Homeless Management Information System (HMIS)
Policies and Procedures

CoC KS-505 and MO-604
Greater Kansas City Area

HMIS Lead Agency
Mid-America Regional Council

Adopted by HMIS Lead Agency Governing Board
July 17, 2017

HMIS Policies and Procedures

Overview

1.1. Purpose of HMIS

The McKinney-Vento Homeless Assistance Act, as amended by the Homeless Emergency Assistance and Rapid Transition to Housing Act of 2009 (HEARTH), requires that the U.S. Department of Housing and Urban Development (HUD) ensure operation of community-wide Homeless Management Information Systems (HMIS) with consistent participation by recipients and sub-recipients of applicable federal grants. The HMIS has many uses, including:

- Collecting unduplicated counts of individuals and families experiencing homelessness;
- Analyzing patterns of use of assistance provided in a community; and,
- Providing information to project sponsors and applicants for needs analyses and funding allocations.

Additionally, HMIS is essential to coordinate services, evaluate performance, ensure accountability in the use of public funds, and inform public policy. Ultimately, the HMIS serves as the foundation for all planning to prevent, reduce, and eliminate homelessness.

The two Continuum of Care organizations, Greater Kansas City Coalition to End Homelessness and United Community Services of Johnson County, entered into a formal agreement with the Mid-America Regional Council (MARC) to serve as the HMIS Lead Agency. The HMIS Lead Agency role is to administer the local HMIS to ensure that it meets the needs of local agencies, the two CoCs and the community at-large. The HMIS Lead Agency must develop written policies and procedures for all HMIS participating agencies using the system, execute participation agreements with each of these agencies and their system users, and monitor and enforce compliance by all participating agencies with the requirements set out in the participation agreement. The HMIS Lead Agency is responsible for maintaining the *HMIS Policies and Procedures* manual and all related documents, training system users, and providing technical assistance.

The HMIS software vendor selected by the HMIS Governing Board for the two CoCs is CaseWorthy, Inc. The HMIS system is referred to as “CaseWorthy” in operational manuals.

1.2. Key Terms

1. Continuum of Care: a community-based collaborative that oversees homeless system planning and coordination, including the HMIS implementation.

2. HMIS Lead Agency: the organization that administers and operates the HMIS.

3. Participating Agency: any agency that contributes data or uses the HMIS.

4. Exempt Agency: any agency that is explicitly exempt from entering data into the HMIS by federal regulations. This includes victim services providers.

5. Client: a person who receives services at an HMIS participating agency.

6. Personally Identifiable Information (PII). Defined in OMB M-07-16 as "...information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

1.3. Data Ownership

Policy: The participating agency retains rights over all information it enters into the HMIS. The participating agency has the right to use and modify information entered into the HMIS. The participating agency has the right to download its client information, ensuring the protection of the security of the client data as outlined in Section 4.11. If a participating agency decides to terminate its use of the HMIS, the client data will be maintained in the HMIS as outlined in Section 3.7 regarding Participation Termination.

Procedures:

1. The participating agency entering client information will secure authorization from the client to enter the personal data into the HMIS, and to allow for sharing of the information with other agencies using the HMIS.
2. If a participating agency downloads client data into another electronic system or prints the information in hard copy, the agency will ensure the privacy and security of the client data consistent with Section 4.11.
3. In the event that MARC is no longer the administrator of the HMIS, the HMIS Governing Board will select a new HMIS Lead Agency and transfer the custodianship of the data within the HMIS to another organization for continuing administration. In such event, participating agencies will be informed in a timely manner.

1.4. Voluntary Participation

The HMIS Governing Board, on behalf of the two CoCs, encourages agencies that serve persons who are homeless or at risk of homelessness and are not required to participate in the HMIS to do so voluntarily.

Having more service providers in the HMIS creates the potential for:

- More effectively coordinating client services through case management and referral information sharing;
- More accurate tracking of client returns to the homelessness prevention and assistance system;
- More accurate counts of homeless persons and system resources, which could be used to understand the gaps in the service system;
- Better information about community-wide needs, which can help guide advocacy efforts, policymaking, and funding allocations; and

- Better information about system outcomes, which can be used to guide service targeting and performance improvement efforts.

For these reasons, the HMIS Lead Agency will actively work to recruit service providers to participate in the HMIS.

1.5. HMIS Documentation Amendment Process

Policies:

- The HMIS Lead Agency and HMIS Governing Board will guide the amendment of *HMIS Policies and Procedures* and related policies and forms.
- The HMIS Governing Board will approve the *HMIS Policies and Procedures* and *Data Quality Plan*.

Procedures:

1. Once the HMIS Policies and Procedures and Data Quality Plan are approved by the HMIS Governing Board, the two CoC boards will be asked to review and accept the policy documents.
2. Proposed changes may be offered from any participant in HMIS, including clients.
3. Proposed changes may be identified by the HMIS Project Manager to comply with HUD or another regulatory agency's requirements.
4. Proposed changes will be reviewed by the HMIS Project Manager.
5. Proposed changes will be discussed by the HMIS Governing Board at a regularly scheduled meeting. The board will take action it deems appropriate on whether or not to make changes to the HMIS policies and procedures.
6. Once changes are approved by the HMIS Governing Board, they will be shared with the two CoC boards for their review and acceptance. Changes will be sent to all HMIS participating agencies.
7. Each of the participating agencies will receive a copy of any changes to the revised *HMIS Policies and Procedures* (or other documents) and will be asked to confirm receipt of the changes by email to the HMIS Project Manager. The agency will also be asked to circulate the revised policies and procedures within their agency to staff and volunteers using the HMIS System.
8. Trainings on changes to HMIS documentation will be scheduled as needed.

2. Stakeholder Responsibilities

2.1. HMIS Governing Board

1. Select an HMIS Software for the two CoCs and secure their concurrence.
2. Approve and maintain *HMIS Policies and Procedures*.
3. Approve and maintain the *Data Quality Plan*.
4. Evaluate performance of the HMIS Software.
5. Oversee the work of the HMIS Lead Agency
6. Establish a budget and set fees for use of the HMIS system.

7. Perform other duties as outlined in the Memorandum of Agreement between the two Continuum of Care organizations and the Mid-America Regional Council for operation of the HMIS Lead Agency role.

2.2. HMIS Lead Agency

1. MARC is responsible for the administration of the HMIS system in support of agencies serving clients in the three-county area
2. MARC will assign sufficient staffing (and/or contractors) to provide HMIS support services to participating agencies.
3. MARC will establish an HMIS Help Desk, enabling participating agencies and system users to receive professional technical assistance.

2.2.1. HMIS Lead Agency staffing support will include:

1. Oversee the collection, analysis and presentation of HMIS data for reporting to federal, state, and local governments, and other appropriate parties.
2. Oversee HUD HMIS grant application and reporting process.
3. Oversee the overall administration of the HMIS software.
4. Oversee HMIS help desk and designate staff responsible to manage, coordinate and support its operation.
5. Maintain documents and ensure compliance with HUD HMIS Data and Technical Standards and *HMIS Policies and Procedures*.
6. Serve as the HMIS Security Officer.
7. Serve as point of contact on HMIS Data Standards compliance, staying abreast of any changes.
8. Engage with new and current participating agencies to identify business needs; identifying opportunities for customization within the HMIS application.
9. Work with HMIS Governing Board to devise and monitor quality benchmarks.
10. Complete site visits at participating agencies to monitor compliance with *HMIS Policies and Procedures*.
11. Provide technical guidance on HMIS implementation to participating agencies.
12. Maintain contact with HMIS software vendor to ensure optimal performance.
13. Ensure the HMIS database is secure and not over capacity
14. Identify problematic areas and conduct research to determine the best course of action to correct the data.
15. Analyze and solve issues with current and planned systems as they relate to the information and management of client data.
16. Analyze reports of data duplicates or other errors to provide ongoing appropriate interdepartmental communication and monthly or daily data reports.
17. Work with participating agencies to maintain accurate Housing Inventory Count within HMIS.
18. Assist in defining specifications for updates to data elements in the HMIS.
19. Assist participation agencies with performance evaluation activities.
20. Provide technical assistance and training to system users to ensure optimal use of the HMIS system to meet program needs.

