry. Universal Data Elements are as follows:

1. Name;
2. Full Social Security Number;
3. Date of Birth;
4. Race;
5. Ethnicity;
6. Gender;
7. Veteran Status;
8. Disabling Condition;
9. Prior Living Situation
    - Length of stay in prior living situation
    - Date Homelessness Started
    - Number of times the Client has been on the streets, in ES in the past three years
    - Total number of months homeless on the street or in ES in the past three years
    -
10. Zip of Last Permanent Residence;
11. Project Start Date;
12. Project Exit Date;
13. Destination;
14. Relationship to head of household;
15. Client location;
16. Housing Move-In Date and

All participating agencies will collect Coe Program Specific categories. Program Specific Data Elements are as follows:

1. Income and sources;
2. Non-cash benefits;
3. Health Insurance;
4. Physical disability;
5. Developmental disability;
6. Chronic health condition;
7. **HIV/AIDS;**
8. Mental Health Disorder;
9. Substance Use Disorder;
10. Domestic violence
11. Current Living Situation
12. Date of Engagement
13. ;
14. Contact;

15. Date of engagement;
16. Services Provided;
17. Financial Assistance Provided;
18. Referrals Provided;
19.
20. Housing Assessment Disposition; and
21. Housing Assessment at Exit.

Please note that additional data may be required for a specific program. The above listed data elements are not inclusive to all projects recording data in HMIS.

Compliance:

- Data Timeliness: Client data should be entered in HMIS within 3 business days.
- Data Completeness: There should be no missing (null) data for required elements. Responses that fall under unknown (don't know or refused) should not exceed 5%.
- Data Accuracy: The percentage of client files with inaccurate HMIS data shall not exceed 5%. For example, if the sampling includes 20 client files, then 19 out of 20 of these files must have the entire set of corresponding data entered correctly in HMIS.

Standard Operating Procedures

Agency Participation

HMIS Access is available to HUD CoC Program providers, Emergency Solutions Grant (ESG) service providers and other service providers in the East Saint Louis/Belleville/Saint Clair County Continuum of Care IL- 508 geographical service area. Service providers must be actively involved with the local Continuum of Care and receive validation from a federal program funder/service provider. Final Approval of HMIS access is granted by the HMIS lead agency.

Procedure:

HMIS Utilization Request – ALL HUD Required Participation

- Following the announcement of a renewal grant or an initial grant award, the partner agency will submit and/or update the following documents to the HMIS Lead agency:
    1. Agency Partner Agreement (Attachment A)
    2. Project Information Form (Attachment D)
    3. End User List (Attachment E)

Please submit HMIS agency participation documents to the HMIS Lead agency:

Attention: HRC Coordinator
St. Clair County
Intergovernmental Grants Department
19 Public Square, Suite 200
Belleville, IL 62220
(618) 825-3218
Christina.Anderson@co.st-clair.il.us

- Please allow 30 days for full HMIS utilization following the submission of a new participating agency request or new project request.

HMIS Projects

Any HMIS participating agency can utilize HMIS for the data collection of any project.
Requests for additional projects must be submitted in writing accompanied with an updated Project Information Form (Attachment D). Any project requests that are not in line with HUD data standards and that require additional report formats are subject to additional costs.

End User Participation

HMIS Access is available to individuals identified by an approved participating agency. The individual must have completed New User and Confidentiality training prior to HMIS access.

Procedures:

Adding End Users

- The participating agency authorized representative will I submit a request to add a new end user under their agency. The request must be submitted in writing to the HMIS Lead agency accompanied with the following:

    1. User Policy, Responsibility Statement and Code of Ethics Agreement (Attachment B);
    2. End User Access List (Attachment E),

- New End Users will complete the New User Training and Confidentiality Training by accessing the Pathways MISI website: https://www.pcni.org/training. The trainings are followed by a short quiz and a request for the new user's e-mail address. Upon completing the quiz, the system will send an e-mail confirmation to the new user and the quiz score.

- The new user will forward the confirmation e-mail to the HMIS Lead. Once received, a User ID and temporary password will be issued. Please note, if a new user receives a score below 70, a user ID and password will not be generated. The HMIS Lead must be contacted.

  HMIS data entry is accessed through Pathways MISI at the following website: https://sp5.servicept.com/illinois

Additional training inciudes the following:

- Continuum of Care (CoC) Program Reporting - HUD Annual Progress Report.
- Emergency Solutions Grant (ESG) Reporting - Progress Reports for Coe monitored ESG Grantees.

Additional trainings are offered on-line and are accessible through https://www.pcni.org/training.. Additional End User assistance is also available through the HMIS Support portal at https://help.pathwaysmisi.org/support/home.

Terminating End Users

If end-user participation is terminated at the agency level, the Partner Agency's Executive Director or other authorized representative must submitin writing a request to terminate HMIS access within 24 hours and include an updated End user Access List .

