BALANCE OF STATE SPRINGFIELD/JOPLIN

Homeless Management Information System
Policies and Procedures

Updated & Approved by BoS Board 9.2019

mohmis@icalliances.org

CONTENTS

INTRODUCTION

A Homeless Management Information System (HMIS) is a web-based software system that is used by homeless and human services organizations across Missouri to record and store client-level information about the numbers, characteristics and needs of homeless persons and those at risk of homelessness. ServicePoint® is the software solution that has been chosen by the Continuum of Care; Institute for Community Alliances is the HMIS Lead Agency that administers the system and manages user and agency licensing, training, and compliance.

HMIS enables service providers to measure the effectiveness of their interventions and facilitate longitudinal analysis of service needs and gaps within the Continuum of Care (COC). Information that is gathered from consumers by service providers is aggregated (void of any identifying client level information) and made available to policy makers, service providers, advocates, and consumer representatives. Data aggregated from HMIS about the extent and nature of homelessness and poverty in the state of Missouri is used to inform public policy decisions aimed at addressing and ending homelessness at local, state and federal levels. Any agency that provides shelter, housing, and services to individuals experiencing homelessness and those at risk of homelessness qualifies to participate in HMIS.

Guidance for the implementation of Missouri's HMIS is provided by a broad-based advisory board that is committed to understanding the gaps in the system of series intended to end homelessness.

This document provides the policies, procedures, guidelines and standards that govern HMIS operations, as well as the responsibilities for partner agencies and end users. It is extremely important in the use of HMIS that client confidentiality, privacy, and security are maintained at the highest level. The policies and procedures in this document fulfill basic Department of Housing and Urban Development (HUD) and HMIS requirements.

INSTITUTE FOR COMMUNITY ALLIANCES (ICA)

ICA serves as the HMIS Lead Agency for five CoCs in Missouri, including: Balance of State, Joplin, Springfield, St. Louis City, and St. Louis County. The policies outlined in this manual pertain specifically to the continua of Balance of State, Springfield and Joplin. 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 "Lead Agency" or "HMIS Lead Agency".

CONTACT INFORMATION

HMIS Lead Agency: 1123 East Broadway Blvd. Sedalia, MO 65301

Missouri's HMIS website may be used as a resource for obtaining the most up-to-date information: www.icalliances.org/missouri

HMIS Help Desk: mohmis@icalliances.org

SYSTEM ADMINISTRATORS

The Lead Agency's System Administrators provide frontline technical support to HMIS users, facilitate supplemental trainings and HMIS user meetings, and are responsible for setting up projects and new users in ServicePoint®. They also conduct Technical Assistance Assessment site visits and desk monitoring for partner agencies.

HMIS System Administrators make every attempt to respond to all requests in a timely manner; however, System Administrators travel frequently, so you may not always receive an immediate response to a direct request. For the quickest response, please contact our helpdesk at mohmis@icalliances.org between the hours of 8:00 a.m. to 5:00 p.m., Monday through Friday, excluding most national holidays.

SERVICEPOINT®

ServicePoint® is the HMIS database system used by the Balance of State, Springfield, and Joplin continua.

HMIS BENEFITS

Use of HMIS provides numerous benefits for service providers, homeless persons, and the State of Missouri.

Benefits for service providers:

- Provides online, real-time information about client needs and the services available for homeless persons.
- Assures confidentiality by providing information in a secured 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 services for homeless persons are needed the most.

- Allows agencies to better evaluate the effectiveness of specific interventions and programs,

Benefits for homeless persons:

- Intake information and needs assessments are maintained historically, reducing the number of times homeless persons must repeat their stories to multiple service providers.
- The need to provide intake and life history only one time demonstrates that service providers consider the homeless person's time valuable and restores some of the consumer's dignity.
- Multiple services can be easily coordinated, and referrals can be streamlined.

