Spokane City/County CoC Homeless Management Information System (HMIS) Policies and Procedures Manual

Policies and Procedures Manual

Overview

The CoC for its Homeless Management Information System (HMIS) Implementation develops these policy standards and subsequent procedures of data usage for all users and user agencies. This manual serves to protect the confidentiality of all personal information entered into the Homeless Management Information System while identifying the reasonable, responsible, and limited uses and disclosures of data, which comply with federal regulations set by the Department of Housing and Urban Development (HUD) and state regulations. Its purpose is to provide guidance based on federal and state regulations for agencies in their daily operations. It in no way should serve as a substitute or supersede any federal or state regulations outlined and updated by HUD in its Data and Technical Standards. All agencies are responsible for maintaining their own compliance with federal and state regulations as well as any outside applicable regulations such as the Health Insurance Portability and Accountability Act (HIPAA) standards.

Policies and Procedures Manual

Table of Contents

I. Roles and Responsibilities

A. *Community, Housing, and Human Services Department (CHHSD) (HMIS Lead Agency)*

Policy: The Community, Housing, and Human Services Department (CHHSD) is the HMIS Lead agency and is responsible for system administration and project management of the CoC's HMIS database for CoC WA502

Procedure: The HMIS Lead Agency will engage in the following in support of the HMIS:

A. Respond to CoC and HMIS Committee concerns and needs.
B. Oversee the day-to-day administration of the HMIS Program.
C. Ensure system integrity and availability.
D. Provide effective training on software and related issues, including ethics and client confidentiality.
E. Secure and manage contracts with the software vendor and ongoing communications.
F. Provide staffing and a budget for operation of the HMIS.
G. Provide training to participating agencies on all funder and CoC guidelines and requirements for the collection and entry of data.
H. Provide technical support to participating agencies.
I. Regularly review data quality and related system metrics and provide reports to the HMIS Committee for review.
J. Monitor HMIS participating agencies to ensure compliance with established HMIS policies and procedures. Report violations to the HMIS Committee for recommendation and possible submission to the CoC.
K. Educate the CoC and HMIS Committee leadership to enhance their participation in, and understanding of, the HMIS Program.
L. Maintain knowledge about program components and data usage in order to guide end users on program design to ensure the most efficient, and accurate, data is collected.
M. Staff the HMIS Committee.

B. *Spokane City/County Continuum of Care (CoC) Governance Board*

Policy: the Spokane City/County Continuum of Care (CoC) Governance Board

will provide oversight of the HMIS Program.

Procedure: the CoC will engage in the following in support of the HMIS:

A. Support HMIS participation through funding considerations when deciding funding for CoC projects, giving preference to agencies/organizations that comply with HMIS participation requirements.
B. Regularly review data quality and other reporting updates submitted by the HMIS Committee.
C. Regularly monitor HMIS Lead and participating agencies for compliance.
D. Ensure CoC participating agencies participation and investment in the HMIS through promotion of the HMIS as the sole repository of data within the CoC.
E. Ensure CoC participating agencies work with HMIS Lead staff to ensure the accuracy of all data in the system to include, but not limited to, the data which populates: CoC NOFA, AHAR, PIT, System Performance Measure's Report and other reports as needed.
.

D. Covered Homeless Organization (CHO)

Definition: Any CHO ('Agency') (including all its affiliates) that records, uses or processes* PII (Personally Identifiable Information) on clients experiencing homelessness or those at risk of experiencing homelessness for an HMIS (Section 4.1.1, *2004 HMIS Data and Technical Standards*).
*Processing refers to any and all operations performed on the PII (i.e. collection, maintenance, etc.).

Policy: Any CHO participating in the HMIS will abide by all policies and procedures outlined in this manual and as specified in the HMIS Partner Agency Agreement.

Procedure: Any CHO, organization, or group, who has signed the Partner Agency Agreement will be given access to the HMIS database through trained HMIS Users (see E. HMIS Users below).

Policy: CHOs are responsible for communicating needs and questions regarding the CoC's HMIS directly to the CHHS Department's HMIS Team.