End User Access

Any staff or other person who has been granted a User ID and password that is found to have willfully committed a breach of system security and/or client confidentiality shall have his or her access to the database revoked immediately.
Any person who has been granted a User ID and password that is found to have committed a negligent breach of system security and/or client confidentiality after a warning and correction shall have his or her access to the database revoked immediately. A revoked user may be subject to discipline by the Agency pursuant to the Agency's personnel policies.

All participating end users will be assigned a username and password for use by the identified end user and this user ID and password shall not be shared with anyone.

Termination of Agency Participation

If an agency decides to end participation in HMIS, the participating agency will no longer have access to HMIS. The HMIS Lead, under the direction of the Continuum of Care, shall make reasonable accommodations to assist the participating agency to export data. Any costs associated with exporting the data will be the sole responsibility of the participating agency.

Partner Agency HMIS Participation Termination

Voluntary

- The Partner Agency shall inform the HMIS Lead Agency in writing of their intention to terminate their agreement to participate in HMIS.
- The HMIS Lead Agency will keep all termination records on file with the associated Agency Partner Agreement.

Lack of Compliance

- When the HMIS Lead Agency determines that a Partner Agency is in violation of the terms of the partnership, the Agency will be reported to the CoC Board of Directors in effort to work with the Executive Director of Partner Agency to resolve the conflict(s).
- If the Executive Director is unable to resolve the conflict(s), the CoC Board of Directors will be called upon to resolve the conflict. If that results in a ruling of termination:
    1. The Partner Agency will be notified in writing of the intention to terminate their participation in HMIS.
    2. The HMIS Lead Agency will notify Pathways MISI to revoke access of the Partner Agency endusers to HMIS.
    3. The HMIS Lead Agency will keep all termination records on file with the associated Partner Agency Agreement.

HMIS Security and Access Requirements

All workstations accessing the HMIS need to be protected by a securely configured firewall that is installed at a point between the network and the internet. Each workstation also must have an anti-virus and anti-spyware program.

Site Security Assessment

1. Prior to HMIS access, the HMIS Lead Agency will review and assess the security measures in place to protect client data.

All computers authorized to access HMIS must meet the following minimum requirements:

- Internet Access: HMIS Partner Agencies need to have an Internet connection.
-
- Firewall protection: It is required that all computers used to access HMIS have up-to-date firewall protection with automatic updates.

- Anti-virus protection: All computers used to access HMIS database require up-to-date anti-virus protection software. Anti-virus protection software should be set to update automatically and should be checked periodically toensure it is current.

- Log-On Password Protection: All computers used to access HMIS database-require log-on passwords.

- Password protected screen-saver: All computers used to access HMIS require an up-to-date password protected screen-saver. The screen-saver should beset to turn on every 2-3 minutes when the computer is not in use.

Workstation Security Procedures

- Workstation monitors are to be placed in such a manner as to prohibit unauthorized individuals from viewing the data on the screen. When unable to achieve this, the use of a privacy screen on the monitor is allowed.

- If it is necessary to write down your HMIS username and/or passwords, it must be stored in a secure location such as a locked drawer or cabinet. This information should not be placed under a keyboard, monitor, or in any location where non-designated HMIS Users may find it. Do not share your login information with anyone.

- When you are away from your computer, log out of HMIS and lock down your workstation.

Hard Copy Security – All files with client information are stored in a locked cabinet/office. No papers will be left on a desk.

Data Sharing

The HMIS in St. Clair County is a shared, "open" data system. This means identifying client data can be viewed by any agency that has signed a Data Sharing Agreement. Sharing data enables agencies to coordinate care across multiple providers, reduces data entry and minimizes the burden on the client to re-tell their story.

Some Partner Agencies, require enhanced security and privacy requirements based on the vulnerability of the population they serve. This includes providers covered by the Health Insurance Portability and Accountability Act (HIPAA), Clients participating in these programs will have "closed" files that are only visible to Users at the agency providing services.

User Group Meetings

All HMIS participating agencies are required to have a designated person to participate in User Group Meetings. Both CoC projects and Non CoC projects must participate at some level due to the importance of system data quality.

User group meetings will provide feedback on system performance and the need for system enhancements. Meetings also allow for input and support for policy enforcement and serves as the link between end users and the HMIS Lead. Meetings will increase training and help to ensure proper procedures are taking place and all paperwork and confidentiality requirements are being followed at the agency level. The designated person is expected to effectively communicate what is covered in the meetings to all end users at the participating agency.

User group meetings are normally scheduled for the third Thursday of the month. The meeting location is St. Clair County Intergovernmental Grants Department at 19 Public Square, Suite 200 in Belleville, IL or via zoom from 2:00 pm -3:00pm.

Confidentiality and Privacy

All participating agencies shall only release client HMIS information with written consent by the client, unless otherwise provided in the relevant laws and regulations.

