MINNESOTA'S HMIS

Homeless Management Information System

MINNESOTA HMIS POLICIES

v. 2018.1

HMIS Governing Board
hmismn.org

Contents

1. INTRODUCTION

The Minnesota Homeless Management Information System (HMIS)[1] is a collaborative project of the ten Minnesota Continua of Care (CoC), the State of Minnesota, and participating Partner Agencies. The HMIS is an internet-based database that is used by homeless service organizations across Minnesota to record and store client-level information to better understand the numbers, characteristics, and needs of homeless persons and those at risk of homelessness. Mediware Information Systems, Inc. administers the central server and provides the HMIS software, ServicePoint. As of June 2016, the Institute for Community Alliances (ICA) is the Lead Agency/State System Administrator administering the system and managing user and agency licensing, training, and compliance. (Note: ICA is hereinafter referred to as simply the "Lead Agency.")

HMIS enables service providers to measure the effectiveness of their interventions and facilitate longitudinal analysis of service needs and gaps. Information that is gathered from clients via interviews conducted by service providers is aggregated and made available to policy makers, researchers, service providers, and advocates. Data about the extent and nature of homelessness in the state of Minnesota are used to inform public policy decisions aimed at addressing and ending homelessness at local, state, and federal levels.

Guidance for the implementation of Minnesota's HMIS is provided by a broad-based Governing Board. Board committees work closely with the Lead Agency to secure funding, set and manage priorities within available funding, collect and incorporate user feedback, and provide appropriate oversight and guidance. The Continua of Care, Minnesota Tribal Collaborative, and State Agencies select, and users elect, representatives to serve on the Governing Board, while committees are open to all stakeholders who may wish to participate in the direction of Minnesota's HMIS. Meeting information is available on the Minnesota HMIS website.

This document provides the policy guidelines and standards that govern HMIS operations, as executed by the Lead Agency and Local System Administrators,[2] and also describes the responsibilities of Partner Agencies and users. It was approved by the HMIS Governing Board on January 8, 2018 and replaces two earlier documents: "Minnesota's HMIS Policies and Procedures" (November 2014) and "Minnesota HMIS System Administrator Policies & Procedures" (December 2014). It will be reviewed annually by the Lead Agency and the HMIS Governing Board.

[1] A glossary of terms is provided in Appendix A.

[2] Local System Administrators include both Continuum of Care Coordinators and designated Local System Administrators, as they both have the same level of access in HMIS and are often one and the same.

1.1 Contact Information

Minnesota HMIS website: hmismn.org
HMIS Help Desk: MNHMIS@icalliances.org
Lead Agency: icalliances.org
1508 E. Franklin Ave.
Suite 100
Minneapolis, MN 55404

1.2 Participating Entities

Regardless of funding source, entities which may use HMIS include, but are not limited to:

- Coordinated Entry Assessors and Priority List Managers
- Day Shelters and Drop-In Centers for persons who are homeless
- Emergency Shelters serving homeless adults, families, and youth[3]
- Transitional Housing programs
- Rapid Re-housing programs
- Supportive Housing programs (whether scattered site or on-site)
- Street and Community Outreach programs to persons who are homeless
- Supportive Service programs serving persons who are homeless

In addition, HMIS participation is a requirement of various funders. On the Federal level, HMIS participation is mandated for service and housing providers that receive funding through the following agencies and funding sources:

Department of Housing and Urban Development (HUD)

- Continuum of Care Program (CoC)
- Emergency Solutions Grant (ESG)
- Housing for Persons with AIDS (HOPWA)[4]

Department of Health and Human Services (HHS)

- Projects for Assistance in the Transition from Homelessness (PATH)
- Runaway and Homeless Youth Program (RHY)

[3] In general, domestic violence programs are prohibited from participation in the HMIS by federal legislation, under the Violence Against Women Act (VAWA). Please see hmismn.org or contact the Lead Agency for additional information.

[4] Only competitively-funded HOPWA projects serving homeless individuals are required to use the HMIS. HOPWA block grants are not required to use the HMIS.

Department of Veterans Affairs (VA)

- Supportive Services for Veteran Families (SSVF)

On the state level, the Minnesota Department of Human Services and the Minnesota Housing Finance Agency require HMIS participation for their grantees under the following programs:

Minnesota Department of Human Services

- Emergency Services Program (ESP)
- Emergency Solutions Grant Program (ESG)[5]
- Long-Term Homelessness Supportive Services Fund (LTHSSF)
- Healthy Transitions and Homeless Prevention (HTHP)
- Housing Support (HS)
- Runaway and Homeless Youth Act (HYA)
- Transitional Housing Program (THP)

Minnesota Housing Finance Agency

- Family Homeless Prevention and Assistance Program (FHPAP)
- Long-Term Homelessness (LTH)

1.3 Federal HMIS Policies

In addition to the Minnesota HMIS Policies contained herein, Minnesota's HMIS must also comply with federal HMIS requirements. These requirements are detailed in a suite of HMIS Data Standard resources, an overview[6] of which is provided below:

Manual Name & Link	**Intended Audience**	**Contents**
HMIS Data Standards Dictionary	HMIS Vendors & HMIS Lead Agencies	The manual provides the detailed information required for system programming on all HMIS elements and responses required to be included in HMIS software. It delineates data collection requirements, system logic, and contains the XML and CSV tables and numbers.

