St. Louis City Continuum of Care

Housing/Homeless Management Information System

Policies and Procedures Manual

October, 2015

Contents

Homeless management information system

policy and procedures manual

This policy and procedure manual is developed in collaboration between the HMIS Advisory Committee and the HMIS Lead Agency for the Saint Louis City Continuum of Care. This manual is authorized by the Executive Committee of the Saint Louis City Continuum of Care.

HMIS governance charter

Introduction

The purpose of the Saint Louis City HMIS is to support the delivery of homeless and housing services, including homeless prevention, in the St. Louis City community. The HMIS should be used primarily to collect and track information related to serving people in housing crises, as well as planning for the elimination of homelessness. On a case-by-case basis, the HMIS Advisory Committee will consider other uses of the database.

Key Support Roles & Responsibilities

City of Saint Louis Department of Human Services

As the Collaborative Applicant for Saint Louis City Continuum of Care (CoC):

- Ensures fiscal and programmatic compliance with all HUD rules and regulations
- Encourages and facilitates participation in HMIS data collection
- Collaborates with the Saint Louis City Continuum of Care to select, approve and execute annual contract(s) with HMIS Lead and/or HMIS Vendor

HMIS Lead

As the HMIS Lead for Saint Louis City Continuum of Care (CoC):

- Ensures the operation of and consistent participation by recipients of funding requiring use of the HMIS system
- Develops written policies and procedures for all HMIS Partner Agencies, which at a minimum includes: a security plan, data quality plan, and privacy plan.
- Executes an HMIS participation agreement with each HMIS Partner Agencies
- Executes an HMIS collaborative agreement with the Saint Louis City Continuum of Care; this agreement defines performance standards for HMIS system maintenance, training, user support, report requirements, and analytical support
- Monitors compliance of all HMIS Partner Agencies
- Provides an unduplicated count of clients served and analyses of unduplicated counts to the Continuum of Care on quarterly basis, and upon request, to HUD
- Ensures that the HMIS Vendor and software is currently in compliance with HMIS standards
- Serves at the primary contact between Partner Agencies and the HMIS vendor

- Serves as the applicant to HUD for grant funds for HMIS Activities of the Continuum of Care's geographic area, as directed by the Continuum, and if selected for an award by HUD, enter into a grant agreement with HUD to carry out the HUD-approved activities

Saint Louis City Continuum of Care (CoC)

- Responsible for selecting one HMIS software system
- Responsible for selecting one HMIS Lead
- Responsible for reviewing, revising, and approving all policy and procedures developed by HMIS Lead; final approval of policies and procedures is the responsibility of the Executive Board of the CoC
- Responsible for implementing all approved and/or revised policies and procedures within six months of approval
- Develops a governance charter and documents all assignments and designations consistent with the governance charter.
- May choose to participate in HMIS with other local Continuum of Care so long as one HMIS vendor and Lead are agreed upon and there is a joint governance charter.
- Executes an HMIS collaborative agreement with the HMIS Lead; this agreement defines performance standards for HMIS system maintenance, training, user support, report requirements, and analytical support

HMIS Advisory Committee

- Responsible for recommending HMIS software system and HMIS Lead
- Governs the implementation of the HMIS system
- Assists in the development of HMIS policies and procedures in collaboration with the HMIS Lead
- Advises and recommends changes to HMIS policies and procedures for approval by the Planning Committee, General Membership, and Executive Committee of the Saint Louis City CoC
- Examines HMIS aggregate data as well as offers comments and suggestions on how data measurements can contribute to fulfillment of strategic goals

HMIS Partner Agencies

- Responsible for ensuring that HMIS processing capabilities remain consistent with the privacy obligations of the Partner Agencies
- Comply with applicable standards set forth by the CoC, HMIS Lead and HUD, including but not limited to issues of privacy and confidentiality
- Develop agency procedures to ensure and monitor compliance and sanctions for non-compliance
- Ensure staffing and equipment necessary to implement HMIS
- Complete an HMIS Agency Partner Agreement with the HMIS Lead
- Designate an HMIS Agency Administrator and Chief Privacy Officer

HMIS PARTICIPATION POLICY

Mandated

Agencies receiving Emergency Solution Grants, Supportive Housing Program grants, Shelter plus Care grants, Section 8 SRO programs, HOPWA grants and other funders within the Continuum of Care will be required to meet the minimum HMIS participation standards. Participating agencies must agree to execute and comply with an HMIS Agency Partner Agreement, as well as, all HMIS policies and procedures. Agencies receiving HUD CoC or Emergency Solutions Grant funding have no current fees associated with participating in the HMIS system.