All participating agencies shall abide by all local, state and federal confidentiality laws and regulations pertaining to: 1) all medical conditions, including mental illness, alcohol and/or drug abuse, HIV/AIDS diagnosis and other such covered conditions; and 2) a person's status as a victim of domestic violence. A general authorization for the release of medical or other information is not enough for this purpose. The Agency is encouraged to seek its own legal advice if a non-partner agency requests identifying confidential client information.

All participating agencies shall provide a verbal explanation of the HMIS database and the terms of consent to the Clients and shall arrange for a qualified interpreter or translator if an individual is not literate in English or has difficulty understanding the Consent form. In addition, the Privacy and Security Notice and HMIS Consumer Notice must be posted in a way it is visible to all clients. In addition, if any agency serves clients whose first language is not English,the agency must provide a translated version.

The Agency shall utilize the HMIS Client Consent-Release of Information form, as developed in conjunction and coordination with Partner Agencies, for all clients providing information to the HMIS. The Client Consent-Release of Information form, once signed by the Client, authorizes Client data to be shared with other providers to coordinate services in the HMIS database and authorizes information sharing with Partner Agencies for the period of one year, subject to the restrictions defined by the Client Consent form. The Agency shall keep signed copies of the Client Consent-Release of Information form for a period of five years. If the Agency is governed by the Health Insurance Portability and Accountability Act (HIPAA), the Agency must utilize its own HIPAA- compliant Consent to Release Information form in addition to the HMIS Client Consent form.

HMIS Data Use

The Lead Agency and the HAC shall use only unidentified aggregate HMIS data for homeless policy and planning activities, in preparing federal, state or local applications for homelessness funding, to demonstrate the need for and effectiveness of programs and to obtain a system-wide view of program utilization in the County. The Agency agrees to allow the HAC Executive Committee to obtain information from the HMIS system for performance monitoring.

Data Entry

Accurate data collection is important for the coordination of services across multiple agencies, determining eligibility for client services, and generating reports.

CoC Level reporting changes are made known through the monthly user group meetings.

Data sharing is allowed only between funding sources or by client consent.

Agency staff shall enter client-level data into the HMIS within 3 working days of client interaction.

The Agency shall consistently enter information into the HMIS database and shall strive for real-time, or close to real-time data entry. "Close to real-time data entry"is defined as within three working days of seeing the Client.

When a client revokes his or her consent to share information in the HMIS database, the Agency shall notify the HMIS Lead Agency of the revocation within 24hours. When the System Administrator is notified of a client revocation, the System Administrator shall remove access to all identifying information about that client within 24 hours.

HMIS Help Desk

- Technical support with HMIS is accessed thru Pathways MISI at: help.pathwaysmisi.org/support/home **or 1-800-536-6474**

Data Quality Plan

The HMIS Lead Agency will work with System Administrators to provide monthly data quality reports to each participating agency to ensure client data stored in HMIS data is as accurate and complete as possible. The HMIS System Administrator will run data quality reports for all provider agencies participating in HMIS on a monthly basis. An email summarizing the agency's potential data quality issues will be sent to a specified contact, with a full report of all agencies' issues sent to the HMIS Lead Agency. Data Quality reports will:

- List Data Quality issues at a client level to make corrections easier
- Specify the project and location (entry or exit assessment) of the affected data
- Include data inconsistencies causing data validation issues (conflicting income answers, disabling condition and disabilities answers)

HMIS Users are expected to:

- correct data quality issues within 10 days.
- contact Pathways MISI staff (by phone or through the support portal) for assistance in resolving issues when necessary
- report to the HMIS Lead agency persistent issues or unresolved assistance requests.

HMIS Operating Form Attachments

Agency Partner Agreement

All agencies approved to access HMIS must have signed an Agency Partner Agreement (Attachment A) and agree to abide by the policies and procedures as outlined in this document. The Agency Partner Agreement is a contract between the Partner Agency and the HMIS Lead Agency. The Agency Partner Agreement outlines specific requirements on confidentiality, HMIS use, data entry, system security, and reporting. Any questions regarding the terms of the Agency Partner Agreement should be submitted to the HMIS Lead Agency. The terms of this agreement will be so long as both parties agree and may be amended from time to time.

User Policy, Responsibility Statement, and Code of Ethics

All end users approved to access HMIS must have signed a User Policy, Responsibility Statement, and Code of Ethics Agreement (Attachment B) to abide by the policies and procedures outlined in the document and the responsibilities of the Agency Partner Agreement. The certification acknowledges that each end user shall utilize all identified privacy, ethics, and responsibilities practices with collection and storage of client level data. The terms of this agreement will be so long as both parties agree and may amended from time to time.

Privacy and Security Notice and HMIS Consumer Notice

All agencies approved to access HMIS must have posted at the data collection site the HMIS Privacy and Security Notice (Attachment C). This Notice describes what information will be collected from the client and how the information is used. This Notice also details client rights regarding HMIS.