[5] The Minnesota Department of Human Services distributes ESG funding as a sub-grantee of HUD. This funding has the same data collection requirements as other ESG funding in the state, which is distributed through cities and counties.

[6] Source: HMIS Data Dictionary, June 2017, Version 1.2.

		The manual also includes critical information about data collection stages, federal partner data collection required elements, and metadata data elements.
HMIS Data Standards Manual	HMIS Lead Agencies & HMIS Users	The manual provides a review of all of the Universal Data Elements and Program Descriptor Data Elements. It contains information on data collection requirements, instructions for data collection, and descriptions that the HMIS User will find as a reference.
HMIS Project Descriptor Data Elements Manual	HMIS Lead Agencies	The Project Descriptor Manual is designed to provide specific information about the Project Descriptors required to be set up in the HMIS by the HMIS Lead Agency.

These documents are typically reviewed and updated each year, and changes tend to be effective October 1, in line with the Federal Fiscal Year.

HMIS Federal Partner Program Manuals contain additional detailed information on HMIS project setup and data collection for federally-funded programs:

- CoC Program Manual
- ESG Program Manual
- HOPWA Program Manual
- PATH Program Manual
- RHY Program Manual
- VA Program Manual

2. JOINING THE HMIS

While HMIS participation is open to homeless service organizations regardless of funding source, all Partner Agencies and users must agree to and abide by HMIS policies and procedures and related requirements. These requirements are described throughout this document, whereas this section focuses specifically on the process of new agencies, projects, and users joining the HMIS.

2.1 Partner Agency Requirements

Agency-Level Documents

In order to obtain and maintain access to the HMIS, Partner Agencies must complete and adhere to the following documents:

1. **Agency Agreements** underwrite the legal relationship between a Partner Agency and the Lead Agency as it relates to HMIS responsibilities and compliance with policies and procedures. The Agency Agreement must be signed by the Partner Agency's executive director. The Lead Agency will retain the original document.

2. **Local HMIS Data Use and Administration Agreements (LSA Agreements)** underwrite the legal relationship between a Partner Agency and Local System Administrator as it relates to HMIS responsibilities and compliance with policies and procedures. The Lead Agency will retain the original document.

3. **Business Associate Agreements** are required for Partner Agencies covered under HIPAA and protect personal health information in accordance with HIPAA guidelines.

4. **Qualified Service Organization Agreements** are required for Partner Agencies covered under Federal Drug and Alcohol Confidentiality Regulations (42 CFR Part 2).

Minimum Technology Requirements

For proper access to the HMIS, Partner Agencies should meet the following minimum technology requirements:

<u>Minimum Computer Requirements</u>

- A PC with a 2 Gigahertz or higher processor, 40GB hard drive, 512 MB RAM, and Microsoft Windows 7 (or later)
- The most recent version of Google Chrome, Safari, Internet Explorer, or Firefox. No additional plug-in is required. It is recommended that your browser have a 128 cipher / encryption strength installed. The browser's cache should be set to "Check for new version of the stored pages: Every visit to page."
- A broadband Internet connection or LAN connection. Dial-up modem connections are not sufficient.
- Virus protection updates
- Mobile devices used for HMIS data entry must use the Mozilla Firefox, Google Chrome, or Apple Safari internet browsers. Apple Safari must be used on the latest version of iOS.

Additional Recommendations

Memory

- Windows 7: 4Gig recommended (2 Gig minimum)

Monitor

- Screen Display: 1024x768 (XGA) or higher; 1280x768 strongly advised

Processor

- A Dual-Core processor is recommended.

Slow system response times that may arise as a result of slow internet connections cannot be controlled by the HMIS Lead Agency.

Staff or Volunteers Eligible to Become HMIS Users

The Partner Agency must have at least one staff member or volunteer who is eligible to become an HMIS user. Users must be paid staff or official volunteers of a Partner Agency. An official volunteer must complete a volunteer application with the Partner Agency, undergo agency training, and record volunteer hours with the agency. Individuals who are solely contracting with a Partner Agency must be subject to the same vetting and training as staff and volunteers who become HMIS users. All users must be at least 18 years old and possess basic computer skills. The Partner Agency is responsible for the actions of its users and for their training and supervision, in accordance with the Agency Agreement.

