Spokane Regional Continuum of Care HMIS Policies and Procedures Manual

Adopted by the City of Spokane Community, Housing and Human Services (CHHS) Board on April 2, 2014

_____

Jerrie Allard, Director of CHHS

TABLE OF CONTENTS

APPENDIX B: HMIS USER AGREEMENT
APPENDIX C: HMIS LICENSE REQUEST
APPENDIX D: HMIS LICENSE REQUEST INSTRUCTIONS
APPENDIX C: CLIENT INFORMED CONSENT
APPENDIX D: CLIENT DISCLOSURE AND PRIVACY RIGHTS
APPENDIX G: HMIS USER MANUAL
APPENDIX H: HMIS FEE SCHEDULE

HMIS TEAM CONTACT INFORMATION

David Lewis, HMIS Program Manager
509.625.6051
dglewis@spokanecity.org

Daniel Ramos

dramos@spokanecity.org

Teague Griffith

tgriffith@spokanecity.org

BACKGROUND

The Spokane Regional Homeless Management Information System ("HMIS") is a tool designed to collect and store client-level data regarding the characteristics and service needs of persons experiencing homelessness or persons at risk of homelessness. HMIS data is used to report to program funders, to complete major annual data projects, to support grant applications and for local strategic planning. The Spokane Regional HMIS has been operating since 1996 and has gained national recognition for both the database project and Spokane's homeless service providers.

In 2004 the HMIS was upgraded to operate on the web. Currently, the City of Spokane Community, Housing and Human Services Department (CHHSD) administer the HMIS, using an online system provided through a software vendor called ClientTrack.

This document provides the policies and procedures that govern HMIS operations, including the roles and responsibilities for participating agency staff. All Participating Agencies are to remain in compliance with policies and procedure listed herein as confirmed in their signed partner agency agreements.

1. TERMINOLOGY

Benchmark: standard a standard against which something can be measured or assessed

Client: An individual about whom a Contributing HMIS Organization (CHO) collects or maintains personally identifiable information:

1. Because the individual is receiving , has received, may receive, or has inquired about assistance from a CHO; or
2. In order identify needs, or to plan or develop appropriate assistance within the CoC.

Continuum of Care (CoC): The range of services provided regionally by nonprofit homeless service providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing

developers, law enforcement, and organizations that serve veterans, organized to assist persons experiencing homelessness and person at risk of homelessness.

Contributing HMIS Organization (CHO): an organization that operates a project that contributes data to an HMIS.

Database: an electronic system for organizing data so it can easily be searched and retrieved.

Homeless Management Information System (HMIS): the information system designated by the CoC to comply with HUD requirements established in notice. The HMIS is used to record, analyze, and transmit client and activity data in regard to the provision of shelter, housing, and services to individuals and families who are experiencing homeless or at risk of experiencing homelessness.

HMIS Lead: an entity designated by the CoC to operate the CoC's HMIS in accordance with HUD requirements established in notice.

Contract Compliance Officer: the staff person assigned duties as outlined in Section 2, Roles and Responsibilities, 2.1a.

HMIS Coordinator: the staff person assigned duties as outlined in Section 2, Roles and Responsibilities, 2.1b.

Clerk III: the staff person assigned duties as outlined in Section 2, Roles and Responsibilities, 2.1c.

Licensed User: also referred to as "user" an individual who uses or enters data in an HMIS or another administrative database from which data is periodically provided to an HMIS.

HMIS Lead Security Officer: the staff person assigned duties as outlined in Section 2.3, HMIS Security Officer Responsibilities, 2.3a.

Agency HMIS Security Officer: the staff person assigned duties as outlined in Section 2.3, HMIS Security Officer Responsibilities, 2.3b.

HMIS Vendor: also referred to as "the vendor", a contractor who provides materials or services for the operation of an HMIS. An HMIS vendor includes an HMIS software provider, web server host, data warehouse provider, as well as a provider of other information technology or support.

Protected Identifying Information: Information about a person that can be used to distinguish or trace a person's identity, either alone or in combination with other information. Generally this includes, but is not necessarily limited to, a person's name and social security number.

Spokane Regional HMIS: The Homeless Management Information System provided by the software vendor and tailored to cover service activities occurring through Spokane City and Spokane County.

2. ROLES AND RESPONSIBILITIES

2.1 HMIS Lead Responsibilities

Policy: The City of Spokane Community, Housing and Human Services Department serves as HMIS Lead and will be responsible for the organization and management of the Spokane Regional HMIS.