21. Activate and disable user accounts as needed.
22. Develop custom reports in the HMIS.
23. Oversee customizations made by program-level system administrators.
24. Maintain a log of client requests to review their data.
25. Support agencies and the two Continuum of Care organizations to define work flows as new policies are implemented, including coordinated entry.

2.2.2. HMIS Security Officer

1. Conduct annual security reviews of participating agencies.
2. Conduct annual security trainings for system users.
3. Assist in developing the *HMIS Security Plan*.
4. Document reports of suspected violations client privacy or data security policies, participating agency responses, and HMIS Lead response, and work with affected agencies as necessary to address suspected violations of client privacy and data security policies.

2.3. Participating Agency

2.3.1. Agency Executive Director/Program Director/Designee

1. Sign the *Agency Participation Agreement* and submit it to the HMIS Manager.
2. Ensure agency compliance with the terms and conditions of the *Agency Participation Agreement* and *HMIS Policies and Procedures.*
3. Ensure personnel with access to the HMIS comply with the terms and conditions of the *System Confidentiality and Use Agreement*.
4. Designate one employee as the agency's HMIS Representative to serve as the primary point-of-contact on HMIS operations at the agency. This point-of-contact may also be designated as a "super-user". A "super-user" is a designated person who is trained on the HMIS and is comfortable training others, both within their organization, and possibly, at other agencies.
5. Designate one employee as the agency's HMIS Security Officer and notify the HMIS Security Officer of this assignment.
6. Support the HMIS Leads effort to resolve HMIS data quality and compliance issues.

2.3.2. Agency HMIS Representative

1. Ensure compliance with HMIS data collection, data entry and reporting requirements as outlined the *HMIS Policies and Procedures*.
2. Serve as primary point-of-contact for communication between the agency and HMIS Lead on HMIS operations.
3. Provide support on resolution of any data quality and reporting issues.
4. Identify agency personnel to access the system and receive HMIS training.
5. Sign *System Confidentiality and User Agreements* to authorize access.
6. Notify the HMIS help desk within 24 hours of relevant personnel changes to ensure system user accounts are deactivated.

2.3.3. Agency HMIS Security Officer

1. Ensure compliance with the privacy and security standards as outlined in the *HMIS Policies and Procedures*.
2. Ensure compliance with the agency-specific data security policies and procedures.
3. Document and investigate suspected violations of client privacy or data security policies.
4. Notify HMIS Security Officer within 24 hours of receiving reports of suspected violations of client privacy and data security policies.
5. Notify HMIS Security Officer of the agency's response to suspected violations of client privacy and data security policies.

2.3.4. System User

1. Sign the *System Confidentiality and User Agreement*.
2. Submit a copy to the HMIS Security Officer
3. Deliver the original to the agency HMIS Representative for record keeping.
4. Complete HMIS training and meet training objectives.
5. Comply with all HMIS agreements, policies and procedures.
6. Report suspected violations of client privacy and data security policies to the agency HMIS Security Officer.
7. Provide feedback to the HMIS Lead Agency on their satisfaction in use of the system.

3. Operational Policies and Procedures

3.1. Hardware, Software, and Network Requirements

Policy: The participating agency is responsible for meeting the minimum hardware, software, and network requirements to access the HMIS, and for providing the necessary maintenance for continued participation.

CaseWorthy is a web-based application that can be accessed from any desktop computer (PC or Mac). CaseWorthy does work on some mobile devices. Participating agencies are encouraged to keep systems updated for optimal functionality. .

Policies:

- The participating agency is responsible for identifying personnel for system training and access.
- Agencies will define the roles for system users within their organization based on the work they do and the agencies' programmatic needs.
- The participating agency will designate new users and identify their roles, providing access by assigning a user name and password.
- The participating agency will notify MARC of any need to change "roles".
- The participating agency may change the role of users and deactivate non-active users.

- The participating agency will notify MARC if they deactivate system users within 24 hours of termination of their service with the agency.

Procedures (To Designate a New System User):

1. The participating agency's designated HMIS Representative may set up a new user at any time. If help is needed, a participating agency could make a request to the HMIS help desk to set up a new user, specifying the new user's name, email address, role and a description of HMIS-related job functions.
2. The new system user will complete the *System Confidentiality and Use Agreement*.
3. The participating agency will inform the HMIS help desk if training is needed, and the HMIS help desk will coordinate new user training.

Procedures (To Change User Role)

1. The participating agency's HMIS Representative will change the user's role and send a confirmation email to the user and copy the HMIS help desk.

Procedures (To Deactivate a System User):

1. The participating agency's HMIS Representative will deactivate users when necessary and inform the HMIS help desk.

3.2. Data Collection

Policies:

- The participating agency is responsible for understanding its HMIS compliance requirements as may be defined by various federal grant programs and funders, and fulfilling any contractual obligations, including but not limited to compliance reports.
- The participating agency is responsible for communicating these requirements to the HMIS Lead Agency to ensure the system is properly configured to collect required data.
- The participating agency is required to collect and enter information into the HMIS as defined in the federal HMIS Data Standards Manual, specifically the Universal Data Elements (UDEs) and the Program Specific Data Elements (PDEs): https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf
- The HMIS Lead Agency will post information about HMIS on MARC HMIS support website.
- The HMIS Lead Agency will provide training and technical assistance on UDEs.

3.3. Data Transfer

Policies:

- The participating agency is permitted to export a copy of their client data from HMIS to another system.
- The participating agency is responsible for adhering to federal, state and local privacy laws within their databases, if it transfers any client data outside of HMIS.

Procedures:

- The participating agency can request training from the HMIS Lead regarding the downloading of client data by submitting a request to the HMIS help desk.

- The HMIS help desk will coordinate this training with the agencies.

3.4. Training

Policies:

- All new users are required to complete HMIS system use and security awareness training before being allowed access to the system.
- All active users are required to complete annual training on security awareness.
- All active users are required to participate in training on any updates to the system, policies or procedures, as needed.
- All users are required to sign the *System Confidentiality and User Agreement*, acknowledging receipt of a copy of the privacy notice (see Section 5) and pledging to comply with the privacy notice and additional terms and conditions for HMIS access.

Procedures:

1. Only authorized agency personnel may request new user training.
2. Optional and required trainings will be announced via email.

3.5. Technical Assistance

Policies:

- The participating agency may request HMIS technical assistance from the HMIS Lead Agency.
- Technical assistance will be focused on the implementation and operation of HMIS for those authorized uses as defined in these *HMIS Policies and Procedures*.

Procedure:

Requests for technical assistance can be submitted, Monday through Friday, 8:00am to 5:00pm, or through the online support ticket.