Designated Agency HMIS Contact

The Partner Agency's Executive Director or their designee must select at least one person to act as the Designated Agency HMIS Contact. Multiple Contacts are most appropriate for large agencies that operate in multiple Continuum of Care regions or have multiple departments. The responsibilities of the Contact are to:

1. Provide updated agency information in a timely manner to the Lead Agency for update in the HMIS. This includes providing notification about new projects, new users, closed projects, and users that no longer work at the agency.
2. Understand and comply with funder data collection and reporting requirements.
3. Ensure that the Partner Agency obtains a unique user license for each user at the agency, and that HMIS access is granted only to staff members that have received training, have completed the User Agreement, and are authorized to use the HMIS. This includes making the Lead Agency aware of any changes to the users of the Partner Agency in accordance with the Agency Agreement.
4. Inform the Lead Agency of any violations of HMIS policies and procedures.

Use of a Comparable Database by Victim Service Providers

Victim service providers, as defined at 24 CFR 576.3, are agencies whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking. Victim service providers must not directly enter or provide data for entry into the HMIS if they are legally prohibited from participating in the HMIS.[7] Individual projects that meet the definition of victim service providers are subject to the same restriction, even if they are a part of an

[7] Victim service providers in Minnesota have historically entered anonymous data into the HMIS. Update (11/1/2017): The HMIS Governing Board and the Lead Agency are working with the Minnesota Coalition for Battered Women on a plan to transition all victim service providers out of the HMIS in order to fully comply with the policy above.

agency whose primary mission is not to provide services to victims of domestic violence, dating violence, sexual assault, or stalking.

Victim service providers that are recipients of funds requiring participation in the HMIS, but are prohibited from entering data in the HMIS, must use a comparable database to enter client information. A comparable database is a database that can be used to collect client-level data over time and generate unduplicated aggregated reports based on the client information entered. The reports generated by a comparable database must be accurate and provide the same information as the reports generated by the HMIS.

Persons fleeing domestic violence, dating violence, sexual assault, or stalking who are served by non-victim service providers are not prohibited from having their data entered into the HMIS. However, a client may refuse to answer HMIS questions in accordance with the Baseline Privacy Policy outlined in Section 5 of these policies. Data sharing is permitted if the client agrees to release their information by signing the Release of Information (ROI) form.

2.2 New Projects

A **Project Descriptor Elements Form** is required for new Partner Agencies and existing Partner Agencies with new projects. The form, which gathers information such as project funding source, target population(s), and beds, allows the Lead Agency to configure data collection appropriately for the agency in the database. Forms should be submitted at least 10 business days prior to the start of the project to allow enough time for processing.

2.3 New Users

In addition to completing New User Training as described in the following section, the following are required for each new user.

License Fee
An annual license fee is required for each user at the Partner Agency. Upon registration for New User Training, the new user will indicate whether the Partner Agency wishes to purchase an additional license or transfer a license from another user at no cost.

User Agreement
A User Agreement listing user policies and responsibilities is electronically signed by each authorized user. An electronic or hard copy of the original document must be kept by the Partner Agency.

3. USER TRAINING REQUIREMENTS

3.1 New User Training

All users are required to attend New User Training with the Lead Agency prior to receiving access to the system. The New User Training Series requires users to take program- and/or project-specific training related to the programs and projects administered by their agency.

Timely Completion
Once a new user begins the HMIS New User Training Series, the user has 20 business days to complete the training series and all required assignments. Lead Agency staff will review the user's assignments and determine if corrections are needed.

Successful Completion
Lead Agency staff may determine that a new user failed to grasp the necessary data entry concepts based on the quality of the user's assignments. Lead Agency staff may use their discretion to require new users to repeat New User Training. If a new user fails to successfully complete their assignments after repeated attempts, Lead Agency staff may use their discretion to determine that the new user is not capable of accurate and complete data entry and may refuse to issue the new user a Minnesota HMIS user license.

Exceptions
If a user requesting a new user license had a license for the Minnesota HMIS in the past 365 days, the user will be given the option to test out of New User Training through a demonstration of fundamental data entry knowledge. The Lead Agency has sole discretion to determine whether the user has successfully tested out of this requirement.

3.2 Ongoing Training

Annual Security Training
All users are required to attend annual security training provided by the Lead Agency to retain their user license.

Recertification Training
At the discretion of the Lead Agency, users may be required to complete a recertification training in the event of significant changes to data collection requirements, data entry workflow, or HMIS policies and procedures. Users who do not complete recertification training in a timely fashion may have their licenses suspended until training has been completed.

New User Training as Remedial Training
If the Lead Agency determines that data entered by a current user does not meet minimum data quality standards, or if a user has not accessed the system within three months of completing New User Training, users may be required to repeat this training.

4. DATA SECURITY

The Lead Agency, Local System Administrators, and Partner Agencies are jointly responsible for ensuring that HMIS data processing capabilities, including the collection, maintenance, use, disclosure, transmission and destruction of data, comply with the HMIS security policies and procedures. When a security standard conflicts with other federal, state and local laws to which the Partner Agency must adhere, the Partner Agency must contact the Lead Agency to collaboratively update the applicable policies for the Partner Agency to accurately reflect the additional protections.