Voluntary

While the Saint Louis City CoC does not require participation in HMIS by agencies that do not receive HUD CoC or Emergency Solutions Grant funding, every effort is made to encourage all homeless service providers to participate in the HMIS system in order to more thoroughly gain an understanding of those experiencing homelessness in Saint Louis City. Non-funded agencies should contact the HMIS Lead for any fees associated with participation.

Minimum Standards to Participate in HMIS

- Partner Agencies will enter into an HMIS Agency Partner Agreement and comply with all HUD regulations for HMIS participation
- Partner Agencies will designate a Chief Privacy Officer. The Chief Privacy Officer is responsible for: managing client questions and complaints about the Privacy Notice, ensuring all new users have completed a User Agreement, monitoring all users compliance with training requirements, and maintaining both user and technological requirements needed for security standards.
- Partner Agencies will designate an Agency HMIS Agency Administrator. The Agency HMIS Agency Administrator is the designated communication point with the HMIS Lead and will be expected to routinely verify data for completeness, accuracy and timeliness and work in collaboration with the HMIS Lead for correcting and managing the agency's data.
- All users are responsible for collecting data elements as defined by HUD and any additional data elements determined by the Saint Louis City CoC.
- All users must enter client-level universal data elements at minimum into the HMIS system within 24 hours of entry into a project and complete appropriate discharge within 48 hours of exit from a project.

HMIS Partnership Termination Policy

Contract Termination Initiated by HMIS Partner Agency

Contributing HMIS Organizations may terminate the HMIS Partner Agreement with or without cause upon 30 days written notice to the HMIS Lead and according to the terms specified in the HMIS Agency Agreement. The termination of the HMIS Agency Agreement by the Partner Agency may impact other compliance regulations, such as contracts with the Department of

Human Services that specify HMIS utilization. In the event of termination of the HMIS Agency Agreement, all data entered into the HMIS system will remain an active, and records will remain open or closed according to any data sharing agreements in place at the time of termination. In all cases of termination of HMIS Partner Agreements, the HMIS Lead will inactivate all users from that agency on the date of termination of contract. The HMIS Lead will notify the HMIS Advisory Committee and the Department of Human Services.

Contract Termination Initiated by HMIS Lead

The HMIS Lead may terminate the HMIS Partner Agreement for noncompliance within the terms of that contract upon 30 days written notice to the HMIS Partner Agency. The HMIS Lead will require any violations to be rectified to avoid termination of the HMIS Partner Agreement.

The HMIS Lead may also terminate the HMIS Partner Agreement with or without cause upon 30 days written notice to the HMIS Partner Agreement and according to the terms specified in the HMIS Partner Agreement.

The termination of the HMIS Partner Agreement may impact other compliance regulations, such as contracts with the Department of Human Services that specify HMIS utilization. In the event of termination of the HMIS Agency Agreement, all data entered into the HMIS system will be maintained by the HMIS Lead until all clients are appropriately exited from the terminated agency.

Prior to any notification of termination, the HMIS Lead must first consult with the CoC Executive Board and the Department of Human Service before any termination is issued.

HMIS technical Standards

The HMIS Lead and HMIS vendor are equally responsible with any and all technical standards determined by HUD. HUD has established that all HMIS software must be able to: produce unduplicated client records, collect all data elements set forth by HUD, report outputs, produce compliance reports for Partner Agencies and the Lead to assess achievements with established benchmarks, and generate standardized audit reports.

Hardware and Computer Requirements

While the HMIS Lead and HMIS vendor maintain software for HUD standards, Partner Agencies are responsible for complying with agency-level system security standards. These system standards aid in the safety and integrity of client records. Partner Agencies must comply with the following hardware and software standards:

1) A secure broadband internet must be used; Wi-Fi is acceptable, if the connection is protected by a network security code.
2) Computers must have an operating system compatible with the current HMIS software
3) Computers must have an internet browser compatible with current HMIS software

4) All workstations must be manually locked by a user if a licensed user leaves a workstation when HMIS software is active
5) All workstations must have current and active security which include:
    a. Real-time antivirus scanning
    b. Automatic virus removal
    c. Anti-Spyware
    d. Firewall
    e. Anti-phishing

The equipment used to connect to the HMIS system is the responsibility of the HMIS Partner Agency. Contributing HMIS Partner Agencies will need to provide their own internal technical support for the hardware, software and Internet connections necessary to connect to the HMIS system according to their own organizational needs.