3.6 Participation Termination

Policies:

In the event of termination of the HMIS Partnership Agreement, all data entered into the HMIS will remain an active part of the HMIS and the records will retain their original security settings.

Procedures:

- HUD-funded agencies in KS-505 and MO-604 are required to participate in the HMIS or a comparable database as a condition of their funding. For those that decide to terminate their contract with the Mid-America Regional Council for the HMIS, this will be addressed in the context of the larger Agency Grant Agreement by MARC. For those participating agencies that are non-HUD-funded, the person signing the initiating HMIS Partnership Agreement will notify MARC with a date of termination in writing. In all cases of termination of the HMIS Partnership Agreement, the System Administrator will deactivate all users from the agency on the date of termination stated by the agency. All client-level data entered into the HMIS will remain an active part of the HMIS and the records will retain their original security settings.

- MARC will terminate the HMIS Partnership Agreement for noncompliance with the terms of the agreement if the participating agency does not abide by the required privacy and security policies and procedures.
- HUD-funded agencies that work with the homeless are required to participate in the HMIS. For those that are terminated, MARC will notify the person that signed the initiating HMIS Partnership Agreement or that person's successor, with a date of termination in writing. MARC will give thirty (30) days written notice to the agency, regardless of funding source, to the attention of the person who initiated the agreement or their successor. MARC requires any HMIS violations to be rectified before the HMIS Partnership Agreement termination is final. MARC may also terminate the HMIS Partnership Agreement without cause upon thirty (30) days written notice to the participating agency.
- In all cases of termination of the HMIS Partnership Agreement, MARC will notify the System Administrator to make inactive all users from the agency on the date of termination. All client-level data entered into the HMIS will remain an active part of the HMIS, and the records will retain their original security settings.

3.7 Adding or Changing Programs or Projects in HMIS

Policies:
Adding a New Project in HMIS by Participating Agency Policy: A number of MARC staff and local agency personnel have been trained as System Administrators. These System Administrators have the ability to add or change agency and project information. The participating agency's HMIS will notify MARC thirty (30) days prior to implementation of a new project.

Procedure:
- At least thirty (30) days prior to anticipated implementation date, participating agency's HMIS will communicate with the HMIS System Manager on changes required.
-
- Changes to Existing Projects in HMIS Policy: The Executive Director or his/her designee will notify MARC of programmatic changes. If the addition of programs or projects requires a change in fees charged to the agency, MARC will inform the agency prior to any changes being implemented.

- The Executive Director or his/her designee will notify MARC of any applicable programmatic changes to existing programs which may have an effect on data collection, data entry, data quality or data reporting at least forty-five (45) business days prior to the implementation date of the change. Recommendations and timelines for the changes will be returned to the participating agency no more than ten (10) business days from receipt date of request. The System Administrator will complete changes at least seven (7) business days prior to the implementation date for final approval from the participating agency.

3.8 Additional Customization Policy

Policies:
The participating agency will be solely responsible for additional database customization costs. This includes the voluntary transfer of existing grant client-level data and custom build reports beyond that of the System Administrator's scope of work.

Procedure:

- The Agency Administrator or Executive Director will notify MARC of any applicable programmatic customization which may have an effect on data collection, data entry, data quality, or data reporting at least forty (40) business days prior to the implementation date of the change. Proposed customization and/or changes must be submitted in writing.
- If support from CaseWorthy is necessary to make the changes, MARC and/or the System Administrator will communicate to CaseWorthy the needs and scope of work for the participating agency. Recommendations and timelines for the changes will be returned to the participating agency, including a Statement of Work from CaseWorthy, if applicable. The System Administrator will complete changes and seek review and final approval from the participating agency. If a participating agency voluntarily transfers an existing grant to another agency, MARC will not pay for client-level data to be transferred. The agency requesting the transfer will be liable for additional CaseWorthy fees.

4. Security Policies

4.1. Purpose

- These security policies are directed to ensure the confidentiality, integrity, and availability of all HMIS information; protect against any reasonably anticipated threats or hazards to security; and ensure compliance by end users.

4.2. System Applicability

- The participating agency and HMIS Lead, including any authorized agents, must follow the security policies established in this section.

4.3. Security Management and Compliance, and Annual Review

- The HMIS Lead is responsible for managing the selection, development, implementation, and maintenance of security measures to protect HMIS information.
- The HMIS Lead must retain copies of all contracts and agreements executed as part of the administration and management of the HMIS or otherwise required.
- The HMIS Lead must complete an annual security review to ensure the implementation of the security requirements for itself and the participating agency, using a checklist to ensure compliance with each requirement defined in this section.

4.4. Disaster Recovery

- The HMIS Lead must develop a disaster recovery plan that includes protocols for communication with stakeholders described in Section 2.
- The HMIS Lead has contracted with a vendor, CaseWorthy, to host the HMIS database server. The vendor will implement technical safeguards to prevent data loss in the event of a disaster. In such an event, the vendor will contact the HMIS Lead and provide a timeline for recovery. The HMIS Lead will communicate the timeline with stakeholders, include instruction to guide operations during the recovery process, and provide periodic updates as well as notification upon successful recovery of any data loss.

4.5. Security Officers

- The participating agency and HMIS Lead will each designate an agency representative to serve as HMIS Security Officer to be responsible for compliance with applicable security policies (see Stakeholder Responsibilities).
- The agency representative must be able to pass a criminal background check in order to serve as HMIS Security Officer.

4.6. Security Awareness Training

- The HMIS Lead will ensure that all system users receive security training before being given access to the system and at least annually thereafter. The HMIS Lead will maintain attendance records for all training events to assure compliance. Information on a participating agency's users completing the security training will be shared with the agency executive or program director.

4.7. Data Security

- The participating agency and HMIS Lead will ensure that devices used to access the HMIS are password protected with automatic system lock after no more than 60 minutes of user inactivity. If participating agencies have more stringent internal policies, those policies will take precedence.
- The participating agency and HMIS Lead must ensure that computers used to access the HMIS have virus protection that is updated automatically.
- The participating agency and HMIS Lead must ensure that internet connections used to access the HMIS from their facilities are set up using network security protocols to prevent unauthorized access to the network and to HMIS data saved locally.

4.8. System Passwords

- The HMIS Lead will provide new system users a temporary password to initially access the system and create their own password.
- Every 90 days the HMIS will prompt system users to change their password.
- System users must not share their password, even among other authorized HMIS users.

- System users must not allow their Internet browser to save their HMIS password.
- System users must not store their password in locations that are easily accessible to others (i.e. under the computer keyboard or posted near the workstation).
- System users will use complex passwords consisting of upper and lowercase letters, numbers 0-9, and special characters !@#$%^&*().
- System users that attempt access more than four times unsuccessfully will need to contact their participating agency's HMIS Representative to reset their password and regain access.

4.9. System Access Physical Location

- Due to the confidential nature of data stored within HMIS, the system must be accessed from a sufficiently private physical location so as to ensure that persons who are not authorized users of the HMIS are not able to view client level data.

4.10. User Inactivity

- User accounts that have not been accessed for 90 or more days will be automatically disabled by the participating agency's HMIS Representative, meaning the user will be unable to access the system.
- For accounts inactive for more than 180 days, the HMIS Representative may submit a refresher request to the HMIS help desk. These re-authorized users must attend and complete refresher training prior to reactivating their account.