4.1 Passwords

Passwords are the individual's responsibility and users cannot share passwords. Any passwords that are written down are to be stored securely and must be inaccessible to other persons. Users are not to store passwords on a personal computer for easier log on.

4.2 Procedure for Reporting Security Incidents

Users and Designated Agency HMIS Contacts should report all unlawful access of the HMIS and unlawful attempted access of the HMIS. This includes borrowing, loaning, sharing, or theft of usernames and passwords. Security incidents should be reported to the Lead Agency within 24 hours of their discovery. The Lead Agency will use the HMIS user audit trail report to determine the extent of the breach of security.

4.3 Violation of Security Procedures

All potential violations of any security protocols will be investigated by the Lead Agency and/or the HMIS Governing Board, and any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to: a formal letter of reprimand, suspension of system privileges, revocation of system privileges and criminal prosecution.

All confirmed security violations will be communicated in writing to the affected client within 14 days, unless the client cannot be located. If the client cannot be located, a written description of the violation and efforts to locate the client will be prepared by the Lead Agency and placed in the client's file at the Agency that originated the client's record.

Any Agency that is found to have consistently and/or flagrantly violated security procedures may have their access privileges suspended or revoked, as described in Section 10.

4.4 Disaster Recovery Plan

Minnesota's HMIS is covered under Mediware Systems Disaster Recovery Plan. Due to the nature of technology, unforeseen service outages may occur. In order to assure service reliability, Mediware Information Systems provides the following disaster recovery plan. Plan highlights include:

- Database tape backups occur nightly.
- Tape backups are stored offsite.
- Seven-day backup history is stored locally on instantly accessible Raid 10 storage.
- One-month backup history is stored offsite.
- Access to a Mediware Information Systems emergency line to provide assistance related to “outages” or “downtime” 24 hours a day.
- Data is backed up locally on instantly accessible disk storage every 24 hours.
- The application server is backed up offsite, out-of-state, on a different internet provider and on a separate electrical grid via secured Virtual Private Network (VPN) connection.
- Backups of the application site are near-instantaneous (no files older than five minutes).
- The database is replicated nightly at an offsite location in case of a primary data center failure.
- Priority-level response (ensures downtime will not exceed four hours).

5. DATA PRIVACY

The Lead Agency, Local System Administrators, and Partner Agencies are jointly responsible for complying with HMIS privacy policies and procedures. When a privacy standard conflicts with other federal, state and local laws to which the Partner Agency must adhere, the Partner Agency must contact the Lead Agency to collaboratively update the applicable policies for the Partner Agency to accurately reflect the additional protections.

5.1 Baseline Privacy Policy

Collection of Personal Information

Personal information will be collected for the HMIS only when it is needed to provide services, when it is needed for another specific purpose of the agency where a client is receiving services, or when it is required by law. Personal information may be collected for these purposes:

- To provide or coordinate services for clients
- To find programs that may provide additional client assistance
- To comply with government and grant reporting obligations
- To assess the state of homelessness in the community, and to assess the condition and availability of affordable housing to better target services and resources

Personal information may also be collected from:

- Additional individuals seeking services with a client
- Other private organizations that provide services and participate in the HMIS

Only lawful and fair means are used to collect personal information. Personal information is collected with the knowledge and consent of clients. While some information may be required by projects or public or private funders to determine eligibility for housing or services, or to assess needed services, clients generally should not be denied assistance if they refuse or are unable to supply certain pieces of information.[8]

Posted Data Privacy Notice

This Notice must be posted and viewable by clients at intake to provide information on their rights and HMIS policies related to personal data. This Notice provides a brief overview of data privacy.

HMIS Data Privacy Notice

This Notice[9] must be reviewed with all clients at intake to provide information on their rights and HMIS policies related to personal data. This Notice provides more detailed information about why HMIS data is collected, when and to whom data may be released, privacy protections, and client rights.

[8] HMIS intake forms include 'Client refused' response categories to allow programs to track refusals. The HMIS Data Standards Manual provides additional information about handling client refusals for federally-required questions.

[9] The HMIS Data Privacy Notice is included as the first page of the Release of Information (ROI) packet.

Inspection and Correction of Personal Information
Clients may inspect and receive a copy of their personal information maintained in the HMIS. The agency where the client receives services will offer to explain any information that a client may not understand.

If the information listed in the HMIS is believed to be inaccurate or incomplete, a client may submit a verbal or written request to have his/her information corrected. Inaccurate or incomplete data may be deleted or marked as inaccurate or incomplete and supplemented with additional information.

A request to inspect or copy one's personal information may be denied if:

- The information was compiled in reasonable anticipation of litigation or comparable proceedings,
- The information was obtained under a promise of confidentiality and if the disclosure would reveal the source of the information, or
- The life or physical safety of any individual would be reasonably endangered by disclosure of the personal information.

If a client's request to view or correct their personal information is denied, the Agency where the client receives services will explain the reason for the denial. The client's request and the reason for the denial will be included in the client's record.