The Notice must be posted in a way it is visible to all clients. In addition, if any agency serves client s whose first language is not English, the agency must provide a translated version.

Project Information Form

All agencies approved to access HMIS must have submitted to the HMIS Lead Agency a current Project Information Form. This document serves to ensure that the most current project information is included in HMIS. Any project changes or updates should be forwarded to the HMIS Lead to update as soon as possible.

End User Access List

All agencies approved to access HMIS must have submitted to the HMIS Lead Agency a current End User Access List. This document serves to verify all CHO's end user access. If an end user access is terminated by the CHO, the HMIS Lead should be notified immediately to end access to the system AND the End User Access list should be updated and submitted. Agencies should review annually for update.

1. Agency Partner Agreement (Attachment A)
2. User Policy, Responsibility Statement, and Code of Ethics Agreement (Attachment B)
3. HMIS Privacy and Security Notice (Attachment C)
4. Project Information Form (Attachment D)
5. End User Access List (Attachment E)
6. HMIS Monitoring Checklist (Attachment F)

HOMELESS MANAGEMENT INFORMATION SYSTEM
Agency Partner Agreement

The Homeless Management Information System (hereinafter "HMIS") is a client information system that provides a standardized assessment of consumer needs, creates individualized services plans and records the use of housing and services which communities can use to determine the utilization of services of participating agencies, identifying gaps in the local service continuum and develop outcome measurements.

The St. Clair County Intergovernmental Grants Department ("IGD") has been selected by the HAC as the Lead HMIS Program Administrator. Municipal Information Systems, Inc. (MISI) has been selected by the HAC as the HMIS Vendor. In this Agency Partner Agreement (hereinafter "Agreement"), "Client" is a consumer of services; "Agency" is the Agency named in this Agreement; and "Partner Agencies" are all the Agencies participating in HMIS.

The Executive Director of the Agency must indicate agreement with the terms set forth below by signing this Agreement.

I. Confidentiality

A. The Agency shall uphold relevant federal, state and local confidentiality regulations and laws that protect client records. The Agency shall only release client records to non-partner agencies with written consent by the client, unless otherwise provided in the relevant laws and regulations.

1. The Agency shall abide by all local, state and federal confidentiality laws and regulations pertaining to: 1) all medical conditions, including mental illness, alcohol and/or drug abuse, HIV/AIDS diagnosis and other such covered conditions; and 2) a person's status as a victim of domestic violence. A general authorization for the release of medical or other information is NOT sufficient for this purpose.
2. Federal, state and local laws seek to protect the privacy of persons with physical and/or mental illness, who have been treated for alcohol and/or substance abuse, have been diagnosed with HIV/AIDS, and/or have been a victim of domestic violence. The Agency is encouraged to seek its own legal advice in the event that a non-partner agency requests identifying confidential client information.

B. The Agency shall provide a verbal explanation of the HMIS database and the terms of consent to the Clients and shall arrange for a qualified interpreter or translator in the event that an individual is not literate in English or has difficulty understanding the Consent form.

C. The Agency agrees not to release any individual client information obtained from the HMIS to any organization or individual without written Client consent. Such written Client consent shall specify exactly what information the Client allows to be released; information that is not specified by the Client shall not be released.

D. The Agency shall ensure that all staff, volunteers and other persons who are issued a User ID and password for the HMIS receive client confidentiality training and have signed a User Policy, Responsibility Statement, and Code of Ethics Agreement.

E. Any staff, volunteer or other person who has been granted a User ID and password that is found to have willfully committed a breach of system security and/or client confidentiality shall have his or her access to the database revoked immediately. Any person who has been granted a User ID and password that is found to have committed a negligent breach of system security and/or client

confidentiality after a prior warning and correction shall have his or her access to the database revoked immediately. A revoked user may be subject to discipline by the Agency pursuant to the Agency's personnel policies.

F. In the event of a breach of system security or client confidentiality, the Agency Director shall notify the HMIS Lead Agency within 24 hours. Any Agency that is found to have had breached of system security and/or client confidentiality shall enter a period of probation, during which technical assistance shall be provided to help the Agency prevent further breaches. Probation shall remain in effect until the CoC Board of Directors has evaluated the Agency's security and confidentiality measures and found them compliant with the policies stated in this Agreement and the User Policy, Responsibility Statement, and Code of Ethics Agreement. Subsequent violations of system security may result in suspension from the system.

G. The Agency understands that the fileserver, which shall contain all Client information, shall be located off-site in a physically secure and electronically monitored facility, and that the client information is backed up daily.

H. The Agency shall have access to all Client data entered by the Agency. The Agency shall diligently record in the HMIS all service delivery information pertaining to individual clients served by the Agency. The Agency shall not knowingly enter false, misleading or biased data, including any data that would unfairly prejudice a client's ability to obtain services, under any circumstances.