Procedure: Users at CHOs will communicate needs, issues and questions to the HMIS Team using the support request application in ClientTrack.

E. HMIS Users

Policy: Any individual who uses ClientTrack must have a signed HMIS User Agreement on file with and abide by all policies and procedures in this Manual, HMIS User Agreement, and other standards and practices as adopted by the CHHSD and/or the HMIS Committee.

Procedure:
CHOs are responsible for identifying the employees needing access to the CoC's HMIS and ensuring that completed HMIS User Agreements are submitted to the HMIS Lead Agency.

HMIS Users are responsible for adhering to policies and procedures in data collection and privacy and security practices, ensuring quality, timely data entry, and correcting errors as they become known.

Directors or managers who do not wish to become an HMIS user but who are ultimately responsible for their agency's HMIS data may attend HMIS trainings as desired and receive aggregate reporting from users they oversee.

Directors and managers are responsible for notifying the HMIS Lead Agency to de-activate an HMIS users account if that person is no longer employed or requires their HMIS account to be revoked. Revocation requests resulting from termination of employment must be received within 24 hours of the termination of employment. The HMIS Program Manager reserves the right to revoke and/or re-instate a user at any time.

F. HMIS Committee

Policy: The CoC will have an HMIS Advisory Committee to provide community feedback on HMIS implementation related activities and issues.

Procedure: The HMIS Committee will engage in the following activities in support of the HMIS:

A) Assist with determining the guiding principles and vision for the HMIS Program, including strategic planning.
B) Assist with expanding HMIS participation and reducing reliance on 'legacy' databases, including: coordination of resources, coordination of data integration, and determination of policies and procedures.
C) Advise on governing policies and procedures for the HMIS Program.
D) Review and provide input on the HMIS cost structure.

E) Evaluate and propose modifications to HMIS program priorities, including scope of work.

F) Provide input on the minimum data requirements for HMIS participating projects.

G) Define criteria, standards, and parameters, for the release of aggregate data and reports out of the HMIS.

H) Advise on compliance and privacy protection provisions in the administration of the HMIS.

I) Advise on HMIS trainings, including course content and training options.

J) Participate in the selection of the HMIS software used by the CoC.

K) Set and evaluate performance standards for the HMIS Lead agency.

L) Provide input into the RFP and evaluation process of Lead HMIS candidates should the CoC Board decide to put this project out to RFP.

II.   Privacy Standards

A.   *Personally Identifying Information (PII)*

Definition: Any information maintained by or for a member of the Spokane City/County CoC or other Covered Homeless Organization about a homeless client or homeless individual which:

- Identifies, either directly or indirectly, a specific individual;
- Can be manipulated by a reasonably foreseeable method to identify a specific individual; or
- Can be linked with other available information to identify a specific individual (Section 4.1.1, *2004 HMIS Data and Technical Standards*).

Policy: A CHO will enter into the HMIS a required set of data variables for each client, including all universal and program specific data elements, which are specified in the HUD HMIS Data and Technical Standards (see Appendix A for list of Data Elements). Clients that do not agree to have their PII entered must be entered per the prescribed anonymous client process.

Procedure: All HMIS users will be trained in appropriate and accurate procedures for entering PII into HMIS. This training is provided by the HMIS staff within the CHHS Department. HMIS users will abide by the HMIS User Agreement and the consent of the client (HMIS Client Release of Information.))

The HMIS Program Manager reserves the right to de-identify any client at any time and to make the final decision on de-identifying client's being served by multiple agencies at once.

B. HMIS Uses and Disclosures

Policy: A CHO may use or disclose PII from an HMIS under the following circumstances:
- To provide or coordinate services to an individual;
- For functions related to payment or reimbursement for services;
- To provide data for new funding applications;
- To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or
- For creating de-identified PII (Section 4.1.3, *2004 HMIS Data and Technical Standards*).

Procedure: All CHOs must comply with or consult the HMIS Lead Agency before providing any information outside of the above stated standards.