Client requests to view or correct their personal information may be denied if they are made in a repeated and/or harassing manner.

5.2 Statewide Data Sharing

As of October 2016, Minnesota's HMIS employs statewide data sharing as a means to implement Coordinated Entry, reduce data collection and entry burden, and facilitate other coordination between Partner Agencies.

Client Release of Information
Statewide Data Sharing is a process guided by the client through the Release of Information (ROI). It is therefore imperative that the client understand the ROI, and that the Partner Agency address any questions the client may have, while respecting the client's right to decline to share data.

Prior to designating any information for sharing with other Agencies, the Partner Agency will obtain the informed consent of the Client, using **Minnesota's HMIS Release of Information**. If a client does not consent pursuant to Minnesota's HMIS Release of Information form, information may be entered into Minnesota's HMIS, but may not be shared with other Partner Agencies. It is the responsibility of the Partner Agency entering information about a client to determine whether consent has been obtained; to make appropriate entries to either designate the information as appropriate for sharing or prohibit information sharing; and to implement any restrictions on information sharing.

Agency Responsibilities
At a minimum, the Partner Agency must meet the following standards:

1. The Partner Agency will use the Minnesota's HMIS Release of Information form (ROI), for all clients where written or verbal consent is required.
    a. If the Partner Agency does not share data with other Agencies, the ROI form is not required. However, the Partner Agency will provide Minnesota's HMIS Data Privacy Notice for review by all clients and provide clients with copies as requested.
    b. If questions arise (for example questions on which programs within the Partner Agency share data with other agencies), the Partner Agency will contact the Lead Agency.
2. The Partner Agency will note any limitations or restrictions on information sharing on a client's ROI with appropriate data entries into Minnesota's HMIS. If questions arise (for example, questions on how to implement restrictions on information sharing), the Partner Agency will contact the Lead Agency.
3. The Partner Agency will be responsible for ensuring that consent is knowing, informed and given by a person competent to provide consent. For example, in the case of a minor, The Partner Agency will comply with applicable laws regarding minor consent by obtaining the consent of a parent or guardian, unless consent of the minor is acceptable under the Minor Consent law (e.g. Minn. Stat. §144.341–144.347). In cases of incompetent adults, the Partner Agency must obtain consent from a person authorized to consent under Minnesota law.
4. If a client withdraws or revokes consent for release of information, the Partner Agency is responsible for immediately contacting the Lead Agency to ensure that client's information will not be shared with other Agencies from that date forward.
5. The Partner Agency that received the client's initial ROI form will scan and upload the signed copy of the form to the HMIS. Partner Agencies may be required to keep the original copy for a period of seven years, as dictated by Partner Agency policy or funder requirements. ROI forms will be available for inspection and copying by the Lead Agency at any time.
6. If an ROI has been properly recorded in the client's HMIS record by another Partner Agency, the Partner Agency need not present the client with another ROI form.[10] However, Covered Entities must always present a ROI form, as detailed in the section below. Other Partner Agencies may elect to do so at their discretion.

Additional Responsibilities of Covered Entities

Partner Agencies that are also Covered Entities under HIPAA and any program subject to 42 CFR Part 2 must obtain a signed Minnesota's HMIS Release of Information form before authorizing the Lead Agency to use or disclose information entered into the HMIS. If a client does not sign Minnesota's HMIS Release of Information form, information may be entered into Minnesota's HMIS, but may not be further disclosed. The information may be used by the Lead Agency as permitted by law and the HMIS Data Privacy Notice. It is the responsibility of the Partner Agency entering information about a client to ensure compliance with HIPAA including ensuring that all appropriate HIPAA Notices have been provided to clients, to determine whether consent has been obtained; making appropriate entries to either designate the information as appropriate for use or disclosure by the Lead Agency or to prohibit such use or disclosure; and implementing any restrictions on the use of the information.

[10] The requirement to scan and upload signed Consent forms is effective as of the date these policies were first adopted. Client records created prior to that date that recorded Consent according to the guidance from that time are considered to have Consent properly recorded.

Covered Entities may utilize their own forms but shall supplement these forms with the information conveyed in “Minnesota’s HMIS: Data Privacy Notice & Client Release of Information.”

Covered Entities must present a separate ROI form to each adult that is seeking services, regardless of whether a ROI form has been presented to them in the past.

No Conditioning of Services

Agency will not condition any services upon or decline to provide any services to a client based upon a client's refusal to sign a form for the sharing of information in Minnesota’s HMIS, unless a program funder or internal management practices require the entry of identified information into the HMIS to deliver services. Further, Partner Agencies may not limit client service or refuse to provide service in a way that discriminates against clients based on information the Partner Agency obtained from the HMIS. Partner Agencies may not penalize a client based on historical data contained in the HMIS.

5.3 Research Uses and Publication of HMIS Data

Research uses and publication of HMIS data are governed by HMIS policies, including Minnesota’s HMIS Data Privacy Notice, Minnesota’s HMIS Release of Information, Agency Agreements, Local HMIS Data Use and Administration Agreements (LSA Agreements), and Business Associate Agreements.