2.1a Contract Compliance Officer Responsibilities

- Monitoring compliance and review of control decisions.
- Overseeing of all contractual agreements with funders, CHOs, vendors.
- Authorizing usage and access to the HMIS.
- Communicating with CHO leadership and other stakeholders regarding the HMIS project.
- Supervising of staff including reasonable divisions of labor; hiring; and orientation of new staff to program operations, guiding principles and policies and procedures.
- Acting as the liaison with HUD and the WA Department of Commerce.

2.1b HMIS Coordinators

- Setting up User Licenses.
- Providing training and technical assistance to licensed users and CHOs.
- Coordinating technical support from software vendor.
- Monitoring agency participation including timeliness and completeness of entry.
- Communicating any planned or unplanned interruption in services.
- Mining the database to respond to the information needs of community stakeholders.
- Developing reports to submit data to funders/partner agencies.
- Measuring data quality.
- Monitoring system login activity/user technical assistance needs,
- Analysis of Data Trends.
- Auditing Policy and Procedure compliance.
- Performing data integration between local and state HMIS systems.
- Revising/updating HMIS forms.

2.1c Clerk III

- Assisting HMIS Coordinators as needed.

2.2 Agency Responsibilities:

Policy: Each participating agency will be responsible for adherence to the Policies and Procedures described in this document and for oversight of all agency personnel that have access to the HMIS.

Responsibilities:

2.2a Agency Director or Designee

- Designating an Agency HMIS Security Officer.
- Reviewing quality and completeness of site/project specific data.
- Notifying an HMIS Coordinator of HMIS staffing changes.
- Training staff on site-specific HMIS procedures.

- Ensuring each licensed HMIS user has completed all required license request forms and Partner agency user responsibility and Confidentiality agreement and that these are passed along to a HMIS coordinator.

2.2b Licensed Users

- Entering HMIS data as accurately and completely as possible.
- Entering HMIS data pertaining to activities occurring in any given month no later than the fifth day of the following month.
- Taking appropriate measures to prevent unauthorized disclosure of sensitive data.
- Reporting security violations.
- Complying with signed HMIS user agreements and partner agency agreements.
- Updating user contact information as needed.
- Logging out of the HMIS system when not actively engaged in data entry, review or analysis.
- Maintaining a unique user name and passwords used to access HMIS. Sharing of User Names and/or passwords is prohibited.
- Directing all HMIS related questions to one of the two HMIS Coordinators.

2.3 HMIS Security Officer Responsibilities

Policy: The HMIS Security Officers are responsible for ensuring compliance with state and federal HMIS data security guidelines and local HMIS data security procedures.

Responsibilities:

2.3a HMIS Lead Security Officer

- Updating HMIS security plan as needed.
- Conducting annual HMIS security monitoring at lead agency and at CHOs.
- Providing technical assistance regarding HMIS security.
- Responding to security incidents.
- Ensuring that criminal background checks are completed for each Agency HMIS security officer.

2.3b Agency HMIS Security Officer

- Reporting security incidents to HMIS Lead Security Officer.
- Ensuring that criminal background checks are completed for each user.

3. Operational Policies and Procedures

3.1 HMIS Access

Policy: Each end user will be designated a user access level that controls the level and type of access the user has within the CoC's HMIS database.

Procedures:

- An HMIS Coordinator, with input from the requesting agency, will assign the level and type of access the user will have in the system.
- Agency Staff is required to communicate to an HMIS Coordinator within one business day when an end user's need for access changes.
- An HMIS Coordinator will terminate a user's access upon email notification from Agency HMIS Coordinator.
- An HMIS Coordinator may revoke user access to anyone suspected or found to be in violation of the policies outlined in this document as stipulated in Section 4 (Violations and Sanctions).
- The table below lists the levels of access tied to existing user roles. Consult an HMIS Coordinator to learn about other customizable roles that may be offered.

User Type	Level of Access
CoC HMIS Coordinator	Access to all information and functions within the CoC's HMIS database.
Agency Staff	Access to data entry and reporting features.

3.2 Data

3.2a Collection of Data

Policy: All users of the CoC's HMIS database will abide by federal, state, and local laws regarding the collection of data. Failure to comply may result in revocation of HMIS access and criminal and/or civil legal penalties.

