HMIS POLICIES AND PROCEDURES MANUAL

Balance of State, Springfield, St. Joseph, Joplin

CONTENTS

VERSION AND REVIEW HISTORY

Version	Description	BoS Date Approved	Springfield Date Approved	Joplin Date Approved	St. Joseph Date Approved
1.0	Original Version	9/2019	2019	2019	*adopted* 11/2021
2.0	Updated	6/2025	10/2025	*adopted* 11/2025	9/2025

INTRODUCTION

This manual describes the policies and procedures that govern the Homeless Management Information System (HMIS), as well as the roles and responsibilities of the HMIS Lead Agency, HMIS Participating Agencies, and HMIS End Users. Standardized policies and procedures are necessary for managing the day-to-day operations of the HMIS implementation.

The policies and procedures in this document fulfill basic Department of Housing and Urban Development (HUD) requirements and have been approved by the Balance of State, Springfield, Joplin, and St. Joseph Continuums of Care.

WHAT IS HMIS?

A Homeless Management Information System (HMIS) is a web-based software system used by homeless and human services organizations to collect client-level information on the characteristics and needs of people at risk of and experiencing homelessness. HMIS is mandated by the U.S. Department of Housing and Urban Development (HUD) for all communities and agencies receiving Continuum of Care (CoC) and Emergency Solutions Grant (ESG) funding.

HUD requires CoCs to designate a single HMIS for the geographic area. Community Services® (formerly known as ServicePoint) is the HMIS software solution designated by 6 of Missouri's Continuums of Care; the software application is a WellSky® product.

What an HMIS is Not

HMIS is not a software that is used by law enforcement to track individuals experiencing homelessness. Furthermore, HMIS data should not be used to determine services and benefits unless federally required. HMIS data should not be used or disclosed in a way that will violate the Fair Housing Act, the Equal Access Rule, and privacy laws.

It's important to note that HMIS software and Case Management software solutions are not synonymous. HMIS has case management functionality, but it does much more than case management software. Bottom line, HMIS software can be used for case management, but Case Management software cannot be used as a Homeless Management Information System.

BENEFITS OF USING HMIS

An HMIS provides significant opportunities to improve access to, and delivery of, housing and services for people experiencing homelessness. An HMIS can accurately describe the scope of homelessness and the effectiveness of efforts to prevent homelessness, reduce returns to homelessness, and make homelessness as brief as possible. An HMIS can strengthen community planning and resource allocation. Use of HMIS provides numerous benefits for service providers, homeless persons, and the State of Missouri.

Service Provider Benefits:

- Provides online, real-time information about client needs and the services available for people experiencing homelessness or at risk of homelessness.
- Assures confidentiality by providing information in a secure system.
- Decreases duplicative client intakes and assessments.
- Tracks client outcomes and provides a client history.
- Generates data reports for local use and for state and federal reporting requirements.
- Facilitates the coordination of services within an organization and with other agencies and programs.
- Provides access to a statewide database of service providers, allowing agency staff to easily select a referral agency.
- Allows agencies to better define and understand the extent of homelessness throughout Missouri.
- Allows agencies to better focus staff and financial resources where homeless services are needed the most.
- Allows agencies to better evaluate the effectiveness of specific interventions and programs.

Client Benefits:

- Agency staff can retrieve records of clients previously served by Partner Agencies, thereby streamlining the intake process.
- An HMIS reduces the frequency with which clients are required to complete intake forms and assessments, should the Agency choose to complete live data entry directly into HMIS. This removes barriers, demonstrates the homeless person's time is valuable and aids in restoring the client's dignity.
- Services and referrals can be coordinated and streamlined.
- HMIS records of enrollments in an emergency shelter or safe haven, or contacts with street outreach workers, can be used to verify homelessness and as 3rd party evidence for documenting chronic homeless status.[1]

HMIS PARTICIPATION

Any agency that provides shelter, housing, or services to individuals at risk of or experiencing homelessness is encouraged to participate in HMIS, regardless of funding source.

[1] When using HMIS to verify homeless status, it should always be considered a starting point for documentation. A gap in HMIS enrollments does not necessarily constitute a break in homelessness.

Examples of entities that use HMIS include, but are not limited to:

- Coordinated Entry Access Levels and Front Doors
- Day Shelters, Cold Weather Shelters, Cooling Shelters, and Drop-In Centers
- Emergency Shelters serving homeless adults, families, unaccompanied children, and youth
- Transitional Housing
- Rapid ReHousing
- Permanent Supportive Housing (site-based or scatted site)
- Street and Community Outreach programs for homeless persons
- Homelessness Prevention and Supportive Services programs serving persons who are homeless or at risk of homelessness

Additionally, HMIS participation is a requirement of various funders. Examples of agencies and federal funding sources that require HMIS participation include but are not limited to:

Department of Housing and Urban Development (HUD)

- Continuum of Care (CoC) Program
- Emergency Solutions Grant (ESG) Program[2]
- Housing for Persons with AIDS (HOPWA) Program[3]
- Youth Homelessness Demonstration Program

Department of Health and Human Services (HHS)

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

Department of Veterans Affairs (VA)

- Supportive Services for Veteran Families (SSVF)

At the state level, Missouri Housing Development Commission (MHDC) requires HMIS participation for their grantees under the following programs:

- Missouri Housing Innovation Program (MoHIP)
- Missouri Housing Trust Fund (MHTF)

Finally, some communities elect to require HMIS as a condition of local funding awards designated for homeless services, such as community block grants.