PARTICIPATING ENTITIES

Regardless of funding source, entities which may 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 for persons who are homeless
- Emergency Shelters serving homeless adults, families and youth[1]
- Transitional Housing programs
- Rapid Re-housing programs
- Supportive Housing programs (whether scatted 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:

HUD

- CoC
- Emergency Solutions Grant (ESG)
- Housing for Persons with AIDS (HOPWA)[2]

Department of Health and Human Services (HHS)

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

Department of Veterans Affairs (VA)

- Supportive Services for Veteran Families (SSVF)

On the state level, the Missouri Housing Development Commission require HMIS participation for their grantees under the following programs:

- Emergency Solutions Grant Program (ESG)[3]

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

FEDERAL HMIS POLICES

In addition to the Balance of State, Springfield/Joplin HMIS Policies and Procedures contained herein, each CoC within the Missouri Implementation must also comply with federal HMIS requirements. These requirements are detailed in a suite of HMIS Data Standard resources, an overview[4] 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. 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 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.

PARTNER AGENCY REQUIREMENTS

Partner Agencies are all agencies that participate in HMIS, enter data and obtain reports from the HMIS system. All partner agencies must agree to and abide by HMIS policies and procedures. Partner Agencies must complete the following documents which are accessible on the ICA website.

AGENCY PARTNER AGREEMENT

In order to obtain and maintain access to the HMIS, Partner Agencies must complete and adhere to the Agency Partner Agreement, a legal agreement between the Partner Agency and the Lead Agency 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.

Procedure:

- The Agency Partner Agreement must be completed by the Partner agency's Executive Director (or equivalent) before the Partner Agency is provided with access to the database, and it must be renewed again each year. The Lead Agency will retain the electrically signed agreements.

Questions regarding the Agency Partner Agreement should be submitted to ICA's Missouri Director, Sandy Wilson, at sandy.wilson@icalliances.org.

TERMINATION OF PARTICIPATION

Reasons for a Partner Agency's voluntary termination of participation include, but are not limited to, the following:

- The Partner Agency is no longer running the project(s) for which they were entering data into HMIS.
- The Partner Agency is no longer being mandated to enter data into HMIS by one of their funders and chooses to no longer participate in HMIS.

Procedure:

- The Partner Agency will inform the Lead Agency in writing 30-days prior to their intention to terminate their agreement to participate in HMIS.
- The Partner Agency will make sure all data in the HMIS database is current and accurate and that all data corrections needed have been completed. The Partner Agency will also run all reports needed prior to termination. If a need for reports from HMIS should arise after termination, the Partner Agency may contact the Lead Agency. The Partner Agency is required to keep copies of release forms (ROI) signed by clients for a period of seven years from the date of expiration. Release forms may be kept in a secure, hardcopy file or may be scanned and uploaded to the ROI tab within the HMIS.

HMIS PRIVACY AND SECURITY NOTICE

The HMIS Privacy and Security Notice describes in detail the client's rights regarding HMIS and how information is kept secure.

Procedure:

- The HMIS Privacy and Security Notice is a word document (located on the ICA website) in which the HMIS Partner Agency's specific information will need to be inserted (i.e., name of agency, address, contact information).
- Insert the name of the HMIS Partner Agency into the Header.
- Insert the HMIS Partner Agency's contact information for which the client may contact to file a complaint
- Insert the HMIS Partner Agency's website information
- The completed HMIS Privacy and Security Notice will be collected during the Partner Agency enrollment.
- The Privacy and Security Notice must be made available to clients upon request.
- If an agency serves clients whose first language is not English, the agency must be able to provide a translated version of the HMIS Privacy and Security Notice or interpretation services.
- 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, according to section 4.1.2 of the HUD Data and Technical Standards.

HMIS CONSUMER NOTICE

The HMIS Consumer Notice notifies the client that the Partner Agency participates in HMIS and that some client information entered in the HMIS is shared with other Partner Agencies. The HMIS Consumer Notice requires that a list of those Partner Agencies be provided for clients to review. The HMIS Consumer Notice directs clients to the Client Informed Consent to Share and Release of Information form.

Procedure:

- The HMIS Consumer Notice must be posted in locations visible to all clients.
- If a Partner Agency serves clients whose first language is not English, the agency must provide a translated version of the HMIS Consumer Notice or interpretation services.