4.11. Personally Identifiable Information (PII) Storage and Management

- System users are responsible for maintaining the security of all client data extracted from the HMIS and any data collected for purposes of entry into the HMIS.

4.11.1. Electronic Data Storage and Management

- System users may only store HMIS data containing PII on devices owned by their agency.
- System users may not store HMIS data containing PII on hard drives or removable media that can be accessed by non-system users.
- System users are responsible for safeguarding HMIS PII that users store on agency-owned devices.
- Electronic transmission of HMIS data containing PII will be limited to secure direct connections or, if transmitted over the internet, the data will be encrypted using a 128-bit key or transmitted using password protected files.
- The participating agency and HMIS Lead are responsible for developing additional policies and procedures for protecting electronic data from theft, loss, or unauthorized access.
- Before disposing of hard drives, USB drives, or other portable electronic media used to store PII, the participating agency will consult with their agency HMIS Security Officer.

4.11.2. Hard Copy Data Storage and Management

- Hard copies of HMIS data containing PII shall be kept in individual locked files or in rooms that are locked when not in use.
- When in use, hard copies of HMIS data containing PII shall be maintained in such a manner as to prevent exposure of PII to anyone other than the system user(s) directly utilizing the information.
- Employees shall not remove hard copies of HMIS data containing PII from their agency's facilities without permission from appropriate supervisory staff unless the employee is performing a regular work function which requires the use of such records outside of the facility.
- Faxes or other printed documents containing PII shall not be left unattended.
- Before disposing of hard copies of HMIS data containing PII, they must be shredded.
- The participating agency is responsible for developing additional policies and procedures for protecting hard copies of HMIS data containing PII from theft, loss, or unauthorized access.

4.12. Security Incidents

- The HMIS Lead must implement a policy and chain of communication for reporting and responding to security incidents.
- The participating agency and HMIS Lead will post the *Privacy Notice* anywhere HMIS data is collected or accessed that articulates the reporting mechanism for suspected breaches of client confidentiality. The notice will include contact information for the agency's HMIS Security Officer. The notice will include additional instructions for reporting anonymously.
- The participating agency and HMIS Lead will maintain records of all security incidents, responses and outcomes.

4.13. Security Policy Complaints

- Complaints related to HMIS security policies and procedures will be considered using the same procedures for amending HMIS Documentation (see Section 1.5).

5. Privacy Policies

5.1. Purpose

- These privacy policies are meant to establish limitations on the collection, purpose, and use of data. It defines allowable uses and disclosures, including standards for openness, access, correction, and accountability. The policies provide protections for victims of domestic violence, dating violence, sexual assault, and stalking.

5.2. Privacy Notice

- The HMIS Lead will post a copy of the *Privacy Notice* on the HMIS support website and will provide a copy of this document to any individual upon request.

- The participating agency must post a copy of the *Privacy Notice* at each workstation where client data is gathered and entered.
- The participating agency must also post a Spanish translation of the *Privacy Notice*, if it serves Spanish-speaking clients.
- Outreach workers inform clients about the *Privacy Notice* and provide a copy, if requested (including a copy of the Spanish translation, if applicable).
- The participating agency will post the *Privacy Notice* to its website, if one exists.
- The participating agency must state in the *Privacy Notice* that these privacy policies may be amended at any time and that amendments may affect information obtained by the agency before the date of the change.
- The participating agency should include in the *Privacy Notice* the contact information for their agency HMIS Security Officer for purposes of seeking additional information or submitting complaints.
- The participating agency must provide a copy of these *Privacy Policies* to anyone who requests it.

5.3. Purpose and Use Limitations

- The participating agency and HMIS Lead may only collect and use HMIS data for the specific internal purposes as defined in this section. Every agency with access to Personally Identifiable Information (PII) must implement procedures to ensure and monitor its compliance with privacy policies and may only collect information by lawful and fair means with the knowledge and consent of the individual.

Authorized Uses of HMIS Data:

- To provide or coordinate services;
- To locate programs that may be able to assist clients;
- To produce agency-level reports regarding use of services;
- To track agency-level, CoC system-level and regional outcomes;
- For agency operational purposes, including administrative functions such as legal, audits, personnel, oversight, and management functions;
- To comply with government and other funding agency reporting requirements;
- To identify service needs in our community;
- To support CoC system-level planning;
- To conduct research for government and educational purposes approved by the HMIS Lead Agency;
- To monitor compliance with *HMIS Policies and Procedures*; and,
- To accomplish any and all other purposes deemed necessary by the HMIS Governing Board.

5.4. Interagency Data Sharing

- All client information entered in HMIS by the participating agency is shared with the agency's system users and with the HMIS Lead.

- With client consent, all client information is shared with system users at other participating agencies for authorized uses.
- The participating agency's Executive Director/Program Director (or equivalent) is responsible for their agency's compliance with the Interagency Data Sharing policies.

5.5 Client Consent

Policies:

- The participating agency may infer client consent to collect and enter information into HMIS from any person who seeks or receives assistance from the agency.
- All information entered into HMIS is shared between the agency's system users and with MARC as the HMIS Lead Agency, based on this *inferred client consent* model.
- In order to share information with other participating agencies, the agency must seek and obtain *informed client consent* using the *Client Release of Information* (ROI) form.
- When clients consent to share information, system users at other participating agencies will have access to the client's record and case history for authorized uses.
- Informed client consent is valid until such time as the client revokes consent.
- Clients who have consented to share information with other participating agencies may revoke consent in writing at any time. This revocation may impact other agencies' access to the client record and data they have entered into the system.
- The participating agency must securely store physical copies of client consent documentation.

Procedures (Initial Consent):

1. Personnel from the participating agency will notify the client that the information they collect will be entered into the HMIS and will explain the purposes for collecting information in the HMIS.
2. At this time, personnel from the participating agency will explain the Release of Information form, and the clients' right to revoke data sharing in writing at any time.
3. For families, an adult client can provide consent on behalf of household members by listing them in the spaces provided on the form and initialing in front of each family member's name. Additionally, the participating agency may seek consent separately from each individual in the household. A legal guardian (or another adult, if a guardian is not present) may sign on behalf of minors in the household.
4. The client will be provided the ROI form for review, will be explained its content, and will be asked to complete it.
5. The client must sign the ROI form as proof that they had an opportunity to review the form and have their questions answered.
6. If the client signs the form and agrees to share information with all participating agencies, agency personnel must indicate their response in the HMIS.
7. If the client declines to share information with all participating agencies, agency personnel must ensure client indicates decision on the ROI, provide a copy to the HMIS Security Officer and maintain a copy with client's documentation.
8. A copy of all completed consent forms will be kept in the client's paper file. These forms may be reviewed by the *HMIS Security Officer* during security reviews.

9. Participating agencies are encouraged to review client demographic or household data in the HMIS system with the client on at least an annual basis and update as necessary.

Procedures (Revocation of Consent):

1. If a client presents a written request to revoke consent for information sharing in the HMIS, agency personnel must store the written request in the client's file, and must indicate their response in the HMIS.
2. If a client verbally requests to revoke consent for data sharing, agency personnel must ask the client to complete the ROI form and follow the process specified in (1) above.
3. A copy of all written ROI requests must be included in the client's paper file and uploaded in the individual's HMIS documents.

Procedure (Renewal of Consent):

If a client consents to share information after previously denying consent, agency personnel must follow the same procedures that were specified above involving the completion of the initial consent form.