Procedures:

- Before data collection begins the client(s) must be presented with the Client Informed Consent form.
- Clients that are currently fleeing, or are otherwise in danger, from DV cannot have any identifiable information entered into the HMIS.
- Participating Agencies must store signed Informed Consent Information Release Form in client paper file for auditing purposes.
- Participating Agencies must post a Privacy Notice that explains the uses and disclosures of information.

- If client refuses consent, the end user should not include any personal identifiers (First Name, Last Name, and Social Security Number) in the HMIS. It is the responsibility of the end user to determine whether or not the inclusion of a Date of Birth (DOB) could identify the client. If it is determined that the DOB would identify the client, an approximate DOB must be entered.
- It is also the responsibility of the end user to determine if there are any other data fields that might identify the client and remove them.
- The Client ID Number, for clients that have refused consent or must otherwise have their identifiers removed, must be written on the client's paper file for internal identification and monitoring.
- User must follow the HMIS Data Entry Manual.

3.2b Release of Data by CHHSD

Policy: All effort will be made to limit the sharing of data that identifies individual clients.

Procedures:

- Requests for data must be submitted to an HMIS Coordinator via email or submission of a ticket through the CoC's HMIS database.
- The CHHSD will abide by all applicable federal and state laws governing data security and confidentiality.

3.2c Data Sharing

Policy: All agencies participating in the CoC's HMIS database will complete, and abide by, the Agency HMIS Participation Agreement.

Procedures:

- If the Agency agrees to the sharing of data, and the client has signed the section of the Client Consent Form permitted the sharing of data, staff will enter MOU #500 in the Information Release and Security portion of the client's record in HMIS.
- If the Agency does not agree to the sharing of data, staff will set the client record to Restrict to Org in the Information Release and Security portion of the client's record in HMIS.

3.2c Data Quality Plan

Data Quality is a term that refers to the reliability and validity of client-level data collected in the HMIS. It is measured by the extent to which the client data in the system reflects actual information in the real world. With good data quality, the CoC can "tell the story" of the population experiencing homelessness. The quality of data is determined by assessing certain characteristics such as timeliness, completeness, and accuracy. In order to assess data quality, a community must first think about what data quality means and document this understanding in a data quality plan. This data quality plan has three components: Data Timeliness, Data Completeness, and Data Accuracy/Consistency. This document may be revised to comply with all HUD guidance established in Notice.

Component 1: Data Timeliness

Entering HMIS data in a timely manner is important for several reasons. First, it reduces human error that may occur when too much time has elapsed between data collection or service transaction and data entry. Second, timely data entry ensures that data is available when it is needed for: monitoring purposes, meeting funder requirements, informing stakeholders, and strategic community planning. Finally, timely data entry is essential for purposes of data integration between the local HMIS and the Washington State HMIS (administered through the Washington State Department of Commerce). As a recipient of state funds the CoC is obligated to transfer HMIS data between the local HMIS and the state HMIS on a monthly basis. When data is changed on the local system after a transfer has been made, it can result in a mismatch between the two systems.

Policy: **HMIS data entry pertaining to activities (project entries, assessments, project exits, and services provided) occurring in any given month shall be entered no later than the fifth day of the following month.**

Procedures:

- If data pertaining to activities occurring in a given month must be corrected in HMIS after the fifth day of the following month, data entry staff must contact an HMIS Coordinator to ensure the corrections are appropriately transferred to the state HMIS.
- Data in HMIS must be corrected if inaccuracies are discovered. However, an agency's data entry process must allow adequate time for data review and completion of necessary corrections prior to each month's fifth day cutoff. Frequent changes to HMIS data after the fifth day cutoff cannot be the norm. Frequent changes made to HMIS data after the fifth day cutoff may result in monitoring findings.
- *Exception:* The CoC recognizes that certain types of projects (high-volume shelters and some services-only projects) may have difficulty entering exit data by the 5th day cutoff in cases where it is not known if clients will be returning for additional service. In such cases, clients must be exited from the project after a period of no service, not to exceed three months. When exit data is entered, including project exit dates, data should be in reference to the date the client last received service through the project.
- *Exception:* The CoC recognizes that occasional structural changes within HMIS may result in the need to modify historical records or create new records dated in the past. An HMIS Coordinator will work with staff to ensure that these changes are made appropriately and that changes are integrated with the state HMIS as needed.