[2] ESG funds are awarded via formula to territories, states, metropolitan cities, and urban counties. Missouri Housing Development Commission (MHDC) is responsible for administering Missouri's state allocation of ESG funds.

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

HMIS PARTICIPATION LETTERS

Some funders require HMIS participating agencies to include an HMIS participation letter with funding applications. Partner Agencies may request HMIS participation letters from their HMIS System Administrator. HMIS participation letters will be provided to agencies that are:

- Current participating agencies, regardless of compliance status
- Agencies that have initiated the onboarding process and are taking steps to participate in HMIS

VOLUNTARY TERMINATION OF HMIS PARTICIPATION

Reasons for a Partner Agency voluntarily terminating participation include, but are not limited to, the following:

a) The Partner Agency is no longer operating the project(s) for which they were entering data into HMIS.
b) The Partner Agency is no longer mandated to enter data into HMIS by their funder and chooses to no longer participate in HMIS.

Policy

An HMIS Authorized Representative of the Agency must inform the HMIS Lead in writing 30 days prior to their intention to terminate HMIS participation.

Agency Procedure

- The Partner Agency will ensure all relevant project data is current and accurate and that all necessary data corrections have been completed.

- The Partner Agency will run any required reports prior to termination. If a need for reports from HMIS should arise after termination, the Partner Agency may contact the HMIS Lead Agency to request the reports.

HMIS Lead Procedure

- The HMIS Lead Agency will run data quality reports to ensure data is complete and accurate. The HMIS Lead will complete all Project Descriptor Data Elements (PDDE) required to close-out the HMIS project and will remove project access from the Agency's end users.

NOTE ON VICTIM SERVICE PROVIDERS

The Violence Against Women Act (VAWA) prohibits Victim Service Providers (VSP) from entering data into an HMIS database. If a VSP receives CoC or ESG funding, they are required to enter data in a comparable database. It is the responsibility of the HMIS Lead Agency to work with Victim Service Providers to ensure the comparable database meets HUD Data Standards and can successfully upload a CoC APR and ESG CAPER.

PROTECTED PROJECTS

Protected projects serve populations that require special security and privacy considerations. These populations include, but are not limited to, medically fragile individuals, unaccompanied children, and at-risk youth.

Protected projects contribute data to HMIS; however, they do not share client information beyond basic identifiers for the purpose of de-duplicating client records in HMIS.

HMIS LEAD AGENCY

CoCs are required to designate an HMIS Lead Agency to administer day-to-day HMIS operations on behalf of the CoC. Institute for Community Alliances (ICA) is the HMIS Lead Agency designated by six of Missouri's CoCs, including Balance of State, St. Louis City, St. Louis County, Springfield, Joplin, and St. Joseph. ICA administers the day-to-day operations and manages end user licenses, agency onboarding, training, and HMIS compliance.

ICA engages in research and produces reports on homelessness and related issues. In cooperation with state and federal agencies, private research firms, and university researchers, ICA works to inform regional and national efforts to end homelessness.

Hereinafter, ICA will be referred to as "HMIS Lead Agency" or "HMIS Lead".

HMIS SYSTEM ADMINISTRATORS

HMIS System Administrators wear many hats. They manage the technical aspects of HMIS operations; work directly with End Users; ensure authorized access to client information; configure HMIS projects for agencies and according to HUD Data Standards; develop, conduct, and document training for HMIS End Users; cover helpdesk and respond to escalated helpdesk tickets; conduct HMIS and Data Quality Monitoring and Technical Assistance Assessments (TAA).

HMIS System Administrators make every attempt to respond to emails and phone calls in a timely manner. However, many System Administrators work in multiple CoCs, participate in a variety of meetings, and travel on-site for HMIS Monitoring and technical assistance. For best practice, please contact the MoHMIS Helpdesk for immediate assistance.

HMIS TECHNICAL SUPPORT

HMIS technical support is a primary responsibility of the HMIS Lead Agency. The purpose of technical support is to resolve end user-initiated inquiries, fix and resolve issues in an organized and timely manner to ensure end user satisfaction and enable continuity and consistency in the HMIS software functionality.

MoHMIS Helpdesk

ICA shall provide technical assistance via the ICA Missouri Helpdesk during regular business hours.

Hours: Monday – Friday, 8am – 5pm (excluding some holidays)
Email: mohmis@icalliances.org
Phone: 314-502-2454

ICA Missouri Knowledge Base

Knowledge Base contains HMIS FAQs, data collection forms, data entry guides, and reporting tip sheets. We strongly encourage all End Users to bookmark Knowledge Base, so they have "How-to" tip sheets right at their fingertips whenever they need help.

ICA Missouri Website

The ICA Missouri website contains various resources, including contact and location information, HMIS Releases of Information, HMIS Privacy Notice, Consumer Notice, a current list of HMIS Participating agencies, request forms, local performance dashboards and more.

HMIS PARTICIPATION REQUIREMENTS

Agencies receiving Emergency Solution Grant (ESG), Continuum of Care (CoC), Runaway Homeless Youth (RHY), Projects for Assistance in Transition to Housing (PATH), Supportive Services for Veteran Families (SSVF), and other funding mandating HMIS participation 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. Depending on the funding source, fees may be associated with HMIS participation. Agencies should contact the HMIS Lead for any such fees.