System Availability

It is the intent of the Saint Louis City Continuum of Care, HMIS Lead and HMIS Vendor that the HMIS system server will be available 24 hours a day, 7 days a week, and 52 weeks a year to incoming connections. However, no computer system achieves 100 percent "uptime." In the event of planned server downtime, the HMIS Lead will inform agencies as much in advance as possible in order to allow HMIS Partner Agencies to plan their access patterns accordingly.

Annual reviews for Technical Standard Compliance will be conducted by each Partner Agency Chief Privacy Officer to ensure agencies are meeting requirements. Additionally, the HMIS Lead will be conducting technical standard compliance on behalf of the entire CoC to ensure Partner Agencies and HMIS system software are in compliance.

HMIS SECURITY PLAN

The HMIS Lead is responsible for establishing a security plan, which must be approved by the Saint Louis City Continuum of Care. This security plan must address the areas of data collection, maintenance, use, disclosure, transmission, destruction of data, and a communication plan for reporting and responding to security incidents. In addition to the security plan, the HMIS Lead must develop a Disaster Recovery Plan and verify that the HMIS Vendor has a Disaster Recovery Plan as well.

HMIS User Access

All users are required to sign a HMIS User Agreement and complete HMIS User Training before receiving access to the HMIS. Credentials will not be issued without a signed User Agreement being on file with the HMIS Lead and the HMIS Agency Administrator.

All HMIS training participants will be given a copy of the HMIS User Agreement at the conclusion of User training. Potential Users will be responsible for completing the User Agreement, obtaining the required signatures and returning the form to the HMIS Lead before

User Credentials will be issued. Once all required paperwork is complete, User Credentials can be obtained by calling the HMIS Help Desk.

Establishing a New Partner Agency

Homeless service providers that are interested in obtaining access to the HMIS system will be required to first contact the HMIS Lead, who will process the request and engage the CoC as necessary.

Once the homeless service provider has been approved for access to the HMIS system, the New Partner Agency will receive a copy of an HMIS participation agreement to review and obtain the appropriate signatures. The HMIS participation agreement will be sent to the HMIS Lead. Once all agreements are finalized, the HMIS Lead will contact the new partner agency regarding obtaining access and new user training.

Data Access Policies

HMIS Users will receive a unique username and establish a password. Usernames and passwords are never to be shared, or documented in a visible or accessible location, which would compromise the integrity and security of the HMIS system. HMIS Users will automatically be prompted to change their HMIS password on a routine basis. If a password is lost or forgotten, the HMIS User should contact the HMIS helpdesk.

HMIS Users must log off the HMIS system or lock the computer any time they step away from the workstation. Automatic password protected screen savers, or network log-off, should be implemented on each computer used for HMIS. Additionally, the HMIS system is set up to auto-log off users who are inactive on the site after a maximum of 10 minutes.

Any paper documentation, such as client authorization forms, should be filed in a locked, secure area and not left unattended. All paper and electronic documentation for any client in the HMIS system must be stored and maintained for a minimum of seven years.

HMIS PRIVACY PLAN

Data Collection Limitation Policy

Partner agencies will only enter client information into the HMIS system that is deemed necessary to provide quality service. Partner agencies, in collaboration with the Saint Louis City CoC, will make a determination of what qualifies as essential for services.

Partner agencies reserve the right to decline services for clients choosing not to share the information requested by the agency as doing so could jeopardize their status as a service provider. The agency assumes that, by requesting services from the agency, the client agrees to allow them to collect information and to use or disclose it as described in the privacy notice and otherwise as allowed or required by law.

Client Notification

Partner Agencies must post notification at each intake desk of the agency advising clients of the Privacy Notice (Appendix A). Clients must also be provided with the short version of the Privacy Notice (Appendix B) which advises them that they can request a copy of the full policy.

The HMIS Privacy Notice should be posted on the agency's web page. Agency should ensure that the address does not appear in the Privacy Notice before it is posted on their website, if the address is not public knowledge.

In addition to the posted notification signs, any client who agrees to allow HMIS User access to their HMIS profile must sign a Client Authorization form. This form must be updated annually.

The agency must provide reasonable accommodations for persons with disabilities throughout the data collection process. Various versions of the Privacy Notice will be made available through the HMIS Lead.