5.6 Access and Correction

- The participating agency must allow a client to inspect and to have a copy of any PII about the client, and offer to explain information that the client may not understand.
- The participating agency must consider any request by a client for correction of inaccurate or incomplete PII pertaining to that client. A participating agency is not required to remove any information but may, alternatively, mark information as inaccurate or incomplete and supplement it with additional information such as an indicator of data quality.

5.7 Other Authorized Data Disclosures

- Client data may be transmitted to reporting systems as mandated by agency funders.
- Other disclosures of client data to persons and organizations not authorized to view the information in the HMIS requires the client's written consent, unless the disclosure is required by law.
- Aggregated data that does not specifically identify any individual client or include PII may be shared with internal and external agents without specific permission.

5.8 Accountability and Privacy Policy Complaints

- Complaints related to HMIS privacy policies and procedures will be considered using the same procedures for amending HMIS Documentation (described in Section 1.5).
- The participating agency must require each member of its staff to sign the *System Confidentiality and Use Agreement* that acknowledges receipt of a copy of the *Privacy Notice* and that pledges to comply with the privacy policies and procedures.

6. Quality Assurance Policies

6.1 Purpose

The purpose of quality assurance policies is to ensure reliable and useable data, establish expectations for participating agencies, and define quality standards.

6.2 Policies

The HMIS Lead Agency will

- Develop a *Data Quality Plan* to assist participating agencies in maintaining and monitoring data quality.
- Define benchmarks and establish policies and procedures to monitor for compliance, including an enforcement mechanism for non-compliance.
- Require the participating agency to adhere to policies and procedures that ensure data meets standards for coverage, timeliness, completeness, accuracy, and consistency.
- Review the plan annually and update as needed.

6.3 Standards

6.3.1 Coverage

The HMIS Lead Agency seeks 100% participation in HMIS from all eligible homeless service providers and agencies within the two CoC's geographic area, with a 60% minimum benchmark for both lodging (residential) and non-lodging (service-only) projects.

6.3.2 Timeliness

The participating agency is required to enter data into HMIS within 2 business days of client interview or interaction resulting in data collection, with the exception of outreach projects that must enter data within 3 business days.

6.3.3 Completeness

The participating agency is required to collect and enter data on 100% of those clients in participating projects.

6.3.4 Accuracy

The participating agency is required to accurately represent in HMIS the information collected from clients and avoid entering misleading or knowingly false information. To accurately represent client information, the agency must follow data collection procedures.

6.3.5 Consistency

The participating agency must ensure personnel only use authorized data collection and entry procedures consistent with individual programmatic requirements.

CASEWORTHY INFORMATION SHARING SYSTEM
Agency Partner Agreement
MO-604 and KS-505

The Caseworthy Information Sharing System (hereinafter "CW") is a client information system that provides a standardized assessment of consumer needs, allows for individualized service plans and records the use of housing and services. The CW system meets HUD standards as a Homelessness Management Information System (HMIS). The two Continua of Care can use this information to determine the utilization of services of participating agencies, identifying gaps in the local service continuum and developing outcome measurements.

The Mid-America Regional Council (MARC) is the Lead Agency and Administrator for the Caseworthy system serving the two Continua. In this Agency Partner Agreement (hereinafter "Agreement"), "Client" is a consumer of services; "Agency" is the Agency named in this Agreement; "CW Agency Compliance Monitor" is the designated CW representative of the Agency, and "Partner Agencies" are all the Agencies participating in the CW system.

The Agency Director must indicate agreement with the terms set forth below by signing this Agreement before a CW account can be established for the Agency.

Confidentiality

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

    a. The Agency shall abide by all local, state and federal confidentiality laws and regulations pertaining to: a) all medical conditions, including mental illness, alcohol and/or drug abuse, HIV/AIDS diagnosis and other such covered conditions; and b) a person's status as a victim of domestic violence. A general authorization for the release of medical or other information is NOT sufficient for this purpose.

    b. Federal, state and local laws seek to protect the privacy of persons with physical and/or mental illness, who have been treated for alcohol and/or substance abuse, have been diagnosed with HIV/AIDS, and/or have been a victim of domestic violence. The Agency is encouraged to seek its own legal advice in the event that a non-partner agency requests identifying confidential client information.

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

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

4. The Agency agrees to notify the MARC Lead Agency Program Manager within one working day when the Agency receives a request from an individual or an organization for client identifying information to be printed out of the CW system.

5. The Agency shall ensure that all staff, volunteers and other persons who are allowed access to the CW system receive Client confidentiality and new user training and have signed a User Policy and Responsibility Statement prior to receiving a User ID and Password.

6. The Agency shall notify MARC Lead Agency Program Manager within 3 working days when a registered user is no longer an employee or has moved to a position with different responsibilities so the issued user ID and password can be nullified.

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

8. In the event of a breach of system security or Client confidentiality, the CW Agency Compliance Monitor shall notify the MARC Program Manager at 816-701-8294 within 24 hours of knowledge of such breach. Any Agency that 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 Program Manager has evaluated the Agency's security and confidentiality measures and found them to be compliant with the policies stated in this Agreement and the User Policy Responsibility Statement and Code of Ethics Agreement. Subsequent violations of system security may result in suspension from the system.

9. The Agency understands CaseWorthy servers are located in a ViaWest data center. ViaWest is one of the world's leading SAS-70 Type II data center operators. The CaseWorthy architecture utilizes a Data Access and Security Component layer through which all transactions and data passing in and out of the database must flow. This layer ensures that data is always contained within a comprehensive security- and privacy-protected environment. In addition, the software contains 128-bit AES Encryption, advanced authentication option exceeding National Institute of Standards and Technology (NIST) standards, and the application runs 100% in browser with no ActiveX controls or 3rd party plugins.

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

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

12. The Agency shall post the "Consumer Notice" sign at each intake desk (or comparable location). The Agency shall provide each Client with the "CW summary of Privacy Notice" and make available upon request the "CW Full Privacy and Security Notice." If the Agency maintains a public web page, the Agency shall post the current version of the "CW Full Privacy and Security Notice" on the web page.

13. If the Agency is governed by the Health Insurance Portability and Accountability Act (HIPAA), and determines that a substantial portion of its Protected Personal Information about homeless Clients or homeless individuals is protected health information as defined in the HIPAA rules, the Agency shall disregard paragraph "L" **except** the Agency shall post the "Consumer Notice." An Agency determined to be HIPAA compliant will provide an attestation of this to MARC, as well as a copy of their privacy notice. In addition, a HIPAA compliant organization will sign a Business Associate Agreement with the MARC on an annual basis. A HIPAA compliant organization will follow HIPAA rules.

14. The Agency shall require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

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

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

    1. Domestic violence;
    2. Sexual violence;
    3. HIV/AIDS;
    4. Alcohol and/or substance abuse;
    5. Mental health; or
    6. Unaccompanied Youth

16. The agency shall take steps to identify any special needs (i.e. listed above) and provide appropriate resources and/or referrals available to the Client.

17. Each Agency that is a user shall have access to identifying and statistical data that the Agency inputs into the CW database for Clients served by that Agency.

18. The CW database is intended as a shared database. Unless an Agency that is a user determines that certain client information should not be shared with others within their Agency or with other Agencies, all data in the CW database, including identifying and statistical data input into the CW database for Clients, will be available to qualified system users.