AGENCY PARTNER AGREEMENT

The Agency Partner Agreement (APA) is an agreement between the Partner Agency and the HMIS Lead as it relates to HMIS responsibilities and compliance with policies and procedures. The agreement also outlines a Partner Agency's specific requirements for maintaining the confidentiality of client information.

Questions regarding the Agency Partner Agreement can be submitted to the MoHMIS Helpdesk.

Policy

The HMIS Lead Agency must execute a written HMIS Participation Agreement with all HMIS Participating Agencies. All Partner Agencies must communicate policies and expectations within the Agency Partner Agreement to staff through providing them with a copy of the signed Agreement, internal training, or other form of communication.

Agency Procedure

- **New Agencies:** To gain access to HMIS, the Agency Partner Agreement must be completed by the Partner Agency's Executive Director (or equivalent) before the Partner Agency is granted access to the database. The HMIS Lead Agency reviews the APA with prospective Partner Agencies during the agency onboarding process.

- **Participating Agencies:** The Agency Partner Agreement must be signed at least once a year.

HMIS Lead Procedure

- The HMIS Lead will send the most recent Agreement to Agency Directors to renew as part of the annual recertification process at the beginning of the HUD Fiscal Year (October).

- Additionally, the HMIS Lead will provide Partner Agencies with the means to update Authorized Representatives and Designated Contacts throughout the year, should they need to make changes.

DATA COLLECTION

All HMIS participating agencies collect a standard set of client information, established under the 2004 HMIS Data and Technical Standards Final Notice. Agencies are responsible for knowing all the Universal and Program Specific data elements in the most current HMIS Data Standards Manual.

HUD encourages CoCs and Agencies to approach data collection, data-informed processes, and the homelessness system design with empathy and consideration as to how *you* would want to be treated if you were experiencing homelessness. Person-centered data collection improves a client's experience during intake and the accuracy of data collected. A person-centered approach centers the individual in every data collection interaction by creating a welcoming, respectful, and collaborative environment.[4]

MINIMUM DATA COLLECTION STANDARDS

All Partner Agencies are responsible for collecting a minimum set of data. These include:

1. Universal Data Elements – Required to be collected by ALL projects participating in HMIS, regardless of funding source.
2. Common Program Specific Data Elements – Data elements required to be collected by specific programs.

The minimum expectations for data entry for all programs entering data in the HMIS are the focus of New User Training. HMIS Projects are configured by the HMIS Lead to collect the required data elements based on information provided by the Partner Agency.

[4] See appendix for links to client-centered data collection resources.

The HMIS Lead will consult with the Partner Agency to ensure proper configuration in the HMIS, but responsibility for providing the HMIS Lead with program details and complying with funder requirements lies with the Partner Agency.

Agencies may collect additional information beyond the minimum required data elements if the data is relevant to the purposes for which it is to be used.

DATA QUALITY

Data quality refers to the reliability and comprehensiveness of Client, Agency, and CoC-level data in HMIS. Components of data quality include:

- Timeliness
- Completeness
- Accuracy
- Consistency

WHY IS DATA QUALITY IMPORTANT? Regardless of whether an agency is federally funded, their HMIS data is included in the CoC's federal reports, including the System Performance Measures (SPM), Longitudinal System Analysis (LSA), and the annual Point-in-Time (PIT) Count and Housing Inventory Count (HIC). Poor data quality can impact a CoC's score in funding competitions.

Partner Agencies are responsible for the overall quality of data entered by their End Users. The goal is to record the most accurate, consistent, and timely information to draw reasonable conclusions about the extent of homelessness and the impact on the homeless service system.

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 people experiencing homelessness and the projects that serve them.

DATA TIMELINESS

Real-time data entry is ideal to ensure quality data entry.

Policy

Partner Agencies are required to enter all data into the HMIS within 72 hours of collecting it from the client.

DATA QUALITY PLAN

To ensure high-quality data, the HMIS Lead Agency, the CoC Board, Partner Agencies, and End Users will regularly and collectively assess and address the quality of data by examining characteristics such as timeliness, completeness, accuracy, and consistency.

Policy

Each Partner Agency must establish a data monitoring plan for their agency and their end users.

HARDWARE AND COMPUTER REQUIREMENTS

While the HMIS Lead Agency and the HMIS Vendor maintain the 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.

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

Partner Agencies must comply with the following hardware and software standards:

- A secure broadband internet must be used; Wi-Fi is acceptable if the connection is protected by a network security code.
- Computers must have an operating system compatible with the current HMIS software.
- Computers must have an internet browser compatible with current HMIS software.
  All devices utilized to access the HMIS must automatically lock after a short period of inactivity. This serves as a safeguard in the event of a licensed user leaving an unattended workstation unlocked when they are actively logged into HMIS.

Minimum Computer Requirements

- 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 has 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 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 is strongly advised.
- Processor: A Dual-Core processor is recommended.

PRIVACY REQUIREMENTS

All Partner Agencies must comply with the baseline privacy requirements in the 2004 HMIS Data and Technical Standards Final Notice with respect to: data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability.

HMIS CONSUMER NOTICE

The HMIS Consumer Notice informs clients that the Partner Agency participates in HMIS and that client information is shared with other HMIS Participating Agencies. Additionally, the Notice informs clients that the Agency's Privacy Notice is available upon request, as well as a list of HMIS Participating Agencies. A copy of the HMIS Consumer Notice and a list of HMIS Participating agencies is available on the Agency Resources page of the ICA Missouri website.