Data may not be released in an aggregated report from a data set that is small enough or unique enough to allow identification of an individual client’s information to be extracted from the report. If it is determined that a preliminary report may not be published due to concerns of release of identifiable data, the Lead Agency or Local System Administrator will remove postings, shred paper copies of the report, and notify review partners to destroy any copies of the report.

A Local System Administrator may not access or use regional, Tribal- or agency-specific data for the purpose of providing their agency or any partner agency a competitive advantage. Data collection and reporting of Tribal-specific information will only be done with the written permission of the Minnesota Tribal Council or its authorized representative.

If a report identifies one or more specific agencies or programs, agencies will be given a period of 15 business days to review and comment on the information as presented in the report. Agency and Continuum of Care review periods may be waived if prior approval is obtained by the Lead Agency or the Local System Administrator.

Data may be released to external stakeholders for research purposes by the Lead Agency, as approved by the HMIS Governing Board. The HMIS Governing Board will approve or deny requests to release data based on the potential benefits and costs to clients, Partner Agencies, and other stakeholders. If at all possible, the release of identified data will be avoided. If identified data is needed, the HMIS Governing Board will work with the Lead Agency to ensure that proper procedures and precautions are in place prior to releasing data.

5.4 Client Complaints, Grievances, and Questions

If a client believes that their rights have been violated related to their personal or private data held in the HMIS, a written complaint may be filed. The complaint may be filed with the Partner Agency serving the client and forwarded to the Lead Agency if resolution is not found. If the client believes that their shelter or services may be threatened due to the complaint, a complaint may be made directly to the Lead Agency. The Lead Agency will report all grievances to the Governing Board, which will act as a final arbiter of any complaints not resolved by the Partner Agency or the Lead Agency.

The Partner Agency and the Lead Agency are prohibited from retaliating against clients for filing a complaint. Identifying information will be kept confidential, unless the client gives express permission for such information to be shared between the Partner Agency and the Lead Agency.

The Partner Agency must make **Minnesota's HMIS Service Recipient Grievance Form** available to clients upon request.

6. DATA QUALITY

Data quality is a term that refers to the reliability and validity of client-level data collected in the HMIS. It is measured by the extent to which the client data in the system reflects actual information in the real world. No data collection system has a quality rating of 100%. However, to present accurate and consistent information on homelessness, it is critical that the HMIS have the best possible representation of reality as it relates to persons experiencing homelessness and the projects that serve them. Specifically, the goal is to record the most accurate, consistent and timely information in order to draw reasonable conclusions about the extent of homelessness and the impact on the homeless service system.

6.1 Minimum Data Collection Standards

All Partner Agencies are responsible for asking all clients a minimum set of questions, or data elements.[11] These required data elements include: (1) the Universal Data Elements required federally and at the state level by the HMIS Governing Board; and (2) Program-Specific Data elements, which depend on the funder and may not be required at all if a program is not funded by a program that requires the use of the HMIS. The minimum expectations for data entry for all programs entering data in the HMIS are the focus of New User Training.

Partner Agency programs are configured by the Lead Agency to collect the required data elements based on information provided by the Partner Agency and its Designated Agency HMIS Contact. Lead Agency staff will consult with the Designated Agency HMIS Contact in attempts to ensure proper setup, but responsibility for complying with funder requirements lies with the Partner Agency.

Agencies may collect additional information beyond the minimum required data elements, as long as the collection of these questions does not interfere with the minimum required data elements.

6.2 Data Quality Plan

To ensure high-quality data, the Lead Agency, Minnesota's ten Continua of Care, Partner Agencies, and users will regularly and collectively assess and address the quality of data by examining characteristics such as timeliness, completeness, and accuracy. This effort is detailed in the Minnesota HMIS Data Quality Plan, which is approved by the HMIS Governing Board and can be found on the Minnesota HMIS Website.

6.3 XML Imports

While HMIS databases are required to have the capacity to accept XML imports, the Lead Agency and the HMIS Governing Board reserve the right to not allow XML imports into Minnesota's HMIS. Allowing XML imports may impact data integrity and increase the likelihood of duplication of client files in the system.

[11] However, as noted in the Baseline Privacy Policy in the prior section, clients may still refuse to answer certain questions.

7. HMIS SOFTWARE VENDOR REQUIREMENTS

Physical Security
Access to areas containing HMIS equipment, data and software will be secured.

Firewall Protection
The vendor will secure the perimeter of its network using technology from firewall vendors. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

User Authentication
Users may only access the HMIS with a valid username and password combination that is encrypted via SSL for internet transmission to prevent theft. If a user enters an invalid password three consecutive times, they are automatically shut out of that HMIS session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Application Security
HMIS users will be assigned a system access level that restricts their access to only necessary and appropriate data.

