Homeless Management Information System (HMIS)

Security and Privacy Plan

COC KS-505

Johnson County Kansas

HMIS Lead Agency

Mid-America Regional Council

Revised June 20, 2020

Contents

1.0 Revision History

Date	Description
06/20/2020	Updated to coincide with revised Policies and Procedures.
08/07/2017	Original

2.0 HMIS Collection of Guiding Documents

This HMIS Security and Privacy Plan is part of a suite of documents used in managing the HMIS. For further understanding of how this Plan is incorporated into the overall collection refer to the documents identified with a checkmark.

	Document Title	Purpose
✓	HMIS Governance Charter	Charter that establishes the governance structure for the operation of the HMIS.
✓	HMIS Policies and Procedures	A codified document that outlines all of the necessary policies, procedures, and rules of HMIS.
	HMIS Data Quality Plan	Plan that facilitates the ability of each CoC to achieve statistically valid and reliable data.
	HMIS Security and Privacy Plan	THIS DOCUMENT
✓	Agency Partner Agreement	Formal signed agreement between the Partner Agency and the HMIS Lead Agency which spells out the key terms of the agreement relating to confidentiality, monitoring, and reporting.
✓	System Confidentiality and Use Agreement	Formal signed agreement for HMIS Users that identifies the terms and responsibilities of using the HMIS system.
✓	Client Release of Information	A signed release giving permission to Partner Agencies to share client data.

3.0 OVERVIEW

3.1 Purpose

The HMIS Lead Agency is responsible for overseeing HMIS privacy and security. MARC as the HMIS Lead Agency manages CaseWorthy LLC's CaseWorthy system, an HMIS-compliant system with appropriate system level security. This plan includes the policies and procedures necessary 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 Agency Users to HUD and other federal, state, and local rules

3.2 Key Terms

Continuum of Care	The local planning entity for homeless programming and service delivery. Where "CoC" is used in this document it is in reference to the Continuum of Care.
HMIS Oversight Committee	A subcommittee of the local Continuum of Care responsible for governance, oversight and troubleshooting of the HMIS for the CoC.
HMIS Lead Agency	The organization that manages, administers, and operates the overall HMIS on behalf of the CoC.
Participating Agency *(Aka Partner Agency)*	Any organization that records, uses, or PII in HMIS. Also known as a Covered Homeless Organization (CHO).
HMIS Lead Agency Administrative Representative *(Aka Agency Lead))*	The individual within a participating agency who has been identified by that agency as the administrative lead or, direct contact person between the Participating Agency and the HMIS Lead. This individual is responsible for ensuring the training of the agency's users, the ongoing proficiency of the Agency System Users, the prompt reporting of terminated users to the CoC's System Administrators, the timeliness of data entry and quality of data entered, data security and any other such tasks as articulated by the CoC and/or included HMIS Policies and Procedures.
Client	A person who receives services at an HMIS participating agency.
Personally Identifiable Information (PII)	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.
Agency System User *(Aka User)*	Individual within a participating agency who has been trained, has demonstrated competency to the satisfaction of the Agency HMIS

	Administrative Lead and uses the HMIS as a function of their responsibilities within the agency.

4.0 SECURITY

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

4.1 System Applicability

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

4.2 System Security

User Authentication

User authentication consists 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
- 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.
- 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.

Virus Protection

The HMIS Lead Agency and each Participating Agency 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

The HMIS Lead Agency and each Participating Agency 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.

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.

Disposal

All technology equipment (including computers, printers, copiers, and fax machines) used to access HMIS, and which will no longer be used to access HMIS will have their hard drives reformatted multiple times. If the device is now non-functional, it must have the hard drive pulled, destroyed, and disposed of in a secure fashion.

System Monitoring

HMIS systems must maintain a user access log; CaseWorthy's software includes a user history for all client records added, deleted, or modified. Partner Agencies must use appropriate methods to monitor the security systems.

4.3 Software Application and Data Security

The CaseWorthy system meets all HUD requirements for Software Security during data entry, storage and review or other processing function.

Electronic Data Transmission and Storage

- 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.

4.4 Hard Copy Security

MARC and each Participating Agency 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.
- 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.

- 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.

4.5 HMIS Security Officer

The HMIS Lead Agency and all Participating Agencies must designate Security Officers to oversee HMIS privacy and security. A single point-of-contact who is responsible for annually certifying that Agencies adhere to the Security Plan, testing the CoC's security practices for compliance.

4.6 Workforce Security

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

4.7 Security and Privacy Awareness Training

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.

4.8 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 Partner Agency's designated Security Officer within one business day. Security Officers should report the issue jointly to the Partner Agency Director and the HMIS Lead Staff within one business day.

The Partnering Agency and HMIS Lead Agency will maintain records of all security incidents, responses, and outcomes.

4.9 Disaster Recovery Plan

- The HMIS Lead must develop a disaster recovery plan that includes protocols for communication with stakeholders.
- 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.

4.10 Annual Security Review

All Partner Agencies must undergo an annual security review, which will include at minimum the completion of a Security Checklist. Agency Administrators will work with the Partner Agency 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.

4.11 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.

5.0 PRIVACY

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.

Partner Agencies 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.

5.1 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*.
- To accomplish any and all other purposes deemed necessary by the HMIS Oversight Committee.

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 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.

5.4 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.

5.5 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. There are circumstances when an agency 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.
- 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.

5.6 Other Authorized Data Disclosures

- Client data may be transmitted to reporting systems as mandated by agency funders.
- Client data may be transmitted to reporting, data warehouse or other similar systems based on the direction of the CoC. Transmission would only occur after approval by the CoC Board of Directors.
- 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.

5.7 Accountability and Privacy Policy Complaints

- An agency must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices.
- 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.
- The HMIS Lead Agency must offer annual training on privacy requirements, and the Partner Agency must require each member of its staff to undergo the annual training.