Component 2: Data Completeness

Data completeness directly impacts the CoC's ability to understand the extent and nature of homelessness, patterns of service use, and the effectiveness of programs and strategies. To ensure ongoing facilitation of confidence in reporting and analysis of HMIS, this document establishes benchmarks for acceptable rates of missing or unknown data for each HMIS data element. Ideally, each agency participating in HMIS would collect 100% of all HMIS data elements for each client served. However, due to the differences in service delivery and data collection requirements that can exist across project types, this is not always possible. Therefore, the CoC has established acceptable rates of missing or

unknown data across each data element and each project type. Special consideration is given to situations where clients have refused consent to have personal identifiers entered into HMIS, or in situations where personal identifiers are prohibited by law from being entered in HMIS. Since clients should never be forced to provide information for entry to HMIS, clients that have refused consent to have personal identifiers entered into HMIS are excluded from calculation of missing or unknown data rates.

Policy: Each project participating in HMIS shall maintain data completeness at or better than the benchmarks for missing (null) and unknown (don't know/refused) as provided in Table ### (to be added at later date).

Procedures:

- Data entry staff shall monitor data completeness and accuracy and make corrections as needed, within timeliness standards.
- An HMIS Coordinator will regularly monitor data completeness in reference to acceptable rates, and will work with data entry staff to ensure corrections are completed if needed.
- If data completeness rates frequently fall out of acceptable ranges, an HMIS Coordinator will contact Program Managers to determine further action needed.
- Data completeness rates outside of acceptable ranges may result in monitoring finding.

Component 3: Data Accuracy/Consistency

Information entered into the HMIS must be valid and must accurately represent the circumstances pertaining to person being served in projects contributing data to the HMIS. False or inaccurate information is considered to be more detrimental to HMIS data quality than incomplete information, as the latter results in a gap that can be acknowledged and mitigated. HMIS data must also be consistent to ensure confidence in reporting and analysis of HMIS data. Consistency pertains to data collection practices as well as a common understanding of all data collection staff.

Policy: All data entered into the HMIS shall be a reflection of information provided by the client, as documented by data collection staff, or otherwise updated by the client and shall reflect the intent of each data element as established by HUD in Notice. Knowingly recording inaccurate information in the HMIS is strictly prohibited.

Procedures:

- On a monthly basis, data entry staff shall review project data and correct any inaccurate data within timeliness standards.
- The CHHS Department will provide standard HMIS training to all new HMIS system users and will develop training materials for ongoing reference.
- The CHHS Department will provide updated training and reference materials in accordance with updated HMIS requirements established by HUD or other funders in notice.
- During annual monitoring, CHHS staff will review client paper files against associated HMIS records to check for accuracy.

3.3 Technical Support

Policy: All requests for technical assistance, where possible, will be submitted via the electronic tracking system provided via the CoC's HMIS database.

Procedures:

- An HMIS Coordinator providing the support will determine how best to provide the requested assistance (e.g. phone, site visit, etc) and will work to resolve issues ASAP.
- The order in which requests are processed is at the discretion of the HMIS Coordinator handling the request.
- The HMIS Coordinator may, if necessary, forward submitted issues to the HMIS Vendor (ClientTrack) for assistance.

3.4 Maintenance of Computer Equipment used to Access HMIS

Policy: Participating Agencies will commit to a reasonable program of equipment maintenance to sustain HMIS operations.

Procedures:

- The participating agency will purchase, maintain, and periodically upgrade equipment capable of running a modern internet browser which is used to access the HMIS system.
- Prior to disposing of any equipment used to access or store HMIS data, the participating agency will ensure that any HMIS data stored on the device has been removed.
- Participating agencies are responsible for troubleshooting onsite hardware and software issues.
- All HMIS data, in electronic or hard-copy form, will be stored in secure locations.
- All equipment used to access the HMIS system will be stored in secure locations.

3.5 Client Rights

3.5a Informed Consent and Confidentiality:

Policy: Personally identifying information about clients served may only be collected and entered into HMIS after first obtaining written informed consent from each adult to whom the information applies.

Procedures:

- Adults may provide consent on behalf of any dependent children.
- Unaccompanied children under age 18 may provide consent for themselves.
- Informed consent may be obtained telephonically, provided that written consent is obtained at the first time the individual is physically present at an organization with access to the HMIS.
- A completed HMIS Informed Consent Form must be stored in each client's paper file.
- Form will be presented, and explained, to all adult signers prior to beginning the collection of data.

3.5b Revocation of Consent:

Policy: Clients may revoke consent to have their personally identifying information in HMIS at any time.