Database Security
Wherever possible, all database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a minimal number of points; as with production servers, production databases do not share a master password database.

Technical Support
The vendor will assist Lead Agency staff to resolve software problems, make necessary modifications for special programming, and will explain system functionality to the Lead Agency.

Technical Performance
The vendor maintains the system, including data backup, data retrieval, and server functionality/operation. Upgrades to the system software will be continuously developed and implemented.

Hardware Disposal
Data stored on broken equipment or equipment intended for disposal will be destroyed using industry standard procedures.

8. LOCAL SYSTEM ADMINISTRATION

Minnesota's HMIS is a collaborative partnership with partners at all levels working to advance HMIS as a tool to inform and support efforts to end homelessness. Continuum of Care Coordinators and designated Local System Administrators, jointly referred to herein as "Local System Administrators," are key partners in analyzing data and meeting needs at a local level. While Local System Administrators must adhere to all policies contained in this document, this section enumerates roles, responsibilities, and policies specific to their work.

8.1 Coordination with the Lead Agency

As local needs and local capacity vary, coordination between the Lead Agency and Local System Administrators is key. The Lead Agency and Local System Administrators will jointly develop and approve a written annual plan for each Continuum of Care that delineates roles and responsibilities of both parties.

Responsibilities may include in-depth support for the following:

- Annual Homeless Assessment Report
- Annual Performance Reports
- Communicating HMIS updates to the Continuum of Care
- Continuum of Care Program Competition
- Housing Inventory Chart
- Maintaining and increasing bed coverage (participation of homeless programs in the HMIS)
- Point in Time Homelessness Count
- Quarterly Data Quality Process
- Supporting continuous quality improvement efforts
- Supporting HMIS user group meetings in the Continuum of Care
- Other projects or tasks as jointly approved by the parties

In the event that the Lead Agency and Local System Administrators cannot agree to a written annual plan, the matter will be escalated to the HMIS Governing Board for discussion and resolution.

8.2 System Configuration

Local System Administrators will not make changes to HMIS providers without prior approval from the Lead Agency and the Designated Agency HMIS Contact for that provider. However, Local System Administrators are allowed to create their own reporting groups in the HMIS for purposes of aggregate reporting.

8.3 Local System Administrator Expanded Reporting Access Agreement"

Due to technical issues with a prior database restructure, Local System Administrators (LSA) are currently unable to view all data within their Continua of Care. To address this problem, the Lead Agency and Policy and Prioritization Committee of the HMIS Governing Board developed the **Local System Administrator Expanded Reporting Access Agreement**. This agreement,

between the Lead Agency and the LSA, technically grants the LSA full visibility to statewide HMIS information in the Advanced Reporting Tool (“ART”) which is used to report on HMIS data. However, the agreement reaffirms that the LSA may only view data from their Continuum of Care as needed for legitimate business purposes.

9. AGENCY SYSTEM ADMINISTRATION

Minnesota HMIS Partner Agencies may elect to develop internal capacity for system administration. Partner Agency System Administrators are trained by the Lead Agency and granted system administration access at the sole discretion of the Lead Agency. While Partner Agency System Administrators must adhere to all policies contained in this document, this section enumerates roles, responsibilities, and policies specific to their work.

9.1 Coordination with the Lead Agency

As Partner Agency needs and capacity vary, coordination between the Lead Agency and Partner Agency System Administrators is key. The Lead Agency and Partner Agency System Administrators will jointly develop and approve a written annual plan for the Partner Agency that delineates roles and responsibilities of both parties. In the event that the Lead Agency and Partner Agency System Administrators cannot agree to a written annual plan, the matter will be escalated to the HMIS Governing Board for discussion and resolution.

9.2 System Configuration

Partner Agency System Administrators will not make changes to HMIS providers without prior approval from the Lead Agency.

10. SPECIAL POLICIES

10.1 User Conflict of Interest

Users who are also clients with files in the HMIS are prohibited from entering or editing information in their own file. All users are also prohibited from entering or editing information in files of immediate family members. All users must sign the Minnesota User Agreement, which includes a statement describing this limitation, and report any potential conflict of interest to their Designated Agency HMIS Contact. The Lead Agency may run an HMIS user audit trail report to determine if there has been a violation or suspected violation of the conflict of interest agreement.

10.2 Users Entering or Reporting on Data for Another Partner Agency

Coordinated Services Agreements allow a specifically named HMIS user to enter client data as, or on behalf of, another specifically named Partner Agency and/or to report on behalf of a specifically named Partner Agency. The signed agreement will be maintained by the Lead Agency. The named HMIS User will have access to the designated HMIS Providers.

11. VIOLATION OF HMIS POLICIES

HMIS users and Partner Agencies must abide by all HMIS policies and procedures found in the HMIS Policies and/or Procedures manuals, the User Agreement, and the Agency Agreement. Repercussion for any violation will be assessed in a tiered manner. Each user or Partner Agency violation will face successive consequences – the violations do not need to be of the same type in order to be considered second or third violations. User violations do not expire. No regard is given to the duration of time that occurs between successive violations of the HMIS operation policies and procedures as it relates to corrective action. Any user or Partner Agency violations may be appealed to the HMIS Governing Board.