Limitations of HMIS Use

Partner agencies will use and disclose personal information from HMIS only in the following circumstances:

1) To provide or coordinate services to an individual.
2) For functions related to payment or reimbursement for services.
3) To carry out administrative functions including, but not limited to legal, audit, personnel, planning, oversight or management functions.
4) Databases used for research, where identifying information has been removed.
5) Contractual research where privacy conditions are met.
6) Where a disclosure is required by law and disclosure complies with and is limited to the requirements of the law. Instances where this might occur are during a medical emergency, to report a crime against staff of the agency or a crime on agency premises, or to avert a serious threat to health or safety, including a person's attempt to harm himself or herself.
7) To comply with government reporting obligations.
8) In connection with a court order, warrant, subpoena or other court proceeding requiring disclosure.

Client Rights to Access and Correction of Files

Any client receiving services from a Partnering Agency has the following rights:

1) **Access to program records**. Clients have the right to review their records in a program in the HMIS. A written request should be made to the HMIS Agency Administrator, who should follow-up on the request within five working days.

2) **Access to full records.** Clients have the right to review their full record in the HMIS. They may make a written request through the HMIS Agency Administrator, who will request approval from the HMIS Lead within five working days.

3) **Correction of an HMIS record**. A client has the right to request that his or her HMIS record is correct so that information is accurate. This ensures fairness in its use.

4) **Refusal**. A client has a right to refuse to participate in HMIS or to provide personal information. The agency's ability to assist a client depends on the documentation of certain personal identifying information, and may decline to provide services to a client who refuses to provide this data.

5) **Agency's Right to Refuse Inspection of an Individual Record**. The agency may deny a client the right to inspect or copy his or her personal information for the following reasons:
   i. information is compiled in reasonable anticipation of litigation or comparable proceedings;
   ii. information about another individual other than the agency staff would be disclosed;
   iii. information was obtained under a promise of confidentiality other than a promise from the provider and disclosure would reveal the source of the information; or
   iv. Information reasonably likely to endanger the life or physical safety of any individual if disclosed.

6) **Harassment.** The agency reserves the right to reject repeated or harassing requests for access or correction. However, if the agency denies a client's request for access or correction, written documentation regarding the request and the reason for denial will be provided to the client. A copy of that documentation will also be included in the client record.

Data Sharing

At initial project intake, the client should receive verbal explanation and written documentation about utilization of the HMIS system for Saint Louis City Continuum of Care. If a client is willing to share information with HMIS, they must sign a Client Authorization form. Any information that will be shared, beyond what is covered by the Client Authorization for HMIS, will require additional written consents and release of information by the client.

The client does have the right to revoke written authorization at any time, unless this is overridden by agency policy or is a part of a conditional agreement with the provider. Once the client has revoked their authorization, no new information may be utilized in HMIS but all historical data remains accessible by the provider.

All Partner Agencies are expected to uphold federal, state, and local confidentiality regulations to protect records and privacy. If an agency is covered by the Health Insurance Portability and Accountability Act (HIPPA), the HIPAA regulations prevail.

Protected Agencies and Domestic Agencies

Protected agencies serve populations that require special security and privacy considerations. Populations include medically fragile, at-risk youth, and those served by Shelter+Care programs. Protected agencies contribute data to HMIS; however, the services provided by the agencies remain hidden beyond basic identification of clients.

Domestic violence agencies are prohibited from entering data into the HMIS. If domestic violence agencies receive CoC or ESG fudning, they are required to have a comparable database, and the HMIS lead will work with agencies to ensure the databases meet standards. Agencies are required to report aggregate data for reporting purposes.

HMIS Data Release Policy and Procedures

Client-Level Data:

HMIS Users may access client-level data for their specified project only after completing appropriate client authorization. Client authorization is good for up to one year. After one year, only historical record information will be available for the project unless an updated client authorization is filed.

Client-level data may also be viewed by only the HMIS Lead and HMIS Vendor for purposes of compliance, software correction, data quality resolution, and other required tasks related to HMIS privacy, security, and data quality standards.

No identifiable client data are to be released to any person, agency or organization without written consent by the client, unless otherwise required by law.

Mandated Reporting

Mandatory reporters should comply with state guidelines for reporters. This obligation supersedes any agency policies that prohibit disclosure of identifying information.

Court-Ordered Subpoenas

There are many situations in which police or other government officials request information from shelters and other service providers. If an HMIS Partner Agency is served with a Subpoena for records, the agency must immediately contact the HMIS Lead and the Chair of the Executive Board of the Saint Louis City Continuum of Care. Once it is established the exact information requested in the subpoena, the Partner Agency and HMIS Lead will work in collaboration to gather the appropriate documentation. Due to the fact HMIS Partner Agencies have data sharing, it is vital to work with the HMIS Lead to only provide information from the listed Partner Agency requested in the subpoena.