Policy

Partner Agencies must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting information and the availability of its privacy notice to any individual who requests a copy.

Partner Agencies that are recipients of federal financial assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and encounter the Partner Agency frequently.

HMIS Lead Procedure

- The HMIS Lead will confirm the Consumer Notice is posted at all intake areas during Technical Assistance Assessment monitoring.

HMIS PRIVACY AND SECURITY NOTICE

The HMIS Privacy and Security Notice describes a client's rights and permissible uses and disclosures of Protected Personal Information (PPI) collected by the Partner Agency. It is extremely important in the use of HMIS that client confidentiality, privacy, and security are maintained at the highest level.

Policy

A Partner Agency must provide a copy of the HMIS Privacy and Security Notice to any individual upon request. If the Partner Agency maintains a public website, the HMIS Privacy and Security Notice must be posted on the agency's website.

If the Partner Agency is a HIPAA covered entity, the Partner Agency is exempt from HMIS Privacy and Security Standards as HMIS Standards give precedence to the HIPAA Privacy and Security Rules.

Partner Agencies that are recipients of federal financial assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and encounter the Partner Agency frequently.

Agency Procedure

- The HMIS Privacy and Security Notice is a Word document located on the Agency Resources page of the ICA Missouri website. The Partner Agency's specific information (e.g., name of agency, address, contact information) will need to be inserted into the document.

1. Insert the Agency name in the document Header.

2. On page 3, insert the contact information of the person clients may contact to file a grievance.

3. On page 4, insert the URL where the Privacy Notice is located on the Agency's website.

- Agencies must require each member of their staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the HMIS Privacy and Security Notice and that pledges to comply with the HMIS Privacy and Security Notice.

HMIS Lead Procedure

- The HMIS Lead will review and collect a copy of the completed HMIS Privacy and Security Notice when onboarding a new Partner Agency.

- Additionally, the HMIS Lead will review the Privacy Notice and confirm it is published on the Partner Agency's website annually during HMIS monitoring.

CLIENT INFORMED CONSENT TO SHARE AND RELEASE OF INFORMATION (ROI)

By signing the HMIS Client Informed Consent to Share and Release of Information (ROI) form, the client gives the Partner Agency permission to share information specified in the ROI within HMIS. Additionally, the client's consent to share gives permission to share information for all household members.

Policy

Partner Agencies must obtain consent to share client information in HMIS **before** entering client information in HMIS. The ROI must be documented in HMIS. Partner Agencies are required to keep signed ROIs for a period of 7 years from the date of expiration. Release forms may be kept in a secure, hard copy file, scanned and uploaded to the Agency's electronic filing system, or scanned and uploaded to the client's file in HMIS.

Regardless of an agency's decision to terminate HMIS participation, the Partner Agency is required to keep Client Consent and Release of Information (ROI) forms for a period of 7 years from the date of expiration.

End User Procedure

- An HMIS ROI must be obtained by Agency staff and recorded in HMIS for each project in which the client is enrolled.

- Prior to entering client data in HMIS, review the ROI with the client. If the client agrees to share information, obtain a signed ROI.

- If the client declines to sign the HMIS ROI, Agency staff must contact the MoHMIS Helpdesk to request a locked record for all household members BEFORE entering information in HMIS.
- In cases where written consent is not possible, Agency staff should write "Verbal Consent" on the Client Signature line at the bottom of the ROI and date the form according to the date when verbal consent was given. The Agency and Personnel information should be completed as usual.
- HMIS ROIs expire one year from the date they are signed, then consent to share information must be obtained again. The start date of the new ROI must cover the period in which new information is being entered into the HMIS. That is to say:
    - A gap may exist between the end date of the expired ROI and the start date of the new ROI.
    - A new ROI does not need to be "backdated" to close a gap between ROIs if NO data is entered in HMIS during the time lapse between ROIs.
    - If the Agency needs to enter data that falls between ROIs, Agency staff must contact the MoHMIS Helpdesk BEFORE entering data into HMIS and wait for further instructions.
- Street Outreach projects have unique rules regarding HMIS ROIs and sharing information. If your Agency operates a Street Outreach project, please refer to the "HMIS ROI Need-to-Know for Street Outreach" article on the ICA Knowledge Base for details.

Due to the vast differences in Partner Agencies, it is at each Agency's discretion whether they require clients to sign one HMIS ROI for the Agency or an ROI for each project in which the client is enrolled. This will be dependent on an Agency's internal filing system and End Users should follow their Agency's internal procedure for obtaining a signed HMIS ROI.

HMIS Lead Procedure

- The HMIS Lead Agency will run reports to ensure ROIs are documented in HMIS. Additionally, the HMIS Lead Agency will audit client records during TAA site visits to ensure client files reflect what is recorded in HMIS.
- System Administrators will assist Agencies in determining best practice for collecting ROIs at the agency level versus project level based on the Participating Agency's needs.

SECURITY REQUIREMENTS

Security has 3 categories: System Security, Software Application Security, Hard Copy Security. Partner Agencies must apply system security provisions to all the systems where Protected Personal Information (PPI) is stored, including, but not limited to, the Agency's networks, desktops, laptops, mini-computers, mainframes and servers.

USERNAME AND PASSWORD

Partner Agencies must secure operating systems with, at a minimum, a user authentication system consisting of a username and a password. Additionally, Agencies must secure all electronic data.

- Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include but are not limited to:
  (1) Using at least one number and one letter.
  (2) Not using, or including, the username, the HMIS name, or the HMIS vendor's name.
  (3) Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time or be able to log on to the network at more than one location at a time.

VIRUS PROTECTION

Partner Agencies must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed.

FIREWALLS

Partner Agencies must protect HMIS systems from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall if there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall.

A workstation that accesses the Internet through a central server will not need a firewall if the server has a firewall.

PHYSICAL ACCESS TO SYSTEMS

Partner Agencies must staff computers stationed in public areas, that are used to collect and store HMIS data, at all times. When workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screensaver when the workstation is temporarily not in use. Password protected screensavers are a standard feature with

operating systems and the amount of time can be regulated. If agency staff are gone for an extended period, they should log off the data entry system and shut down the computer.

HARD COPY SECURITY

Partner Agencies must secure any paper or other hard copy containing Protected Personal Information (PPI) that is either generated by or for HMIS, including but not limited to, reports, data entry forms and signed consent forms.

Agencies must supervise any paper or other hard copy generated by or for HMIS that contains PPI when the hard copy is in a public area. When agency staff are not present, the information must be secured in areas that are not publicly accessible.

DATA RETENTION AND DISPOSAL

Partner Agencies must develop and implement a plan to dispose of, or alternatively, remove identifiers from Protected Personal Information (PPI) that is not in current use 7 years after the PPI was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention).

To delete all HMIS data from a data storage medium, Partner Agencies must reformat the storage medium. Agencies should reformat the storage medium more than once before reusing or disposing of the medium.

ELECTRONIC DATA TRANSMISSION

Protected Personal Information (i.e., name, date of birth, Social Security Number) should never be sent in an unencrypted email. This includes but is not limited to, Protected Personal Information (PPI) in attachments or in the name of attachments, PPI in the subject line of an email, PPI in the body of an email, etc.

End User Procedure

- When emailing an unencrypted email referencing client information, the email should only include the HMIS auto-generated Client ID.
- When emailing HMIS reports, Agency staff should review each tab of the report to ensure the report does not contain PPI.
- Before emailing a screen capture, Agency staff should ensure images do not include PPI. All PPI must be obscured before the image is electronically transmitted.
- When attaching documents to emails, Agency staff should confirm they are attaching the correct document and verify the contents of the attachment, and the name of the attachment does not contain PPI.
- When attaching scanned documents, Agency staff should verify redacted information was not made visible when the document was scanned.

BEST PRACTICES

Emails from Non-HMIS Agencies: If you receive an email containing PPI from an organization that does not participate in HMIS, it's imperative that the HMIS Participating agency does not reply or forward the communication unless all PPI is removed from the email. For best practice,

- Reply to the sender by creating a new email void of PPI.
- Respond by calling the sender and continuing the communication via phone.
- Removing and deleting PPI from an email thread is possible, however this can be laborious and lead to the HMIS Participating agency emailing PPI externally if it's overlooked in the previous email threads.

Internal Email Practices: When emailing client information internally, it is best practice not to include PPI in an email to avoid the information being forwarded outside your organization unintentionally. However, not all employees have access to HMIS, and it may be necessary to exchange PPI in an internal email when serving a client. In these situations, we offer the following best practices.

- Encrypt emails containing PPI when you need to send the communication to someone external to your organization.
- When email encryption is not available, start a new email instead of forwarding the existing internal communication to someone outside your organization.

Email on Mobile Devices: Client privacy is literally in the hands of employees when they have access to company email on a mobile device, so we offer the following best practices to partner agencies.

- Limit access to employees who have a need to respond to company emails from a mobile device.
- Ensure employee cell phones require biometric authentication (preferred) or pin number to access the device.
- Require employees to sign a mobile device agreement ensuring they are aware of security requirements and their responsibility to protect any client information that is accessible via the mobile device.
- If possible, issue a company phone to employees who need to access email on a mobile device to ensure security.
- Finally, ensure email access is promptly deactivated following an employee's termination.

DATA BREACH

The Agency shall maintain the security and confidentiality of the HMIS and is responsible for the actions of its End Users and for their training and supervision.

Policy

In the event of a breach of system security or client confidentiality, the Agency shall notify the MoHMIS Helpdesk within 24 hours of knowledge of such breach.

Any Agency that fails to email or call and/or is found to have had breaches of system security and/or client confidentiality shall enter a period of probation, during which technical assistance shall be provided to help the agency prevent further breaches.

Probation shall remain in effect until the HMIS Lead has evaluated the Agency's security and confidentiality measures and found them compliant with the policies stated in this Agreement and the User Policy and Responsibility Agreement. Subsequent violations of system security may result in suspension from the system.

REVOKING END USER ACCESS

In the event an employee is no longer authorized to have HMIS access, due to a change in employment or job duty, an Authorized Representative of the Agency must notify the HMIS Lead Agency so access can be revoked.

Policy

The Agency will notify the MoHMIS Helpdesk as soon as possible but no later than three (3) business days when an End User is no longer an employee, or does not require access to the HMIS, so the issued User ID and password can be made inactive. The Agency may notify the MoHMIS Helpdesk in advance if a registered User is transferring positions or leaving the Agency.

Agency Procedure

- A designated Authorized Representative for the Agency may submit the User Access Request form to revoke an End User's HMIS access or email the MoHMIS Helpdesk.