CW Use, Data Entry and System Security

1. The Agency shall follow, comply with and enforce the User Policy and Responsibility Statement. Modifications to the User Policy and Responsibility Statement shall be established in consultation with Partner Agencies and may be modified as needed for the purpose of the smooth and efficient operation of the CW system.

2. The Agency shall begin data entry within no more than 30 days of enrollment or notify MARC if there are extenuating circumstances

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

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

5. The Agency shall consistently enter information into the CW database and shall strive for real-time, or close to real-time data entry. "Close to real-time data entry" is defined as within 3 working days of seeing the Client.

6. When a Client revokes his or her consent to share information in the CW database, the Agency shall notify MARC of the revocation within 24 hours. MARC will remove access to all identifying information about that client within 24 hours of notification or by 9 am on the next business day, whichever is later.

7. The Agency shall not include profanity or offensive language in the CW database.

8. The Agency shall utilize the CW for business purposes only.

9. MARC shall provide in person and online training to Agency staff on the use of the CaseWorthy software. MARC shall provide supplemental training to address modifications to the CaseWorthy software when needed. MARC will provide ongoing Technical Assistance and specialized training as needed.

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

a. Visitors and Clients are appropriately escorted to ensure that they do not access staff areas, record storage areas, or other areas potentially containing Client information. Persons not recognized as staff, visitors and Clients shall be challenged for identification.
b. Client records that are retained as hard copy are stored in locking filing cabinets or in rooms that can be locked.

c. Photocopiers, printers and fax machines are located so as to minimize access by visitors and unauthorized persons.
d. Directors and other management or supervisory personnel are familiar with security and confidentiality policies and enforce such policies to ensure the security and confidentiality of the CW database and of Client information.
e. The Agency staff feels comfortable and obligated to report security breaches and misuse of the CW database system.
f. The Agency shall encourage clients to report any breaches of confidentiality that they observe in the Agency.

Cost

The Agency agrees to pay an annual fee to use the HMIS system, and understands that the HMIS Governing Board will establish fees and secure concurrence from the Continuum of Care Boards of Directors. The HMIS Governing Board may be contacted by an agency for a reduction in annual fees if a financial hardship can be demonstrated. Agencies may pay their fee on a quarterly basis. Annual fees for each year will be established by the HMIS Governing Board before October 1 for the next calendar year.

Monitoring

The Agency understands and agrees to periodic data and security site monitoring conducted by Lead Agency Program staff. The purpose of the monitoring is to identify if Agency personnel or volunteers using the CW system need training, technical support or other services to meet data quality standards and benefit from the full use of the CW system. In the event that the Agency has significant, unresolved compliance findings identified either in data monitoring summaries or site visits, a series of steps will be taken according to the Data Quality Monitoring Plan and Privacy and Security Monitoring Plan. (Addendums to this agreement).

Reporting

1. The Agency shall be enabled to report on identifying and statistical data on the Clients it serves, subject to the terms of this Agreement regarding Client confidentiality.

2. The Agency shall not be enabled to report on identifying and statistical data on Clients it does not serve.

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

4. MARC shall use only unidentified aggregate CW data for policy and planning activities, in preparing federal, state or local applications for funding, to demonstrate the need for and effectiveness of programs and to obtain a system-wide view of program utilization in the two Continua.

Indemnification

The Agency hereby agrees to indemnify, defend and hold harmless MARC and all Agencies using the CaseWorthy HMIS system (including their respective officers, directors, employees, professional

advisors, and agents) from and against all demands, claims, suits, proceedings, judgments, settlements, arbitration awards, damages, loss, cost, expense (including reasonable attorneys' fees and costs of litigation), sanctions, fines and penalties arising out of or resulting from any acts or omissions of the agency and/or any of its personnel in violation of this Agreement.

Limitation of Remedies
No party shall be liable for any special, indirect, consequential or punitive damages (including loss of profits) under or in connection with this Agreement.

Termination
Either Party may terminate this Agreement upon thirty (30) days written notice to the other party. In addition, either party may terminate this Agreement if the other party ("Defaulting Party") fails to comply with any of its obligations under this Agreement and such failure is not cured within seven (7) days after the Defaulting Party receives a written notice of default from the other party. Termination of this Agreement shall be without prejudice to any claims or obligations arising or accruing hereunder prior to the date of termination. Sanctions for violating this Agreement may include, in addition to any other remedies available at law or in equity, the requirement of additional training, or the suspension/revocation of HMIS privileges.

Term of Agreement
The term of this Agreement is for three (3) years, and may be renewed on an annual basis by mutual consent of both parties. The HMIS Governing Board will review and renew its license agreement with CaseWorthy, and notify participating agencies of all renewals.

Miscellaneous

1. This Agreement may only be modified by a written amendment signed by both parties.

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

3. This Agreement shall be interpreted and enforced in accordance with the laws of the State of Missouri.

AGREED TO:

_____ _____ _____

Agency Director/Executive Officer *(signature)* *(date)*

_____

Agency Name

_____ _____ _____

Street Address City Zip Code

_____

_____ _____ _____

MARC Executive Officer *(signature)* *(date)*

SECURITY AND PRIVACY POLICY – HMIS LEAD AGENCY

The Mid-America Regional Council (MARC) serves as the Homelessness Management Information System (HMIS) Lead Agency for two Continuum of Care organizations (KS-505 and MO-604). The CaseWorthy HMIS system will serve over 50 agencies in the greater Kansas City area. MARC's privacy and security policy is designed to:

- Ensure the confidentiality, integrity, and availability of all HMIS information to protect clients served by local agencies
- Protect against any reasonable anticipated threats to security
- Ensure compliance by End Users to HUD and other federal, state and local rules

Key terms used

Covered Homeless Organization (CHO) – any organization (employees, volunteers, and contractors) that records, uses or processes Protected Personal Information

Protected Personal Information (PPI) – any information about a homeless client that (1) identifies a specific individual, (2) can be manipulated so that identification is possible, or (3) can be linked with other available information to identify a specific individual

Security Policy

MARC as the HMIS Lead Agency and each CHO must apply system security provisions to all systems where PPI is stored, including, but not limited to, the HMIS Lead Agency and CHO networks, desktops, laptops, tablets and servers. Security has three categories: system security, software application security, and hard copy security.

The following section (a) covers security for client data to be obtained for purpose of transitioning the data from the current HMIS vendor system, MAACLink, to the new system, CaseWorthy.

a. System Security

User Authentication: MARC as the HMIS Lead Agency will utilize CaseWorthy LLC's CaseWorthy system, an HMIS-compliant system with appropriate system level security. As MARC works to transition the CHOs from the current HMIS vendor to CaseWorthy, MARC will receive and evaluate HMIS client data for mapping data fields from one system to another and to identify duplicate records. MARC will receive the client records using a secure FTP site, and will store the records on a separate server that is password protected. The separate server will have SQL server 2016 with no Windows authentication and create SQL server accounts with specific permissions to access the database. MARC's two database analysts, the IT director and Network Administrator will have access to the server. MARC will also use SQL audits for tracking purposes. MARC will set up required password protection standards for use of this server. Once MARC has successfully completed mapping the current client data to CaseWorthy and no longer needs this server to complete the transition, the server will be cleaned of all data using procedures outlined below.