CLIENT INFORMED CONSENT TO SHARE AND RELEASE OF INFORMATION

By signing the Client Informed Consent to Share and Release of Information form, hereinafter referred to as the ROI, the client understands that any information shared with a Partner Agency participating in HMIS is kept confidential and that only those authorized to input data into HMIS can view their personal, identifying information; all health information, however, will not be shared. The client has the right to refuse to answer certain questions. The sharing of information does not guarantee that services will be provided. Declining to share information does not prohibit the provision of services. If the client revokes authorization, all information regarding that household entered into the database from that date forward will not be shared with other Partner Agencies.

Procedure:

- Prior to entering client data into HMIS, review the ROI with the client. If the client agrees to share information, obtain a signed ROI.
- If the client refuses to sign the HMIS ROI, contact the Helpdesk to lock the client's record.
- The agency must obtain an ROI and record in HMIS. Agencies are required to keep copies of release forms signed by clients for a period of seven years from the date of expiration. Release forms may be kept in a secure, hardcopy file or may be scanned and uploaded to the ROI tab within the HMIS.
- A new ROI must be signed yearly for active clients.
- HMIS ROIs need to be obtained for each project a client is enrolled in and recorded into HMIS.

CLIENT RIGHTS

THE RIGHT TO INFORMATION

Clients have the right to a copy of their Universal and Project-specific data contained within HMIS.

Procedure:

- Client submits a written request for a copy of their information contained within HMIS to the Partner Agency.
- Partner Agencies are required to provide the Client a printed copy of the Client Status Report from HMIS.
    - The information in this report is based on the last update in HMIS and includes:
        - Basic demographics
        - Housing status
        - Employment and education information
        - Household members
        - Contact information
        - Residence history
        - Monthly Income
        - Non-cash benefits
        - Expenses

- Goals
- Various Notes
- Service records
- Project information

THE RIGHT TO FILE A GRIEVANCE

Clients have the right to file a grievance regarding potential violations of their privacy rights regarding HMIS participation. Negative actions will not be taken against a client for filing a grievance.

Procedure:

- Partner Agencies must establish a contact person and contact information that is included on the Privacy and Security Notice.

HMIS DATA REQUIREMENTS

All Partner Agencies participating in HMIS collect a standard set of client information, established under the 2014 HMIS Data Standards, known as the Universal Data Elements. Within each CoC there are additional program-specific data elements that are required to produce the necessary CoC-level aggregate reports.

The standard set of data elements collected in HMIS is referred to as the Core Data Elements. Agencies are responsible for knowing all the Universal and Program-specific data elements. These data elements can be found at HUD Exchange.

Accurate data collection is important for the coordination of services across multiple agencies, determining eligibility for Client services, and generating reports from ServicePoint®. Guidelines articulating the minimum expectations for data entry for all programs entering data in HMIS, are posted on Institute for Community Alliances' Missouri HMIS webpage under forms.

Procedure:

- HMIS Partner Agencies and HMIS Users will collect all Core Data Elements and any Project-specific data elements as required by their project type. HMIS Users are required to ensure data quality of the information they collect and enter in HMIS, as stated in the HMIS User Policy and Responsibilities Agreement. This is accomplished by reviewing the data the Client has provided for accuracy and completeness and correcting any identified data quality issues.

HMIS TECHNICAL STANDARDS

The HMIS Lead Agency and HMIS Vendor are equally responsible for all technical standards determined by HUD. HUD has established that all HMIS software must be able to:

- Produce unduplicated client records
- Collect all data elements set forth by HUD
- Report outputs
- Produce compliance reports for HMIS Lead Agencies and their Partner Agencies to assess achievements towards established benchmarks
- Generate standardized audit reports

HARDWARE AND COMPUTER REQUIREMENTS

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

The equipment used to connect to the HMIS system 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 system according to their own organizational needs.

PROTECTED AGENCIES AND DOMESTIC VIOLENCE AGENCIES

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

Domestic violence agencies are prohibited from entering data into an HMIS database. If a domestic violence agency receives CoC or ESG funding, they are required to have a comparable database, and the HMIS Lead Agency will work with the Agency to ensure the database meets standards. For reporting purposes, domestic violence agencies are required to report aggregate data.

SHELTER POINT IN TIME COUNT

HUD requires that all CoC complete a Sheltered Point-in-Time count. The HMIS Project and its staff collect the required data on homeless individuals currently in Emergency Shelter, Transitional Housing, or being temporarily housed in a hotel or motel by an agency. Agencies enrolled in HMIS will have the data they have submitted via survey cross-referenced with their data in HMIS. If there are inconstancies, the agency will be contacted and asked to correct the inaccurate data entries.