Program-Level (aggregate) Data:

The HMIS Lead will supply HMIS Advisory Committee a report analyzing program-level data on a quarterly basis. These quarterly reports will be utilized to help inform systematic practice for the Continuum of Care. At a minimum, the HMIS Advisory Committee will report findings and offer practice suggestions to the Planning Committee twice a year.

Agencies will be able to request access to aggregate-level data. The HMIS Agency Administrator will make requests through the HMIS Lead, who will outline appropriate use and dissemination of aggregated data. Training and support will be made available through the HMIS Lead. Public release of community-wide statements based on aggregate data requests must be coordinated through DHS. No individually identifiable client data will be reported in any of these reports.

Extracted Data

The report-writer function of the HMIS system should allow client data to be downloaded to a file on the local computer. Confidentiality of clients is left vulnerable on the local computer unless additional measures are taken. For security reasons, unencrypted data may not be sent over a network that is open to the public. For example, while unencrypted data might be stored on a server and accessed by a client computer within the private local area network, the same unencrypted data may not be sent via email to a client computer not within the same local area network. HMIS users should apply the same standards of security to local files containing client data as to the HMIS database itself. Security questions will be addressed to the HMIS Lead.

Data Retrieval for Research or Comparative Purposes

While the HMIS is a useful resource, it is not always comprehensive enough to fully understand the nature and extent of homelessness, how individuals access mainstream or other federal programming resources, and the most effective prevention.

To gain a better understanding of the needs and service usage of individuals who are experiencing a housing crisis, and to assist with planning, implementation and allocation of resources, the data may be used or disclosed data for research conducted by an individual or institution with approval by the CoC Executive Board.

To identify trends and patterns of service usage to better implement homeless and prevention services, the CoC Executive Board may approve the HMIS Lead, with appropriate consent or agreements, to cross-reference HMIS client-level data with other public databases including: those relating to employment, family services, child welfare, criminal justice, prevention, and healthcare.

HMIS Data Quality Plan

It is ultimately the responsibility of the Saint Louis City Continuum of Care Executive Committee and HMIS Lead to ensure quality data is submitted to HUD. In an effort to direct service provisions in an effective and efficient manner and assist the Saint Louis City Coc in obtaining strategic goals, the HMIS Lead is responsible for setting Data Quality benchmarks and a Data

Quality Plan (as approved by the Saint Louis City CoC).

HMIS Data Quality reviews of client-level data will be used by the HMIS Agency Administrator and by the HMIS Lead to monitor data quality and indicate possible additional trainings needed for improvement. HMIS Data Quality reviews of program-level data will be used by the HMIS Lead to report continuum-wide improvement suggestions, and recommendations for integrations with other mainstream and Federal Programming data. Program-level data quality may also be used by various Saint Louis Continuum of Care committees for system analysis and evaluations.

Data Quality Standards and Monitoring

- All data entered will be accurate
- In all reports of shelter, housing or services provided for a client, the client must be eligible to receive the services from the listed provider
- Universal data elements at minimum must be entered into the HMIS system within 24 hours of entry into a project and complete appropriate discharge within 48 hours of exit from a project.
- Per HUD data standards, blank entries in required data fields are not allowed.
- Entries of "client does not know" or "client refused" in required data fields will not exceed 10 percent required for CoC reporting.
- HMIS Agency Administrators will perform monthly data quality checks using the Data Quality Plan.
- Any patterns of errors identified by users will be reported to the HMIS Agency Administrator. When patterns of error have been discovered, users will be required to correct the data, data entry processes (if applicable) and will be monitored for compliance.
- Any pattern of error between Partner Agencies should be reported to the HMIS Lead

Data Collection Requirements

Partner Agencies are responsible for completing, at minimum, the HUD defined Universal Data Elements (UDE's) and any HUD Program-specific Data Elements required for the agency's project. Partner Agencies may also be required to collect data elements determined by the HMIS Advisory Committee as vital. Partner Agencies will do their due diligence to collect and verify client information upon client initial program enrollment or as soon as possible. Any information collected by the Partner Agency must be documented into HMIS within 24 hours of entry into a project and complete appropriate discharge within 48 hours of exit from a project.

Data Quality Training Requirements

In order for the HMIS system to be a benefit to clients, a tool for Partner Agencies and a guide for planners, all users must be adequately trained to collect, enter, and extract data. The HMIS Lead will be responsible for developing an annual training schedule. The annual training schedule must include various types and levels of training- for HMIS Agency Administrators, beginning users and advanced users. Trainings can be offered either directly or through HMIS

Lead approved, contracted trainers.