MARC as the HMIS Lead Agency will require a user authentication system consisting of a username and password. Passwords must be at least 8 characters long and meet reasonable industry standards, including but not limited to:

- At least one number and one letter
- Not using, or including, the username, the HMIS name, or the HMIS vendor's name, and/or
- Not consisting entirely of any work found in the common dictionary or any of the above spelled backwards

MARC s the HMIS Lead Agency will require users to change their passwords every 90 days. Users will be locked out from the system after 4 unsuccessful log in attempts. 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 may 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.

Once the CaseWorthy system goes live, HMIS Lead Agency staff and CHO system users must follow the User Authentication requirements stated above.

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

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

Public Access: NA. MARC may choose to implement a public portal to allow CHOs to have clients enter or update some of their information. At the time such a public portal is implemented, the CHO must follow HUD requirements for security protections.

Physical Access to Systems with Access to HMIS Data: A CHO must staff computers stationed in public areas that are used to access the CaseWorthy system 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. MARC has established a timeframe of 60 minutes to log a user out of the system if not in active use. This log out will automatically show a password protected screen saver. A CHO may commit itself to additional security protections consistent with HMIS requirements, including timeframe to log users out of the system after a period of inactivity. MARC will require that all CaseWorthy system uses change their passwords every 90 days and only allow users to attempt unsuccessfully to log in four times before they are locked out of the system. A CHO may set more stringent standards for their users regarding changes to passwords or log in attempts.

Disaster Protection and Recovery: The CaseWorthy system operated by CaseWorthy LLC will maintain a backup to the system stored in a secure off-site location where the required privacy and security standards also apply. For purposes of working with client data during the transition from MAACLink to CaseWorthy, MARC as the Lead Agency will use a server, mini-computer or mainframe housed in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors must be used to protect systems used for collecting ad storing all of the HMIS data. If a CHO exports data from the CaseWorthy system and stores it electronically, the CHO will follow the same security measures as the HMIS Lead Agency described in this paragraph.

Disposal: In order to delete all HMIS data from a data storage medium, MARC and a CHO must reformat the storage medium more than once before reusing or disposing of the medium. When MARC disposes of servers, the agency wipes and/or destroys the drives. MARC wipes workstation drives before disposing.

System Monitoring: HMIS data must maintain a user access log. A CHO must use appropriate methods to monitor the security systems. CaseWorthy software includes a user history for all client records added, deleted, or modified.

b. Software Application Security: The CaseWorthy system meets all HUD requirements for Software Security during data entry, storage and review or other processing function. See User Authentication described above.

Electronic Data Transmission: MARC and a CHO must encrypt all HMIS data that are electronically transmitted over the Internet, publicly accessible networks or phone lines to current industry standards. The current standard is 128-bit encryption. Unencrypted data may be transmitted over section direct connections between two systems. A secure direct connection is one that can only be accessed by users who have been authenticated on at least one of the systems involved and does not utilize any tertiary systems to transmit the data. A secure network would have secure direct connections.

Electronic Data Storage: MARC and a CHO must store all HMIS data in a binary, not text, format (CaseWorthy does this).

c. **Hard Copy Security:** MARC and a CHO must secure any paper or other hard copy containing PPI that is either generated by or for HMIS, including but not limited to reports, data entry forms and signed consent forms. MARC and a CHO must supervise at all times any paper or other hard copy generated by or for a HMIS that contains PPI when the hard copy is in a public area. The information must be secured when staff are not present.

HMIS Security Officer

As the HMIS Lead Agency, MARC must designate one staff member as the HMIS Security Officer. [MARC designates Helen Krosky, HMIS Project Manager, as the HMIS Security Officer.] If the designated employee changes, MARC will notify the two CoCs within 72 hours of the appointment of a new HMIS Security Officer.

Each agency using the system (CHO) must also designate a HMIS Security Officer to be responsible for ensuring compliance applicable security standards within their organization. The CHO Security Officer does not need to be an End User but they must be an employee of the participating organization. For any CHO without employees, the HMIS Security Officer must be the President, Chair, or other top-level representative responsible for the participating organization.

Workforce Security

The HMIS Lead Agency and each CHO must have a workforce security policy that includes conducting a criminal background check on its HMIS Security Officer and on any users with Agency Administrator level access or greater. Criminal Background checks must be completed at least once. On request, CHOs must verify to HMIS when the most recent criminal background check has been completed for each applicable staff member. The background check must include local and state records; CHOs are strongly encouraged to include federal records as well, but are not required.

Security and Privacy Awareness Training and Follow-up

The HMIS Lead Agency will conduct a security and privacy awareness training on an annual basis, which will be required for all End Users and Security Officers. This training will cover relevant statutory and regulatory requirements, local policies, and best practices for HMIS Privacy and Security. If an End User or Security Officer does not attend the required annual training, their access to CaseWorthy will be restricted until they attend training.

Reporting Security Incidents

Any End User or Security Officer suspecting violations of Security and Privacy policies should report incidents in writing.

> **Chain of Reporting**: End Users should report issues first to their CHO's designated Security Officer within one business day. Security Officers should report the issue jointly to the CHO Director and the HMIS Lead Staff within one business day.

Disaster Recovery Plan

The Disaster Recovery Plan for HMIS is the responsibility of our HMIS Vendor, CaseWorthy, which hosts and houses the data on remote servers. The vender, CaseWorthy will perform regular scheduled backups of the system to prevent loss of data. In the event of a disaster involving substantial loss of data or system downtime, HMIS Lead Agency will contact CHO Security Officers by phone or email within one business day to inform them of the expected scale and duration of the loss or downtime.

Annual Security Review

All CHOs must undergo an annual security review, which will include at minimum the completion of a Security Checklist. Agency Administrators will work with the CHO Security Officer to schedule an audit and will assist with performing the review. The results of the annual review must be returned to the HMIS Security Officer via Fax or Email the same day they are completed. Any items needing to be fixed must be fixed within 10 working days.

Contracts and other arrangements
The HMIS Lead Agency must retain copies of all contracts and agreements executed as part of the administration and management of HMIS or required to comply with HUD policies.

PRIVACY POLICY

Data Collection Limitations: A CHO may collect PPI only after obtaining oral or written consent from the individual and using lawful and fair means. The CHO should only collect information when appropriate to the purpose for which it is obtained or when required by law. A CHO must post a sign at each intake desk (or comparable location) that explains the reasons for collecting the information.

Data Purpose and Limitations: A CHO must develop and implement a plan to dispose of or alternatively remove identifiers from PPI that is not in use for 7 years after the PPI was created or last changed (unless a statutory, regulatory, contractual or other requirement mandates longer retention). A CHO must specify in its privacy notice the purpose for which it collects PPI, including disclosure for the specified purpose. PPI may not be disclosed directly or indirectly for any government agency for inclusion in any national homeless database unless required by statute. The CHO must maintain an audit trail containing the date, purposes and recipient of some or all disclosures of PPI. The CHO must make the audit trail of disclosures available to the homeless individual on request.

Openness: A CHO must publish a privacy notice describing its policies and practices for the processing of PPI and provide a copy of the privacy notice to any individual upon request. A CHO must post a sign stating the availability of its privacy notice. The privacy notice may be amended at any time and that amendments may affect information obtained by the CHO before the date of the notice change. The CHO must make reasonable efforts to offer a client a copy of the privacy notice at or around the time of data collection.

Access and Correction: A CHO must allow an individual receiving services to inspect and have a copy of any PPI about the individual. There are circumstances when a CHO may reserve the ability to deny requests: anticipation of litigation, information obtained under a promise of confidentiality, or disclosure could endanger the life or physical safety of an individual. A CHO must offer to explain any information that the individual may not understand and consider any request by an individual for correction of inaccurate or incomplete PPI. A CHO is not required to remove any information, but may alternatively mark information as inaccurate or incomplete and supplement it with additional information.