I. If this Agreement is terminated, the HMIS Lead Agency and the remaining Partner Agencies shall maintain their right to the use of all Client data previously entered by the terminating Partner Agency, subject to the guidelines specified in this Agreement.

J. The Agency shall utilize the HMIS Client Consent—Release of Information form, as developed in conjunction and coordination with Partner Agencies, for all clients providing information to the HMIS. The Client Consent—Release of Information form, once signed by the Client, authorizes Client data to be entered into the HMIS database and authorizes information sharing with Partner Agencies for the period of one year, subject to the restrictions defined by the Client Consent form.

K. If the Agency is governed by the Health Insurance Portability and Accountability Act (HIPAA), the Agency must utilize its own HIPAA-compliant Consent to Release Information form in addition to the HMIS Client Consent form.

L. The Agency shall keep signed copies of the Client Consent—Release of Information form for a period of three years.

M. IGD does not require or imply that services must be contingent upon a Client's participation in the HMIS database. Services should be provided to Clients regardless of HMIS participation provided the Clients would otherwise be eligible for the services.

N. The Agency shall have access to identifying and statistical data on all Clients who consent to have their information entered in the HMIS database, except for data input into the database by "Blind Service Providers". Blind Service Providers are agencies serving specific protected client. Populations. Clients served by Blind Service Providers typically have one or more of the following characteristics:

1. Domestic violence;

2. HIV/AIDS;
3. Alcohol and/or substance abuse; or
4. Mental health.

O. An Agency that is a Blind Service Provider shall have access to identifying and statistical data that the Agency inputs into the HMIS database for clients served by that Agency.

II. HMIS Use, Data Entry and System Security

A. The Agency shall follow, comply with and enforce the User Policy, Responsibility Statement and Code of Ethics. Modifications to the User Policy, Responsibility Statement and Code of Ethics shall be established in consultation with Partner Agencies and may be modified as needed for the purpose of the smooth and efficient operation of the HMIS. HMIS Lead Agency shall announce approved modifications in a timely manner.

B. The Agency shall only enter individuals in the HMIS database that exist as Clients under the Agency's jurisdiction. The Agency shall not misrepresent its Client base in the HMIS database by knowingly entering inaccurate information. The Agency shall not use the HMIS database with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity.

C. The Agency shall use Client information in the HMIS, as provided to the Agency or the Partner Agencies, to assist the Agency in providing adequate and appropriate services to the Client.

D. The Agency shall consistently enter information into the HMIS database and shall strive for real-time, or close to real-time data entry. "Close to real-time data entry" is defined as withing three working days of seeing the Client.

E. When a Client revokes his or her consent to share information in the HMIS database, the Agency shall notify the HMIS Lead Agency of the revocation within 24 hours. Whe the System Administrator is notified of a client revocation, the System Administrator shall remove access to all identifying information about that client within 24 hours.

F. The Agency shall ensure that all staff, volunteers and other person who are issued a User ID and password refrain from including profanity or offensive language in the HMIS database.

G. The Agency shall utilize the HMIS for business purposes only.

H. MISI shall provide introductory training to Agency staff on the use of the Compass Rose software, MISI shall provide supplemental training regularly to accommodate changes in Agency staff, and address modifications to the Compass Rose software when needed.

I. MISI shall be available to provide technical assistance to Agency staff.

J. The Agency shall ensure that a staff, volunteers and other persons representing the agency regularly attends user group meetings.

K. The Agency shall ensure that all staff, volunteers and other persons who are issued a User ID and password for HMIS receive client and system security training that covers all items in the HMIS User Policy, Responsibility Statement and Code of Ethics.

L. The Agency shall take the following additional steps to ensure the security of the HMIS database system and the confidentiality of Client data:

1. Visitors and Clients are appropriately escorted to ensure that they do no access staff areas, record storage areas, or other areas potentially containing Client information. Persons not recognized as staff, visitors and clients shall be challenged for identification.

2. Client records that are retained as hard copy are stored in locking filing cabinets or in rooms that can be locked.

3. Photocopiers, printers and fax machines are located so as to minimize access by visitors and unauthorized persons.

4. Directors and other management or supervisory personnel are familiar with security and confidentiality policies and enforce such policies to ensure the security and confidentiality of the HMIS database and of Client information.

5. The Agency staff feels comfortable and obligated to report security breaches and misuse of the HMIS database system.

6. The Agency shall encourage clients to report any breaches of confidentiality that they observe in the Agency.

III. Reports

A. Agency Reports

1. The Agency shall be enabled to report on identifying and statistical data on the Clients it serves, subject to the terms of this Agreement regarding Client confidentiality.
2. The Agency shall not be enabled to report on identifying and statistical data on Clients it does not serve.

B. Area Reports

1. The Agencies of an area shall be able to report on non-identifying and statistical data only for that area.

2. The Homeless Action Council (HAC) in collaboration with the Executive Committee shall develop protocols on customizing and releasing reports.