HMIS PARTICIPATION LETTERS

Partner Agencies may request HMIS participation letters from their HMIS system administrator. This letter may be submitted with the Partner Agency's application for funding for various funding sources. HMIS participation letters will be provided for those agencies that are:

- Domestic violence agencies that have provided aggregate level data during the last two Point-in-Time counts
- Currently enrolled Partner Agencies in compliance
- Currently enrolled Partner Agencies not in compliance
- New Agencies that have started the HMIS enrollment process

DATA RETENTION AND DISPOSAL

For records stored within HMIS, HUD requires that data be retained for seven years after the data was created or last changed, as indicated in the 2004 HMIS Data & Technical Standards.

Other obligations (federal, state, local, or contractual requirements) may necessitate retention past HUD's seven year threshold.

DATA MONITORING

Partner Agencies are responsible for the overall quality, accuracy, and completeness of data entered by their staff.

The HMIS Lead Agency conducts an annual Technical Assistance Assessment (TAA) visit with each Partner Agency and its HMIS Users. The Partner Agency will be given two week notice of the date and time of the visit. The TAA visit determines if the Partner Agency is meeting HMIS requirements as defined in the Agency Partner Agreement, HMIS User Policy and Responsibilities Agreement, HUD, and other federal partners. The TAA visit also serves to identify areas where the Partner Agency requires additional technical assistance to bring the agency into compliance with all data and security standards. In addition, these TAA visits allow HMIS Users to provide feedback and receive assistance with software issues.

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 completed 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.

The Lead Agency also completes an annual desk monitoring on all projects entered in HMIS for data quality and will send a report of findings to each Partner Agency.

TRAINING REQUIREMENTS

DESIGNATING A NEW HMIS USER

Individuals working for or on behalf of an Agency (employee, contractor, volunteer, etc.), that need access to HMIS, must be designated as an HMIS User by the Partner Agency's authorized representative.

HMIS NEW USER TRAINING

Procedures:

- The Partner Agency's Authorized Representative will complete and submit the User Access Request form.
- The Lead Agency Project Manager assigned to the Partner Agency's CoC will review the request to determine if it should be approved or denied.
- All Users must sign the User Policy and Responsibilities form and are required to complete all new-user trainings with the Lead Agency prior to receiving access to the system. If the Lead Agency determines that data entered by a current End User does not meet minimum data quality standards, the End User may be required to complete the training again.

- All Users must watch the Security and Privacy Awareness video and pass the Security and Privacy Awareness test.
- All users must watch the Data Standards video and pass the Data Standards test.
- All new Users must view interactive ServicePoint® training videos specific to their Agency's funding type and complete funding-specific, data entry practice cases.
- Once a new User begins the HMIS new user training series, the User has 14 days to complete the training series and all required assignments. The Lead Agency's system administrators will review the User's practice cases to determine if any corrections are needed.
- If the user fails to complete all requirements within 14 days, including corrections, the User will be required to start the training series from the beginning.
- The Lead Agency may determine that a new User failed to grasp the necessary data entry concepts based on the quality of the user's homework and may use their discretion to require new Users to repeat the new-user training.
- If a new User fails to successfully complete the homework requirements for data entry after repeated attempts, the Lead Agency reserves the right to refuse HMIS access to a new User if it has been determined that the User is not capable of accurate and complete data entry.
- If a User Access Request form is submitted for a new User that previously had access to the Missouri HMIS, the User will be required to complete the training series again.

ONGOING USER TRAINING REQUIREMENTS

- All Users are required to complete annual security training to retain their user license.
- HMIS User Meetings are held quarterly and serve as an opportunity for HMIS Users to come together and share ideas, troubleshoot problems, and address HMIS policy concerns. All Partner Agencies are required to have at least one HMIS user attend 75% of these meetings.

DATA SECURITY

The Lead Agency 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.

DATA BREACH

In the event of a breach of system security or Client confidentiality, the Agency shall notify the ICA Missouri Helpdesk within 24 hours of knowledge of such breach (mohmis@icalliances.org or 314-655-4780, ext. 8). 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 Responsibilities form. Subsequent violations of system security may result in suspension from the system.