Procedures:

- To revoke consent, clients should submit a request to staff at the agency that initially collected their data or contact an HMIS Coordinator.
- If the request is submitted to Agency staff, a ticket must be submitted via the HMIS Issue Tracker system. An HMIS Coordinator will complete the request ensuring that all identifiable information is removed.

3.5c: Record Access:

Policy: Clients have the right to know what information is contained in their HMIS records, the right to know who entered the information, and the right to know which agency that person was associated with at the time the information was entered.

Procedures:

- Requests for this information should be directed to an HMIS Coordinator at the City of Spokane.

3.5d Refusal to Provide Information:

Policy: Clients have the right to refuse to provide information for HMIS purposes, and cannot be denied service due to this refusal.

Procedure:

- When clients refuse to provide information the staff person entering data into the HMIS should indicate the appropriate response of 'Refused'.

3.6 System Availability

Policy: The system will be available at all times to licensed users, except as needed for maintenance.

Procedures:

- The HMIS Lead Agency will inform end users of planned or unplanned interruptions in service and will work to resolve service as quickly as possible.

3.7 Participation Fees

Policy: The CHHSD reserves the right to charge participation fees.

Procedure:

- Participating Agencies should consult the HMIS Fee Schedule document for current HMIS participation costs.

4. Security Policies and Procedures

4.1 User Authentication

Policy: The HMIS can only be accessed with a valid username and password combination. An HMIS Coordinator will provide unique username and initial password for eligible individuals after completion of required training and signing of the HMIS User Agreement and receipt of these Policies and Procedures.

Procedures:

- Users must sign the HMIS User Agreement and are responsible for adhering to the letter, and intent, of the agreement.
- HMIS Coordinator will be responsible for the distribution, collection, and storage of the signed HMIS User Agreements and receipts of these Policies and Procedures.
- An HMIS Coordinator will assign new user with a username and an initial password.
- End user will be required to create a permanent password within 1 business day or access will be terminated.
- Users will maintain password confidentiality. The sharing of passwords or accounts is prohibited.
- Agency staff is required to notify An HMIS Coordinator when user leaves employment with the Agency, or no longer needs access, within one business day.
- An HMIS Coordinator will terminate access upon notification by agency staff within one business day.

4.2 Extracted Data Security Measures

Policy: Users will maintain the security of any client data extracted from the HMIS and stored locally in compliance with all applicable state and federal laws.

Procedures:

- Extracted data that contains personally identifiable information must be stored in a secure location that is not accessible to the general public, is secured via physical or electronic means, and is restricted to only those staff that has an immediate need.
- Any security questions can be addressed to an HMIS Coordinator.

4.4 Backup and Recovery Procedures

Policy: The HMIS Lead Agency will coordinate with the Vendor to ensure proper backup and recovery, if needed, of HMIS data.

Procedure:

- The Vendor will perform regular schedule backups of the system to prevent the loss of data, per contract.

4.5 Hardware Security Measures

Policy: All computers and networks used to access HMIS must have virus protection software and firewall installed. Virus definitions and firewall must be regularly updated.

Procedures:

- HMIS Lead Agency must confirm that Participating Agencies have virus protection software and firewall installed prior to granting HMIS access
- Anti-Virus software must be set to automatically update.
- Firewall must be placed between any computer and internet connection for the entire network, be protected with at minimum Wired Equivalent Privacy (WEP), use Network Address Translation (NAT), and maintain the most recent virus security updates.
- The Agency Director, or Designee, is responsible for ensuring Agency compliance.

4.6 Security Review

Policy: Each HMIS Lead Agency will complete an annual security review to ensure the implementation of the security requirements for itself and Participating Agencies, per the HMIS Security Checklist

Procedures: (Waiting on HUD guidance)

4.7 Violations and Sanctions

Policy: Any user found to be in violation of these policies and procedures may have their HMIS access suspended or revoked and may be liable for civil and/or criminal penalties.

Procedures:

- Users are obligated to report suspected instances of non-compliance to the Agency Program Manager, or Designee, who will in turn notify an HMIS Coordinator ASAP.
- An HMIS Coordinator will investigate potential violations.

5. Appendices

APPENDIX A: AGENCY PARTICIPATION AGREEMENT

APPENDIX B: HMIS USER AGREEMENT

APPENDIX C: HMIS LICENSE REQUEST

APPENDIX D: HMIS LICENSE REQUEST INSTRUCTIONS

APPENDIX E: CLIENT INFORMED CONSENT

APPENDIX F: HMIS FEE SCHEDULE