C. The Agency may make aggregate data available to other entities outside of the system for funding or planning purposes pertaining to providing services to homeless persons. However, such aggregate data shall not directly identify individual Clients.

D. The Lead Agency and the HAC shall use only unidentified aggregate HMIS data for homeless policy and planning activities, in preparing federal, state or local applications for homelessness funding, to demonstrate the need for and effectiveness of programs and to obtain a system-wide view of program utilization in the County. The Agency agrees to allow the HAC Executive Committee to obtain

information from the HMIS system for performance monitoring.

IV. Terms and Conditions

A. Neither the Lead Agency nor the Agency shall transfer or assign any rights or obligations without the written consent of the other party.

B. This Agreement shall be in force, provided funding is available, until revoked in writing by either party.

C. This Agreement may be terminated with 30 days written notice.

Agency Director Name _____ Agency Director Signature _____ Date _____

Agency Name _____

Street Address _____

City _____, Zip Code _____

Agency Contact E-mail Address _____

Mailing Address _____

City _____, Zip Code _____

Telephone Number _____

User Policy, Responsibility Statement, and Code of Ethics

USER POLICY

Partner agencies shall share information for provision of services to homeless persons and those at risk of homelessness through a networked infrastructure that establishes electronic communication among the partner agencies.

The Client Consent/Release of information form shall be signed if the Client agrees that information about their situation can be entered into the HMIS database system. Minimum data entry on each consenting client includes:

- General information identifying the Client by name, indicating family status and latest residential history;
- Data detailing the client's current housing situation and the cause of their housing crisis;
- Shelter and Transitional housing utilization information, when appropriate.

Data necessary for the development of aggregate reports of homelessness service includes services needed, services provided, referrals and Client goals and outcomes.

The HMIS database system is a tool to assist agencies in focusing services and locating alternative resources to help homeless persons. Therefore, agency staff must use the Client information in HMIS only to target services to Clients' needs.

USER RESPONSIBILITY

Your username and password give you access to HMIS and the Service Point software. Initial each item below to indicate your understanding and acceptance of the proper use of your username and password. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination from HMIS database access, and may result in disciplinary action from the partner agency as define in the partner agency's personnel policies.

I agree to maintain the confidentiality of client information in HMIS in the following manner:

_____ My username and password are for my use only and will not be shared with anyone.

_____ I will take reasonable means to keep my password physically secure.

_____ I will only view, obtain, disclose, or use the database information that is necessary to perform my job.

_____ I understand that the only individuals who may view or hear HMIS client information are authorized users, and I will take these steps to prevent casual observers from seeing or hearing HMIS client information:

_____ I will log off of HMIS before leaving my work area, or make sure that the HMIS database has "timed out" before leaving my work area.

_____ I will not leave unattended any computer that has HMIS "open and running".

_____ I will keep my computer monitor positioned so that persons not authorized to use HMIS cannot view it.

_____ I will store hard copies of HMIS information in a secure file and will not leave such hard copy information in public view on my desk, or on a photocopier, printer or fax machine.

_____ I will properly destroy hard copies of HMIS information when they are no longer needed.

_____ I will not discuss confidential client information with staff, clients, or client family members in a public area.

_____ I will not discuss confidential client information on the telephone in any areas where the public might overhear my conversation.

_____ I will not leave messages on my agency's answering machine or voicemail system that contains confidential client information.

_____ I will keep answering machine volume low so that confidential information left by callers is not overheard by the public or unauthorized persons.

_____ I understand that a failure to follow theses security steps appropriately may result in a breach of client confidentiality and system security. If such a breach occurs, my access to HMIS will be terminated and I may be subject to further disciplinary action as defined in the partner agency's personnel policy.

_____ If I notice or suspect a security breach, I will immediately notify the Director of my Agency.

USER CODE OF ETHICS

1. HMIS users will treat partner agencies with respect, fairness and good faith.

2. Each HMIS user will maintain high standards of professional conduct in his or her capacity as a HMIS user.

3. HMIS users will use HMIS in good faith to benefit Clients.

4. HMIS users have the responsibility to relate to the Clients of other partner agencies with full professional consideration,

5. Clients have the right to receive assistance even if they do not choose to provide their information to the HMIS.

I understand and agree to comply with all the statements listed above.

_____
HMIS User Name (please print)

_____ _____
HMIS User Signature Date

_____
Agency Authorized Name (please print)

_____ _____
Agency Authorized Signature Date

Pathways
COMMUNITY NETWORK INSTITUTE

Privacy & Security

HMIS

HUD HMIS Requirements for Homeless Services Providers

Attachment C

Complying with HUD's HMIS Privacy & Security Rules

In 2004, HUD issued its Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice. The Notice includes HMIS Privacy and Security Standards which define functional requirements for HMIS software providers and operational requirements for HMIS administrators and Covered Homeless Organizations (CHO). A CHO is any organization that records, uses or processes protected personal information (PPI) on homeless clients for an HMIS. These organizations are more commonly called Service Providers.