DISASTER RECOVERY PLAN

Missouri's HMIS is covered under Wellsky's 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).

HMIS USER PASSWORD REQUIREMENTS

- Creation: Passwords are automatically generated from the system when a User is created. The System Administrator will communicate the system-generated password to the User.

- Use: The User will be required to change the password the first time they login to the system. The password must be:
    - A minimum of 8 characters with at two special characters.
    - Passwords should not be easily guessed or found in a dictionary.
    - Passwords are the individual's responsibility and Users cannot share passwords. Users may not keep written copies of their password in a publicly accessible location.
- Storage: 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 login.
- Expiration: Passwords expire every 45 days. Users may not use the same password consecutively. Passwords cannot be re-used until two password selections have expired.
- Unsuccessful login: If a User has three unsuccessful login attempts, the User account will be "locked" and permission to access HMIS will be revoked until the User's password is reset. To have a password reset, email the Lead Agency's System Administrator at mohmis@icalliances.org or use the reset password feature in ServicePoint.

REMOVING HMIS USERS

PARTNER AGENCY NOTIFICATION

In the event an employee is no longer authorized to have access to HMIS, due to a change in employment or job duty, the Partner Agency must send written notification identifying any HMIS User needing access removed to their HMIS System Administrator within three working days.

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.

MINIMUM DATA COLLECTION STANDARDS

All Partner Agencies are responsible for asking all clients a minimum set of questions, or data elements. 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. Lead Agency staff will consult with the Partner Agency 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.

DATA QUALITY PLAN

To ensure high-quality data, the Lead Agency, the CoC board, Partner Agencies, and users will regularly and collectively assess and address the quality of data by examining characteristics such as timeliness, completeness, and accuracy. Each Partner Agency must establish a data monitoring plan for their agency and their users.

DATA TIMELINESS

Real time data entry is ideal to ensure quality data entry. All data is required to be entered into HMIS within 72 hours of collecting the data from the client.

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.

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 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 User and Partner Agency shall be notified of the violation in writing by ICA. The User's license will be suspended until the Agency has notified ICA of actions taken to remedy the violation. ICA will provide necessary training to the User and/or Partner Agency to ensure the violation does not continue or reoccur. ICA 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 User and Partner Agency will be notified of the violation in writing by ICA. 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 suspension, the suspension will continue until the Agency notifies ICA of the action(s) taken to remedy the violation. ICA 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 User and Partner Agency will be notified of the violation in writing by ICA. ICA will convene a review panel made up of CoC Board Committee members who will determine if a User's license should be terminated. The User's license will be suspended for a minimum of 30 days, or until the CoC Board committee(s) notifies ICA of their determination, whichever occurs later. If the advisory committee determines the User should retain their license, ICA will provide necessary training to the User and/or Agency to ensure the violation does not continue or reoccur.
- **Fourth and consecutive violations**. If the 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 a User or the Agency will immediately be subject to the consequences listed under the third violation above.

ICA shall conduct a minimum of two TAAs with each Partner Agency each year, and at least one of the TAAs each year will be conducted on site at the Agency. TAAs will be conducted to determine if the Agency requires additional technical assistance in order to be in compliance with the Agency Partner Agreement, the HMIS Policies and Procedures Manual, and any CoC-specific requirements. ICA shall issue a letter stating that the Agency is or is not in compliance within five business days of conducting the TAA and shall distribute the letter as noted below.

- If the Agency is determined to be out of compliance, the letter will contain the steps required for the Agency to come into compliance and the timeframe in which the Agency must come into compliance. If the Agency does not come into compliance within the designated

timeframe, ICA will write another letter explaining that the Agency has not taken the steps prescribed to come into compliance and shall distribute the letter as noted below.

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

ICA 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. ICA 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, ICA 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.

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.

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 CoC Board Committee(s).

1 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.
2 Only competitively funded HOPWA projects serving homeless individuals are required to use the HMIS. HOPWA block grants are not required to use the HMIS.
3 The Missouri Housing Development Commission 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.
4 Source: HMIS Data Dictionary, June 2017, Version 1.2.