END USER REQUIREMENTS

The HMIS Lead is responsible for ensuring the HMIS implementation is an effective tool for preventing and ending homelessness within the CoC.

As such, it is the responsibility of the HMIS Lead Agency to ensure all participants in the HMIS implementation have sufficient and adequate training to make effective use of the HMIS.

Policy

Partner Agencies and End Users are required to demonstrate their knowledge of all information shared through ICA's various communication channels including, but not limited to, HMIS User Meetings, HMIS Newsletters, and Knowledge Base. This information is designed to ensure the security of the HMIS database, the security and confidentiality of client data, and to stay current with any modification to HMIS policies, procedures, and guidelines.

HMIS USER ACCESS

Prior to allowing any individual to access the HMIS, ICA shall require the receipt of a valid User Access Request form, a User Policy and Responsibility Agreement, and documentation of necessary training.

Policy

For security purposes, the User Access Request form must be submitted by a Designated Authorized Representatives of the Agency. The Agency will only request HMIS user access for paid employees, supervised volunteers or interns who need access to the HMIS for legitimate business purposes. The Agency will limit the access of such employees, volunteers and interns to only those records and projects required for work assignments.

Agency Procedure

- A Designated Authorized Representative of the Agency must submit the User Access Request form to request HMIS access for a new user.

HMIS Lead Procedure

- The HMIS Manager assigned to the Agency's CoC will review all requests to add a new End User to determine if it should be approved or denied.

NEW USER TRAINING

If the user access request is approved, the Agency's assigned HMIS System Administrator will initiate the new user training. HMIS login credentials for the live database will not be issued to any individual who has not completed the minimum required training.

If a User Access Request form is submitted for a user who previously had access to the Missouri HMIS, the End User will be required to complete the training series again.

USER POLICY AND RESPONSIBILITY AGREEMENT

To ensure compliance with HMIS Policies and Procedures manual, the Agency Partner Agreement, and Privacy and Security Standards, HUD requires HMIS Lead's to execute an HMIS End User Agreement, hereinafter referred to as the User Policy and Responsibility Agreement, with all HMIS End Users. The Agreement outlines End User responsibilities and expectations.

End User Procedure

- New users must read the User Policy and Responsibility Agreement, placing a check next to each policy, and sign the Agreement.

SECURITY AND PRIVACY AWARENESS TRAINING

To ensure compliance with HUD Security and Privacy Standards, all End Users must complete the Security and Privacy Training.

End User Procedure

- Watch the pre-recorded Security and Privacy Awareness video and complete the associated test with a passing score.

HMIS DATA STANDARDS TRAINING

The HMIS Data Standards training is designed to train End Users on the details of HUD's Universal Data Elements and Program Specific Data Elements as defined in the current HMIS Data Standards Manual.

End User Procedure

- Watch the pre-recorded Data Standards Training video and complete the associated test with a passing score. In addition to the training video, HMIS End Users are provided a link to HUD's HMIS Data Standards Manual and are encouraged not only to use it to complete their training, but also to save the link for future reference.

COMMUNITY SERVICES® BASICS TRAINING

The Community Services® Basics training is an introduction to navigating the CoC's designated HMIS software, Community Services®.

End User Procedure

- Watch the pre-recorded demonstration of Community Services® and complete the associated test with a passing score.

HMIS PRACTICE CASE TRAINING

All new users must watch pre-recorded HMIS training videos and complete at least one practice case specific to the programs and projects for which they will enter data.

End User Procedure

- End Users will be given access to ICA's HMIS Training Site, along with a practice case (i.e., test client intake forms). After watching the pre-recorded training video, the new user will use the HMIS Training Site to simulate the steps demonstrated in the training video.

- In most cases, the HMIS practice cases are completed in 3 consecutive segments (Project Entry, Update, Project Exit). End Users will work on one segment at a time.

- Upon completing the Entry, Update, or Exit segment, the End User will notify the MoHMIS Helpdesk so their work can be reviewed in the training site.

HMIS Lead Procedure

- The MoHMIS Helpdesk will review end user practice cases to determine if any corrections are needed. If any errors are identified, Helpdesk will inform the user so they can make the necessary corrections.
- Once corrections have been completed, Helpdesk will send the next part of the practice case.

The HMIS Lead Agency may determine that an End User failed to grasp the necessary data entry concepts based on the quality of the user's practice cases and use their discretion to require the End User to repeat the new-user training.

If a new user fails to successfully complete the practice cases after a minimum of three attempts, and after receiving one-one-one training from ICA staff, the HMIS Lead reserves the right to refuse HMIS access if it has been determined that the End User is not capable of accurate and complete data entry. CoCs may develop additional local policies to guide this decision.

ANNUAL RECERTIFICATION AND OTHER TRAINING

Recertification is the process whereby HMIS End Users complete refresher training to maintain their access to HMIS. All End Users are required to complete the User Policy and Responsibilities Agreement, Security and Privacy Awareness training, and HMIS Data Standards training at the start of a new HUD Fiscal Year to maintain HMIS access.

Modifications to HMIS Access
Additional practice case training may be required, should a current End User's HMIS access change to include data entry for a program or project type in which they haven't previously been trained.

CLIENT RIGHTS

A comprehensive description of client rights can be found in the Privacy and Security Notice and Client Consent to Share and Release of Information (ROI).