End-User Initial Training
All HMIS Users must complete approved training before being given access to HMIS. Users should be trained on: user of HMIS software and the confidentiality/security requirements of the Privacy Notice. As part of the training, each employee and volunteer of your agency who collects, reads, or is otherwise exposed to client information must be given a copy of the full Privacy Notice, be allowed to read it, then must sign the Acknowledgment enclosed in this manual as Appendix C to confirm they have read and understood the policy.

It is encouraged that all HMIS Users also receive agency-specific training in order to fulfill Partner Agency expectations for entering data.

Ongoing Training
In order to remain current on HUD standards and local continuum expectations, all HMIS users are required to complete annual training and training on all HMIS software updates. These ongoing trainings can be in the form of: attendance to User Group meetings, HMIS Lead approved online/in-person trainings, and individualized meeting with HMIS Lead representatives. The HMIS Lead and HMIS Agency Administrators will communicate training opportunities to users.

Documentation of training will be made available from the HMIS Lead. It is the expectation that the Agency Chief Privacy Officer will maintain a record of each HMIS User's completed training hours for year. Training record should be submitted in the annual compliance review.

Annual reviews for data quality, security and privacy standards compliance will be conducted by each Partner Agency Chief Privacy Officer and HMIS Agency Administrators to ensure agencies are meeting requirements. The HMIS Lead will work with HMIS Agency Administrators to schedule annual site-visits to ensure compliance across the Saint Louis City CoC.

HMIS Grievance Policy

Client Grievance
Clients have the right to be heard if they feel that their confidentiality rights have been violated, if they have been denied access to their personal records, or if they have been put at personal risk or harmed. Each agency must established a formal grievance process for the client to use in such a circumstance. To file a complaint or grievance they should contact the agency's Chief Privacy Officer. HMIS Partner Agencies will report all HMIS related client grievances to the HMIS Lead. The HMIS Lead will record all grievances and will report any common trends in complaints to the HMIS Advisory Committee.

Partner Agency Grievance

It is encouraged that if any issues arise, problems should be presented and resolved at the lowest possible level. If HMIS users have an issue with HMIS software, policy or HMIS Lead representative, they should first reach out to the HMIS Agency Administrator. If an issue cannot come to a successful resolution with the HMIS Agency Administrator, the issue should be presented to the HMIS Lead.

The HMIS Lead will attempt to resolve issues between the Partner Agencies and the HMIS Vendor. The HMIS Lead will also present any CoC systematic issues or policy concerns to the HMIS Advisory Committee.

HMIS Non-Compliance Sanctions

The HMIS Lead is responsible for establishing appropriate sanctions for non-compliance issues. These sanctions must be approved by the Saint Louis City Continuum of Care, and may include suspension of HMIS system access. Additionally, HMIS Partner Agency must also have agency-specific sanctions for users not in compliance with HMIS policies and procedures.

Appendix A: Full Privacy Policy

Homeless Management Information System
Privacy and Security Notice

A written copy of this policy is available by request.

I. PURPOSE

This notice describes the privacy policy of Municipal Information Systems, Inc. The policy may be amended at any time. We may use or disclose your information to provide you with services and comply with legal and other obligations. We assume that, by requesting services from our agency, you agree to allow us to collect information and to use or disclose it as described in this notice and as otherwise required by law.

The Homeless Management Information System (HMIS) was developed to meet a data collection requirement made by the United States Congress and the Department of Housing and Urban Development (HUD). Congress passed this requirement in order to get a more accurate count of individuals who are homeless and to identify the need for and use of different services by those individuals and families. We are collecting statistical information on those who use our services and report this information to a central data collection system.

In addition, many agencies in this area use HMIS to keep computerized case records. This information may be provided to other HMIS participating agencies. The information you may agree to allow us to collect and share includes: basic identifying demographic data, such as name, address, phone number and birth date; the nature of your situation and the services and referrals you receive from this agency. This information is known as your Protected Personal Information or PPI.

Generally, all personal information we maintain is covered by this policy. Generally, your personal information will only be used by this agency and other agencies to which you are referred for services.

Information shared with other HMIS agencies helps us to better serve our clients, to coordinate client services, and to better understand the number of individuals who need services from more than one agency. This may help us to meet your needs and the needs of others in our community by allowing us to develop new and more efficient programs. Sharing information can also help us to make referrals more easily and may reduce the amount of paperwork.

Maintaining the privacy and safety of those using our services is very important to us. Information gathered about you is personal and private. We collect information only when appropriate to provide services, manage our organization, or as required by law.