- First Violation – the user and Partner Agency will be notified of the violation in writing by the Lead Agency. The user's license will be suspended for 30 days, or until the Partner Agency notifies the Lead Agency of action taken to remedy the violation. The Lead Agency will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. The Lead Agency will notify the HMIS Governing Board of the violation during the next scheduled Governing Board meeting following the violation.

- Second Violation – The user and Partner Agency will be notified of the violation in writing by the Lead Agency. The user's license will be suspended for 30 days. The user and/or Partner Agency must take action to remedy the violation; however, this action will not shorten the length of the license suspension. If the violation has not been remedied by the end of the 30-day user license suspension, the suspension will continue until the Partner Agency notifies the Lead Agency of the action taken to remedy the violation. The Lead Agency will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. The Lead Agency will notify the HMIS Governing Board of the violation during the next scheduled Governing Board meeting following the violation.

- Third Violation – the user and Partner Agency will be notified of the violation in writing by the Lead Agency. Lead Agency will notify the HMIS Governing Board of the violation and convene a review panel made up of Governing Board members who will determine if the user's license should be terminated. The user's license will be suspended for a minimum of 30 days, or until the Governing Board review panel notifies the Lead Agency of their determination, whichever occurs later. If the Governing Board determines the user should retain their user license, the Lead Agency will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. If users who retain their license after their third violation have an additional violation, that violation will be reviewed by the Governing Board review panel.

Any user or other fees paid by the Partner Agency will not be returned if a user's or Partner Agency's access to the HMIS is revoked.

Notifying the HMIS Lead Agency of a Violation
It is the responsibility of each Designated Agency HMIS Contact and user to notify the HMIS Lead Agency within 24 hours of when they suspect that a User or Partner Agency has violated any HMIS operational agreement, policy, or procedure. A complaint about a potential violation must include the User and Partner Agency name and a description of the violation, including the date or timeframe of the suspected violation. Complaints should be sent in writing to the HMIS

Lead Agency at mnhmis@icalliances.org. The name of the person making the complaint will not be released from the HMIS Lead Agency if the individual wishes to remain anonymous.

Violations of Local, State or Federal Law

Any Partner Agency or user violation of local, state or federal law will immediately be subject to the consequences listed under the Third Violation above.

Potential to Escalate

All violations will be assessed by the Lead Agency and depending on their severity may be subject to the consequences listed under the Third Violation above as determined by the Lead Agency.

Multiple Violations within a 12-Month Timeframe

During a 12-month calendar year, if there are multiple users (three or more) with multiple violations (two or more) from one Partner Agency, the Partner Agency as a whole will be subject to the consequences listed under the Third Violation above.

12. APPENDIX A: GLOSSARY

Designated Agency HMIS Contact – The individual responsible for HMIS use at each partner agency.

Homeless Management Information System (HMIS) – an internet-based database that is used by homeless service organizations across Minnesota to record and store client-level information to better understand the numbers, characteristics and needs of homeless persons and those at risk of homelessness.

HMIS Governing Board – the group of HMIS stakeholders who are responsible for approving and implementing the HMIS Policies and Procedures, and for funding, planning, and overseeing improvements to Minnesota's HMIS. Information on board composition, committee responsibilities, and meeting times can be found on the Minnesota HMIS Website.

HMIS Lead Agency – The HMIS Lead Agency is responsible for the technical design, implementation, and operation of the HMIS. In doing so, the Lead Agency provides Partner Agencies and users with training and technical support, ensures compliance with HMIS policies and procedures, and plans and jointly approves with the HMIS Governing Board an annual budget and work plan. Minnesota's HMIS Lead Agency is the Institute for Community Alliances.

HMIS Vendor – The HMIS Vendor designs the HMIS software and provides ongoing support to the System Administrators. Minnesota's HMIS Vendor is Mediware Information Systems.

Local System Administrators – Persons trained and approved by the HMIS Lead Agency who provide reporting or system administration support.

Partner Agencies – The homeless service organizations that use the HMIS.

Program-Specific Data Elements – Questions that are designed, managed, and required by at least one of the HMIS federal or state partner programs. Federal Program-Specific Data Elements are subject to change every year on October 1, whereas State Program-Specific Data elements are subject to change every year on July 1.

Universal Data Elements (UDEs) – The minimum set of questions that all homeless programs in the HMIS, regardless of funding source, must complete for all clients served. Federal UDEs are outlined in the HMIS Data Dictionary and the HMIS Data Standards Manual, and are subject to change every year on October 1. Minnesota UDEs are determined by the HMIS Governing Board and are subject to change every year on July 1.

Victim Service Provider – a nonprofit agency with a primary mission to provide services to victims of domestic violence, dating violence, sexual assault, or stalking.