Accountability: A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. The HMIS Lead Agency must offer annual training on privacy requirements, and a CHO must require each member of its staff to undergo the annual training. A CHO must require each member of its staff to sign a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

System Confidentiality and Use Agreement

HMIS is a client information system used to assess the needs of those individuals that utilize social services related to homelessness ("clients"), creates individualized service plans and records the use of housing and services, which communities can use to understand the utilization of services, identify gaps in the local service continuum and develop outcome measurements. Participating agencies and their system users must comply with the HMIS Policies and Procedures. Mid-America Regional Council (MARC) is the HMIS Lead Agency and serves as system administrator for the two Continuum of Care ("CoC") organizations serving Jackson, Wyandotte and Johnson counties.

A. Confidentiality

I understand that I will be allowed access to confidential information and/or records in order to perform my specific job duties. I further understand and agree that I am not to disclose confidential information and/or records without the prior consent of the appropriate authority(s).

I understand that my User ID and Password to HMIS are issued for my use alone. I further understand that I am solely responsible for all information obtained, through system access, using my unique identification. At no time will I allow any other person to use ~~of~~ my account to access ~~to~~ HMIS. I understand that accessing or releasing confidential information and/or records, or causing confidential information and/or records to be accessed or released, on myself, other individuals, clients, relatives, etc., outside the scope of my assigned job duties would constitute a violation of this agreement. I understand my supervisor will be notified immediately of any violation and disciplinary action will be taken, up to termination of employment.

B. User Responsibilities

Users shall enter accurate, complete and timely data in accordance with the HMIS Policies and Procedures. **Please read each statement below and <u>sign your initials</u> to indicate you understand and accept the terms**.

___ My user ID and password are for my use only and must not be shared with anyone.

___ I will take reasonable measures to keep my password secure.

___ I understand that ~~the~~ only authorized users can view information in the system and the clients to whom the information pertains.

___ I will only access and use information that is necessary to perform my job.

___ If I am logged into the system and must leave my computer, I will first log out.

___ Any hard copies of electronic records will be kept in a secure file.

___ When hard copies are no longer needed, I will ensure they are properly destroyed.

___ If I notice or suspect a security breach or abuse of client confidentiality, I will immediately notify my HMIS Site Administrator or the HMIS System Administrator.

By affixing my signature to this document I acknowledge that I have been apprised of the relevant laws, concerning access, use, maintenance, and disclosure of confidential information and/or records which shall be made available to me through my use of the HMIS.

I further agree that it is my responsibility to assure the confidentiality of all information, which has been issued to me in confidence, even after my access to HMIS has ended.
Pursuant to this agreement I certify that I have read and understand the laws concerning confidential information and/or records.

By signing the System Confidentiality and Use Agreement, you agree to comply with these terms and conditions. Failure to uphold these terms may result in loss of access or privileges.

USER NAME [PRINT]	DATE	AGENCY REPRESENTATIVE NAME [PRINT]	DATE
USER SIGNATURE	DATE	AGENCY REPRESENTATIVE SIGNATURE	DATE

Privacy Notice

The U.S. Department of Housing and Urban Development (HUD) requires that each jurisdiction that receives funding from HUD have a Homeless Management Information System (HMIS) in place. This agency participates in the greater Kansas City HMIS System, an electronic data collection system that stores information about the men, women, and children who access homeless and other human services in a community. The purpose of HMIS is to assist in determining your needs and to evaluate the effectiveness of services provided.

We only collect information that is needed to provide you services, or that we consider relevant to helping us understand the scope and dimensions of homelessness in order to design effective service delivery. We do not disclose your information without written consent, except when required by our funders or by law, or for specific administrative or research purposes outlined in our HMIS Privacy Policies. By requesting information and accepting services from this agency, you give consent for us to enter your information into the HMIS.

The collection and disclosure of all personal information is guided by strict security standards. You have the right to see your personal information collected by this partner agency and request changes if incorrect. Your information will only be used by this agency and other community agencies to which you are referred for services. You also have the right to refuse certain data to be entered into the HMIS database. A full copy of our agency's HMIS Privacy Policies is available upon request for your review.

Client Release of Information

To provide you with the most effective and efficient service, we must collect certain data for our Homeless Management Information System (HMIS). This secure and confidential database operated by trained representatives allows our agency and other community providers to work together with you to make sure you are receiving the assistance you need in a timely manner. Beyond that, the HMIS allows the Continuum of Care to get an accurate count of all people experiencing homelessness or who are at risk of homelessness in the greater Kansas City area. To better coordinate with other agencies, you have the right to consent to release your information to these other agencies.

FOR DATA BEING ENTERED INTO THE HMIS, I UNDERSTAND THAT:

 Staff of other agencies who will see my information have promised to protect it.
 Information I give about physical or mental health problems will not be shared with others.
 Partner Agencies may share information that does not identify me to others.
 I have the right to request who has looked at my file.
 I understand I have the right to ask, "Can I refuse to answer that question," and how my refusal might affect my receipt of services.
 I have the right to view confidentiality policies used by HMIS.
 If I receive assistance through the Supportive Services for Veteran Families (SSVF) Program that my personally identifying information will be exported from HMIS and uploaded to a Veterans Administration (VA) Repository to meet VA-required reporting.
 Another Partner Agency may enter my data into HMIS and therefore may retain the paper copy file.
 If I decide at a later date that I no longer want my information in HMIS, I can request that it be archived (not made available for further use by other agencies).
 I am responsible for making all household members aware their information will be entered in HMIS and they have the option to contact this agency with any questions or concerns.

Please review the information below and sign and date where indicated.

I understand that this agency will enter my information into the Homeless Management Information System (HMIS) called CaseWorthy. The information I have provided is true and correct. My information may be shared among local authorized service providers for the purpose of connecting me to services. My name, date of birth, social security number, or other information that would identify me personally will never be shared with anyone without my authorization. An agency representative has answered my questions about my privacy concerns.

By signing this release form, I fully understand the above terms and conditions.

CLIENT NAME [PRINT]	DATE	CLIENT SIGNATURE	DATE

AUTHORIZED PERSONNEL NAME [PRINT]	DATE	AUTHORIZED SIGNATURE	DATE

Client Consent on Behalf of Household Members

An adult head of household may provide consent on behalf of family members to share their information in the HMIS.

FAMILY MEMBER NAME 1 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 1 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 2 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 3 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 4 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 5 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 6 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 7 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]

Client Revocation of Consent

CaseWorthy Client Information Sharing System

I hereby revoke permission for the partner agencies in the Continuum of Care to share my personal information and information regarding me and/or my family members in the CaseWorthy Client Information Sharing System.

Identifying information will be removed from the system (check all that apply):

- ☐ Name
- ☐ Social Security Number
- ☐ Day and Month of Birth
- ☐ Last Permanent Address
- ☐ Phone Number

Non-identifying information will remain (check all that apply):

- ☐ Gender
- ☐ Year of Birth
- ☐ Any other non-identifying information

Client Name: _____

Client Signature _____
(Parent or Guardian, if minor & relationship)

Date _____

Executed at:

Name of Partner Agency _____

Agency Witness Name _____

Agency Witness Signature _____

Date ----------