II. CONFIDENTIALITY RIGHTS:

This agency has a confidentiality policy that has been approved by its Board of Directors. This policy follows all HUD confidentiality regulations that are applicable to this agency, including those covering programs that receive HUD funding for homeless services. Separate rules apply for HIPPA privacy and security regulations regarding medical records.

This agency will use and disclose personal information from HMIS only in the following circumstances:

1) To provide or coordinate services to an individual.
2) For functions related to payment or reimbursement for services.
3) To carry out administrative functions including, but not limited to legal, audit, personnel, planning, oversight or management functions.
4) Databases used for research, where identifying information has been removed.
5) Contractual research where privacy conditions are met.
6) Where a disclosure is required by law and disclosure complies with and is limited to the requirements of the law. Instances where this might occur are during a medical emergency, to report a crime against staff of the agency or a crime on agency premises, or to avert a serious threat to health or safety, including a person's attempt to harm himself or herself.
7) To comply with government reporting obligations.
8) In connection with a court order, warrant, subpoena or other court proceeding requiring disclosure.

III. CLIENT RIGHTS:

Any client receiving services from your agency has the following rights:

1) **Access to records**. Clients have the right to review his or her record in the HMIS. They may request review of the record within five working days.
2) **Correction of an HMIS record**. A client has the right to request that his or her HMIS record is correct so that information is accurate. This ensures fairness in its use.
3) **Refusal**. Your agency's ability to assist a client depends on the documentation of certain personal identifying information. You may decline to provide services to a client who refuses to provide this data.

4) **Agency's Right to Refuse Inspection of an Individual Record**. You may deny a client the right to inspect or copy his or her personal information for the following reasons:

a. information is compiled in reasonable anticipation of litigation or comparable proceedings;
b. information about another individual other than the agency staff would be disclosed;
c. information was obtained under a promise of confidentiality other than a promise from this provider and disclosure would reveal the source of the information; or
d. Information reasonably likely to endanger the life or physical safety of any individual if disclosed.

7) **Harassment.** The agency reserves the right to reject repeated or harassing requests for access or correction. However, if the agency denies your request for access or correction, you will be provided written documentation regarding your request and the reason for denial. A copy of that documentation will also be included in your client record.

8) **Grievance.** You have the right to be heard if you feel that your confidentiality rights have been violated, if you have been denied access to your personal records, or if you have been put at personal risk, or harmed. Our agency has established a formal grievance process for you to use in such a circumstance. **To file a complaint or grievance you should contact our Chief Privacy Officer.**

IV. HOW YOUR INFORMATION WILL BE KEPT SECURE:

Protecting the safety and privacy of individuals receiving services and the confidentiality of their records is of paramount importance to us. Through training, policies, procedures and software, we have taken the following steps to make sure your information is kept safe and secure:

1) The computer program we use has the highest degree of security protection available.
2) Only trained and authorized individuals will enter or view your personal information.
3) Your name and other identifying information will not be contained in HMIS reports that are issued to local, state or national agencies.
4) Employees receive training in privacy protection and agree to follow strict confidentiality standards before using the system.
5) The server/database/software only allows individuals access to the information. Only those who should see certain information will be allowed to see that information.

6) The server/database will communicate using 128-bit encryption, which is an Internet technology intended to keep information private while it is transported back and forth across the Internet. Furthermore, identifying data stored on the server is also encrypted or coded so that it cannot be recognized.
7) The server/database exists behind a firewall, which is a program designed to keep hackers and viruses away from the server.
8) The main database will be kept physically secure, meaning only authorized personnel will have access to the server/database.
9) HMIS Agency Administrators employed by the HMIS and the agency support the operation of the database. Administration of the database is governed by agreements that limit the use of personal information to providing administrative support and generating reports using aggregated information. These agreements further insure the confidentiality of your personal information.

V. BENEFITS OF HMIS AND AGENCY INFORMATION SHARING:

Information you provide us can play an important role in our ability and the ability of other agencies to continue to provide the services that you and others in the community are requesting.

Allowing us to share your name results in a more accurate count of individuals and the services they use. Obtaining an accurate count is important because it can help us and other agencies:

1) Better demonstrate the need for services and the specific types of assistance needed in our area.
2) Obtain more money and other resources to provide services.
3) Plan and deliver quality services to you and your family.
4) Assist the agency to improve its work with families and individuals who are homeless.
5) Keep required statistics for state and federal funders, such as HUD.

VI. COMPLIANCE WITH OTHER LAWS:

This agency complies with all other federal, state and local laws regarding privacy rights. Consult with an attorney if you have questions regarding these rights.