We have created this guide as an easy reference for homeless service providers that are participating in their local HMIS implementations and want to make sure they are in full compliance with HUD HMIS rules. This guide describes the minimum Privacy and Security standards HUD has mandated for CHOs. All verbiage below is quoted directly from the HMIS Data and Technical Standards Final Notice.

HMIS Privacy Standards and HIPAA

Any CHO that is covered under HIPAA is not required to comply with the privacy or security standards in this Notice if the CHO determines that a substantial portion of its PPI about homeless clients or homeless individuals is protected health information as defined in HIPAA rules. Exempting HIPAA covered entities from the HMIS privacy and security rules avoids all possible conflicts between the two sets of rules.

4.2.1 - Collection Limitation

A CHO may collect PPI only when appropriate to the purposes for which the information is obtained or when required by law. A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information. Consent of the individual for data collection may be inferred from the circumstances of the collection. Providers may use the following language to meet this standard:

"We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate."

4.2.2 - Data Quality

A CHO must develop and implement a plan to dispose of or, in the alternative, to remove identifiers from, PPI that is not in current use seven years after the PPI was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention).

4.2.3 - Purpose Specification and Use Limitation

A CHO must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures.

4.2.4 - Openness

A CHO must publish a privacy notice describing its policies and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page.

4.2.5 - Access and Correction

In general, a CHO must allow an individual to inspect and to have a copy of any PPI about the individual. A CHO must offer to explain any information that the individual may not understand. A CHO must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

4.2.6 - Accountability

A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

Security Standards

This section describes the standards for system, application and hard copy security. All CHOs must comply with the baseline security requirements. A CHO may adopt additional security protections that exceed the baseline requirements if it chooses.

4.3.1 - System Security

A CHO must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a CHO's networks, desktops, laptops, minicomputers, mainframes and servers.

User Authentication: A CHO must secure HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements.

Virus Protection: A CHO must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed. A CHO must regularly update virus definitions from the software vendor.

Firewalls: A CHO must protect HMIS systems from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization.

Physical Access to Systems with Access to HMIS Data: A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use.

4.3.3 - Hard Copy Security

Applicability: A CHO must secure any paper or other hard copy containing personal protected information that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms.

Security: A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PPI when the hard copy is in a public area. When CHO staff are not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location.

Potential Requirements

HUD has issued an HMIS Proposed Rule, which contains the following requirements for CHOs:

- each CHO must designate a security officer and must conduct workforce security measures
- each HMIS user must complete security training at least annually
- each CHO must conduct an annual security review

These requirements may change as the Proposed Rule is updated and finalized based on public comments and legal review. HUD has not indicated when the HMIS Final Rule will be issued.

Provider Configuration Worksheet

Phase II

In ServicePoint entities are called "Providers". The agency level provider is referred to as the parent while the subordinate providers of the agency (the programs or projects) are the children. This worksheet will collect additional information not required by HUD to configure the system to your needs. These are items that will help your provider to utilize ServicePoint most effectively and easily.

Please start by telling us which Provider we are configuring:

Provider (Project) Name: _____

Provider Profile

Contact and Program Information

Location Information:				
Mailing Address:				
	Street	City	State	Zip
Physical Address:				
	Street	City	State	Zip
P.O. Box:				
	P.O. Box	City	State	Zip
Agency Contact Numbers:				
Primary Number? ○ Yes	Description:	Number:		
Primary Number? ○ Yes	Description:	Number:		
Primary Number? ○ Yes	Description:	Number:		

Pathways COMMUNITY NETWORK INSTITUTE   MISI

Contact and Program Information (cont'd):

Contact Personnel	Name:	
Title:	Email Address:	
Phone Number: ext.	Description:	
Website Address:	Notes:	
Hide from Provider Profile: ○ Yes ○ No	Primary Contact: ○ Yes	Receives Email: ○ Yes ○ No

Contact Personnel	Name:	
Title:	Email Address:	
Phone Number: ext.	Description:	
Website Address:	Notes:	
Hide from Provider Profile: ○ Yes ○ No	Primary Contact: ○ Yes	Receives Email: ○ Yes ○ No

Contact Personnel	Name:	
Title:	Email Address:	
Phone Number: ext.	Description:	
Website Address:	Notes:	
Hide from Provider Profile: ○ Yes ○ No	Primary Contact: ○ Yes	Receives Email: ○ Yes ○ No

Additional Information

Website Address:
Hours:
Program Fees:
Intake/Application Process:
Eligibility:
Languages:
Volunteer Opportunities:

Additional Information (cont'd)

Wishlists:	
Accessibility:	
Handicap Access: ○ Yes ○ No	Brochures: ○ Yes ○ No
Show on Public Site: ○ Yes ○ No	Printed Directory: ○ Yes ○ No
Is Shelter: ○ Yes ○ No	
Shelter Requirements:	

SERVICES

Search Terms Information

Geography Served

State	County/Parish	City	Zip Code

Services Provided

*Please use the service codes listed in Appendix A to complete this section.