RIGHT TO INFORMATION

Partner Agencies must allow an individual to inspect and to have a copy of any Protected Personal Information (PPI) about the individual. Agencies must offer to explain any information that the individual may not understand. Additionally, Partner Agencies must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual. Agencies are not required to remove any information but may, as an alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

Policy

The Agency must assist a client with viewing their HMIS record within 5 business days of the client submitting a written request.

Agency Procedure

- Upon written request, the Agency must provide the client with a copy of their Protected Personal Information within 5 business days. End Users can use the Print icons in HMIS to print Personal Protected Information in the client's HMIS record.

RIGHT TO DECLINE CONSENT TO SHARE

Clients have the right to decline their consent to share information within HMIS. Declining to share does not prohibit the client's right to the provision of services.

Clients have the right to revoke their consent to share information at any time. If a client revokes their authorization, the Partner Agency should immediately notify the HMIS Lead Agency. All information entered in the HMIS about the household will not be shared with Partner Agencies from that date forward.

RIGHT TO REFUSE TO ANSWER CERTAIN QUESTIONS

Clients have the right to refuse to answer certain questions. Some programs are required to collect specific information to verify a client is eligible for the program's services. Partner Agencies may decline services if they are not provided with information needed to determine client eligibility.

THE RIGHT TO FILE A GRIEVANCE

Clients have the right to file a grievance concerning the Agency's privacy and security policy and practices, including if they feel their right to confidentiality has been violated, if they have been denied access to their personal records, or if they have been put at personal risk, or harmed. Clients have the right to file a grievance without consequence.

Policy

Partner Agencies must establish a procedure for accepting and considering questions or complaints about their privacy and security policies and practices. Agencies must include a contact person and contact information of the Agency staff clients should contact to file a grievance.

TECHNICAL ASSISTANCE ASSESSMENT (HMIS MONITORING)

ICA shall conduct a minimum of one Technical Assistance Assessment (TAA) with each Partner Agency each year. This Technical Assistance Assessment may be completed on-site or remotely at the discretion of ICA. The TAAs will be conducted to determine if the Partner Agency requires additional technical assistance to be in compliance with the Agency Partner Agreement, the HMIS Policies and Procedures Manual, and any CoC-specific requirements.

HMIS Lead Procedure

- The Partner Agency will be given a minimum of two weeks' notice of the date and time of the monitoring.
- Following the TAA monitoring, ICA shall issue a letter stating whether the Agency was found to be compliant within 10 business days of conducting the TAA.
- Letters regarding compliance will be sent to the Agency Director, all designated authorized representatives, designated contacts, any funders who mandate HMIS participation, and the appropriate HMIS Advisory Committee(s).

- If found out of compliance, Partner Agencies will have 30 days to become compliant. The CoC and all funders will be notified if a Partner Agency is out of compliance, as well as when the out-of-compliance Partner Agency has taken the appropriate steps to regain a compliant status. Failure to correct the non-compliant issues can lead to closed access to HMIS and possible funding risks.
- Letters regarding non-compliance shall specify if the Agency as a whole was determined to be out of compliance, or if specific project(s) have been determined to be out of compliance. If only specific projects have been deemed to be out of compliance, the letter shall explicitly state that only those projects have been found out of compliance.

COMPLIANCE AND SANCTIONS

Any User or Partner Agency found to be out of compliance with any HMIS operational policy or procedure found in the HMIS Policy and Procedure Manual, the MoHMIS User Policy and Responsibilities form, and the Agency Partner Agreement will be subject to immediate access revocation pending a formal review by the HMIS Lead Agency of the violation.

Repercussions for any violation will be assessed in a tiered manner as described below. Each End User or Partner Agency violation will face successive consequences.

Violations do not need to be of the same type in order to be considered second or third violations. User violations do not expire and are tied to the individual.

This means that historical violations will follow the User in the event they transfer to another HMIS Participating Agency or have access to the HMIS for more than one participating Agency at a time. 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.

- **First violation**. The End User and Partner Agency shall be notified of the violation in writing by the HMIS Lead Agency. The End User's license will be suspended until the Agency has notified the HMIS Lead of actions taken to remedy the violation. The HMIS Lead Agency will provide necessary training to the User and/or Partner Agency to ensure the violation does not continue or reoccur. The HMIS Lead Agency will notify the applicable CoC Board Committee(s) of the violation and actions taken to remedy the violation at the next scheduled advisory committee meeting.
- **Second violation**. The End User and Partner Agency will be notified of the violation in writing by the HMIS Lead Agency. The End User's license will be suspended for 30 days. The End 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 suspension, the suspension will continue until the Agency notifies the HMIS Lead Agency of the action(s) taken to remedy the violation. The HMIS Lead will notify the applicable CoC Board Committee(s) of the violation and actions taken to remedy the violation at the next scheduled advisory committee meeting.

- **Third violation**. The End User and Partner Agency will be notified of the violation in writing by the HMIS Lead Agency. The HMIS Lead will convene a review panel made up of CoC Board Committee members who will determine if an End User's license should be terminated. The End User's license will be suspended for a minimum of 30 days, or until the CoC Board committee(s) notifies the HMIS Lead Agency of their determination, whichever occurs later. If the advisory committee determines the User should retain their license, the HMIS Lead Agency will provide necessary training to the End User and/or Agency to ensure the violation does not continue or recur.
- **Fourth and consecutive violations**. If the End User is allowed to regain access after the third violation, any violations after the third will be handled in the same manner as a third violation.
- **Violations of local, state, or federal law**. Any violation of local, state, or federal law by an End User or the Agency will immediately be subject to the consequences listed under the third violation above.