VII. PRIVACY NOTICE AMENDMENTS:

The policies covered under this Privacy Notice may be amended over time and those amendments may affect information obtained by the agency before the date of the change. All amendments to the Privacy Notice must be consistent with the

requirements of the Federal Standards that protect the privacy of consumers and guide HMIS implementation and operation.

VIII. DATA QUALITY:

Data Entry Policy: Agency/HMIS users will be responsible for the accuracy of their data entry. Missing data rates are expected to be kept below 10%. **For housing programs, client entry and exit dates are expected to be recorded in a timely manner.** Universal data elements at minimum must be entered into the HMIS system within 24 hours of entry into a project and complete appropriate discharge within 48 hours of exit from a project**.**

Procedure: The Agency must maintain standards for periodically checking data for completeness, accuracy and timeliness. The CoC will also define and maintain a data quality plan to help all Agencies monitor data quality. The HMIS Agency Administrator will perform regular data quality checks using the Data Quality Plan. Any patterns of error will be reported to the Agency Administrator. When patterns of error have been discovered, users will be required to correct the data, data entry processes (if applicable) and will be monitored for compliance.

IX DATA QUALITY PLAN POLICY:

The Data Quality Plan is the official document pertaining to all data quality measures including but not limited to accuracy, completeness and timeliness. This should be referenced for all data quality standards. Any questions about materials in this document or items that are unclear should be addressed with the CoC Lead Agency or the HMIS Agency Administrator.

Procedure: The Data Quality Plan should be referenced and followed for all data quality procedures. Agencies must retain copies of this document and have available for all relevant staff members. If questions are left unaddressed, they should be brought to the attention of the HMIS Lead in a timely manner.

X AGENCY USER AGREEMENT:

All staff are required to sign a HMIS User Agreement and complete HMIS User Training before receiving access to the HMIS. Credentials will not be issued without a signed User Agreement being on file with the CoC Lead and the HMIS Agency Administrator.

Procedure: All HMIS training participants will be given a copy of the HMIS User Agreement at the conclusion of User training. Potential Users will be responsible for completing the User Agreement, obtaining the required signatures and returning the form to the HMIS Lead before User Credentials will be issued. Once all required paperwork is complete, User Credentials can be obtained by calling the HMIS Help Desk.

Appendix B: Short Version of Privacy Policy

Homeless Management Information System
Summary of Privacy Notice

Introduction. HMIS is a computer system for data collection that was created to meet a requirement for the United States Congress. This requirement was passed in order to get a more accurate count for individuals and families who are homeless and to identify the need for various services. Many agencies use this system and share information.

Information in the HMIS System about you that we may share includes:

1) Basic identifying demographic data (name, address, phone number, date of birth).
2) The nature of your situation.
3) Services and referrals you receive from our agency.

Our ability to assist you depends on having certain personal identifying information. If you choose not to share the information we request, we reserve the right to decline services as doing so could jeopardize our status as a service provider. We assume that, by requesting services from our agency, you agree to allow us to collect information and to use or disclose it as described in this notice and otherwise as allowed or required by law.

Your personal data will be used only by this agency or others to which you are referred for services.

Confidentiality Rights: Maintaining the privacy and safety of those using our services is very important to us. This agency follows all confidentiality regulations and also has its own confidentiality policy.

Your Information Rights: As a client, you have the following rights:

1) Access to your record at your request.
2) Request a correction of your record.
3) File a grievance if you feel that you have been unjustly served, put at personal risk, harmed, or your personal information was not handled correctly.

When Information Is Disclosed: The full Privacy Notice sets forth situations when your personal information might be disclosed.

Benefits of HMIS and Agency Information Sharing: Allowing us to share your real name results in a more accurate count of individuals and services used. A more accurate count is important because it can help us and other agencies to meet the needs of our clients, such as:

1) Better identify and coordinate client need for services and to demonstrate types of assistance needed in our area.

2) Obtain additional funding and resources to provide services.
3) Plan and deliver quality services to you and your family.
4) Assist the agency to improve its work.
5) Keep required statistics for state and federal funders.
6) Promote coordination of services so your needs are better met.
7) Make referrals easier by reducing paperwork.
8) Avoid having to report as much information to get assistance from other agencies.

You may keep this summary of the policy. A copy of the full privacy notice is available upon request.

Appendix C: Employee Acknowledgment

_____

Agency Name

Employee Acknowledgment of Privacy Notice

I, _____, hereby acknowledge that I have received, read and pledge to comply with the Homeless Management Information System Privacy Notice.

_____ _____

Date Name