These codes will help your users enter services more quickly. They will also help other providers find your agency/program, so they can refer clients to you.

Services Provided

Primary*: , , , , , , ,
Secondary*: , , , , , , ,
Occasional*: , , , , , , ,

Service Settings

Service Quick List
Service Code*: , , , , , , ,
Referral Quick List
Provider (Agency/Program): , , , , , ,

APPENDIX A – SERVICE CODES

Below are some of the most commonly used services codes. If you do not see a service listed your provider uses, please put a description of the service in place of a code. We will try to find a matching service code for those services. Based on AIRS Taxonomy, June 2018.

SERVICE CODE	SERVICE DESCRIPTION
B	Basic Needs
BD	Food
BD-1800	Emergency Food
BD-1800.2000	Food Pantries
BD-1800.2000-620	Occasional Emergency Food Assistance
BD-1800.2000-640	Ongoing Emergency Food Assistance
BD-1875.2000	Food Banks/Food Distribution Warehouses
BD-5000.1500	Congregate Meals/Nutrition Sites
BH	Housing/Shelter
BH-1800	Emergency Shelter
BH-1800.8500-300	Homeless Motel Vouchers
BH-3800	Housing Expense Assistance
BH-3800.7000	Rent Payment Assistance
BM-3000.1000	Bedding/Linen
BM-6500.1500	Clothing
BM-6500.1500-130	Clothing Vouchers
BM-6500.1500-150	Diapers
BM-6500.1500-250	General Clothing Provision
BM-6500.6500	Personal/Grooming Needs
BM-6500.6500-700	Public Restrooms
BM-6500.6500-710	Public Showers/Baths
BT	Transportation
BT-4500	Local Transportation
BT-4800.4550	Long Distance Bus Services
BT-8300.1000	Bus Fare
BT-8300.2500	Gas Money
BT-8500.1000	Local Transit Passes
BV-8900.9300	Utility Service Payment Assistance
BV-8900.9300-180	Electric Service Payment Assistance
BV-8900.9300-250	Gas Service Payment Assistance
DF-7000.1200	Birth Certificates
DF-7000.3300	Identification Cards
LE	General Medical Care
LH-5100.6500	Prescription Expense Assistance
NT	Temporary Financial Assistance
PH-1000	Case/Care Management
PH-1000.4500	Long Term Case/Care Management
PH-2400.1300	Case/Care Management Referrals
RF-2500	Group Counseling
RX	Substance Use Disorder Services
TJ-3000	Information and Referral

User Policy, Responsibility Statement, and Code of Ethics
Agency Partner End User List

Agency: _____

List **Existing** and **NEW** authorized persons to have access to HMIS under Agency authorization. (Please print)

Name	E-mail

List persons **no longer authorized** for access to HMIS under Agency authorization. (Please print)

Name

_____
Agency Authorization Name and Title (Please Print)

_____ _____
Agency Authorized Signature Date

Attachment E

HMIS Monitoring Checklist

Attachment F

		Yes	No
1.	Does the organization have a Privacy Officer?		
	Who?		
2.	Is data entered directly into HMIS as it is being collected?		
3.	Is data collected on paper forms? (if yes, attach copy of form)		
4.	Is a notice of privacy practices posted at all locations where intake takes place?		
5.	Does the organization have a privacy policy?		
6.	Are paper and or electronic copies of the privacy policy available on request?		
7.	Is the agency's privacy policy posted on its public web site?		
8.	Are procedures in place to protect information printed and/or downloaded from HMIS?		
9.	Is printed information kept in a room that is locked when staff is not present?		
10.	Is printed information kept in a locked file cabinet or locked drawer within that locked room?		
11.	Do the procedures specifically address protection, retention and destruction of printed material?		
12.	Do the procedures specifically address protection, retention and destruction of computer files?		
13.	Are staff and volunteers required to attend training on these procedures? (collect copy of procedures for CoC files)		

14.	Do all computers have currently supported operating systems?		
15.	Are all computers configured to automatically download and install all security updates?		
16.	If no, does IT staff or a contractor manually install security updates on a regular basis?		
17.	Do all computers have the latest versions of all installed Internet browsers?		
18.	Does at least one firewall protect each computer?		
19.	Is antivirus and firewall software installed on all computers?		
20.	Are all computers configured to automatically download and install antivirus/firewall software updates?		
21.	If no, does IT staff manually install antivirus/firewall software updates on a regular basis?		
22.	Is a password always required to use all computers?		
23.	Must all computer users log in again after a short period of inactivity?		
24.	Are all computers in locations that are not accessible without an escort?		
25.	If no, are publicly accessible computers manned at all times?		