The HMIS Lead Agency may rule a Partner Agency out of compliance at any time if the Agency is found to be out of compliance with the terms of the Agency Partner Agreement, the HMIS Policies and Procedures Manual, or other HMIS-related regulations or requirements established by HUD or other project funders. The HMIS Lead Agency may also choose to conduct additional TAAs with the Agency each year if there is reason to believe the Agency is out of compliance.

The HMIS Lead Agency may issue notification of required data cleanup or catch-up to an Agency or project. The notification of required data cleanup or catch-up will include a timeframe by which the data cleanup or catch-up must be complete. The HMIS Lead Agency shall determine the timeframe based upon the amount of data cleanup or catch-up required and the capacity of the Agency to complete the data cleanup or catch-up. If the Agency does not complete the cleanup or catch-up within the designated timeframe, the HMIS Lead will issue a letter of non-compliance. At this point, the Agency shall have 30 days to complete the data cleanup or catch-up before project funders and the HMIS Advisory Committee are notified.

DATA REQUEST POLICY

All custom data and report requests must be submitted to the HMIS Lead via the Custom Data Request Form available on the ICA Missouri website. The HMIS Lead Agency will review the custom data request and, using the criteria outlined below, determine whether CoC Approval is required. When CoC approval is required, the HMIS Lead will submit the completed Custom Data Request form through the appropriate channels to determine the course of action.

Data Requests not requiring CoC Approval:

- An agency requests data on clients served by their own project, regardless of level of aggregation. Agencies cannot provide identifying client level data pulled directly from the HMIS to any outside entity.
- An agency requests CoC level data.

- A funder requests a project level data on agencies they fund
- A funder requests CoC level data on all projects in their CoC
- A CoC committee requests project or CoC level data

Data Requests requiring CoC Approval:

- Any request, other than an agency requesting their own data, involving personally identifiable client information
- An agency requests data that includes clients served by any project outside of their agency, when requested at project or agency level.
- A funder requests client level data whether identifying information is or is not included.
- A funder requests project level data on a project they do not fund whether identifying information is or is not included
- A CoC committee requests client level data
- Any request from an agency or entity outside of the CoC

PRIORITIZING REPORTS

The HMIS Lead Agency's prioritization process involves assessing the type of request, the regions the request benefits, the primary purpose of the request (i.e., does the report/data primarily serve to house individuals, assess data quality, assist with funding, etc.), the type of requestor, and the time required to complete the request.

Please note that we cannot meet all report requests. Due to limited reporting capacity, we will prioritize requests that benefit multiple participants, such as statewide or CoC-wide datasets.

REPORT TIMEFRAMES

Report delivery times will vary depending on priority requests, mandated reporting cycles, and other outstanding projects.

HMIS Lead Procedure

- Based on the current report queue, the HMIS Lead Agency will make an estimate of when they can begin working on the request. Based on the nature and complexity of the report, the time it will take to fulfill requests can range between 2 weeks (e.g., a simple bug notification) and 10 weeks (e.g., a large-scale project) to fulfill. After prioritization, the HMIS Lead will send an expected delivery date.

For all requests, the more notice you can give, the better. Please note that September-March is the reporting team's busiest time of year.

APPENDIX

HUD RESOURCES

Resource Name & Link	Intended Audience	Contents
HMIS Data Standards Manual	Continuums of Care Participating Agencies HMIS End-users HMIS Lead Agencies	Provides an overview of all the Universal Data Elements and Program Descriptor Data Elements. Contains information on data collection requirements, instructions for data collection, and descriptions that the HMIS User will find as a reference.
2004 HMIS Data and Technical Standards Final Notice	Continuums of Care HMIS Lead Agencies	The Final Notice sets forth the HMIS data standards and privacy and security standards for data confidentiality. It describes the statutory authority that allows HUD to prescribe HMIS data and technical standards.
Client-Centered Data Collection Approach: Virtual Reality Series	Continuums of Care Participating Agencies Anyone collecting sensitive and personal information	A virtual reality training experience that provides a first-person view into trauma-informed approaches to data collection.
Client-Centered Data Collection resources	Continuums of Care HMIS Lead Agencies Participating Agencies Anyone collecting sensitive and personal information	HUD has published various resources on taking a client-centered approach in data collection
HUD Limited English Proficiency Recipient Guidance	Continuums of Care Participating Agencies	Provides guidance to federal financial assistance recipients regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient (LEP) Persons.

ICA RESOURCES

Resource Name & Link	Intended Audience	Contents
ICA Missouri Home Page	Public	Data Dashboards Information on joining HMIS Training Calendar
Agency/User Access Forms	Participating Agencies Authorized Representatives HMIS End Users	User Access Request form Privacy and Security Notice Consent to Share and Release of Information (ROI) HMIS Consumer Notice List of HMIS Providers
Custom Data Request Form	Continuums of Care Participating Agencies HMIS Lead Staff	Custom Data Request form HMIS Lead Agency process details
ICA Missouri Knowledge Base	Participating Agencies HMIS End Users	HMIS tip sheets and guides Data collection forms
ReportCollection	Continuums of Care Partner Agencies End Users	A searchable library of all ICA Missouri custom reports in BusinessObjects.