C. Applying the Standard

Policy: All standards described in this manual pertain to any homeless assistance organization that records, uses or processes personally identifying information (PII) for an HMIS and/or identify as a CHO. One exception exists to this policy: any CHO covered under HIPAA is not required to comply with the standards in this manual if the CHO determines that a substantial portion of its PII about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules (Section 4.1.2, *2004 HMIS Data and Technical Standards*).

Procedure: A CHO must comply with HIPAA rules instead of HMIS policies if it determines that a substantial portion of its PII about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules. Exempting HIPAA covered entities from the HMIS privacy and security rules avoids all possible conflicts between the two sets of rules. Requests for exemption must be submitted, in writing, to the HMIS Program Manager.

D. Other Allowable Uses and Disclosures

Policy: Provided below are additional uses and disclosures of information allowable by HUD standards. It should be noted that these additional uses and

disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards). However, nothing in this standard modifies an obligation under applicable law to use or disclose personal information (Section 4.1.3, *2004 HMIS Data and Technical Standards*).

Procedure: A CHO must comply with below standards for additional disclosure to applicable entities.

1. **Legal:**

   Policy: A CHO may use or disclose PII when required by law to the extent that the disclosure complies with and remains within the boundaries of said law.

   Procedure: A CHO must take immediate actions to notify the HMIS Lead Agency about all legal disclosures. By sharing, or releasing, information CHO is acknowledging that is has the right to share or release said information and assumes liability for the shared or released information. If uncertainty exists about the CHO's authority to disclose, or the action is not specified in this document, the CHO must contact the HMIS Program Manager before approving any disclosure.

2. **Health and Safety**

   Policy: A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PII if:
   - The CHO, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
   - The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

   Procedure: A CHO must take immediate actions to notify the HMIS Lead Agency about all legal disclosures. By sharing, or releasing, information CHO is acknowledging that is has the right to share or release said information and assumes liability for the shared or released information.

3. **Abuse, Neglect, Domestic Violence**

   Policy: CHO may disclose PII about an individual whom the CHO reasonably believes to be a victim of abuse, neglect or domestic violence to any government authority (including a social service or protective services agency) if it is authorized by law to receive reports

of abuse, neglect or domestic violence under any of the following circumstances:

- Where such disclosure is required by law and the disclosure complies and is limited to the confines of said law;
- If the individual agrees to disclosure;
To the extent that the disclosure is expressly authorized by statute or regulation; and the CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; OR if the individual is unable to agree because

of incapacity, a law enforcement or other public official authorized to receive the report represents that the PII for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

Procedure: A CHO that makes a permitted disclosure must promptly inform the individual that a disclosure has been or will be made, except if:

- The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
- The CHO would be informing a personal representative (such as a family member or friend), which it reasonably believes is responsible for the abuse, neglect or other injury, and that informing this personal representative would not be in the best interests of the individual (determined by the CHO).

4. Law Enforcement

Policy: A CHO may, consistent with applicable law and standards of ethical conduct, disclose PII to a law enforcement official under any of the following circumstances:

- In response to a request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PII disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics.
- If the official is an authorized federal official seeking PII for the provision of protective services to the President or other

authorized persons OR for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others).

Procedure: A CHO must take immediate actions to notify the HMIS Program Manager about all legal disclosures. By sharing, or releasing, information CHO is acknowledging that is has the right to share or release said information and assumes liability for the shared or released information.

III.   Privacy Requirements

Policy: All CHOs must comply with the baseline privacy requirements described here with respect to: data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability. A CHO may adopt additional substantive and procedural privacy protections that exceed the baseline requirements for each of these areas in its privacy notice. A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PII. When PII is shared between organizations, responsibilities for privacy and security may reasonably be allocated between the organizations (Section 4.2, *2004 HMIS Data and Technical Standards)*.

Procedure: All CHO policies regarding privacy requirements must at a minimum include the criteria following in this document. Additional requirements may be added at the discretion of each CHO.

AL Limits on Data Collection

Policy: A CHO may collect PII only when appropriate to the purposes for which the information is obtained or when required by law. A CHO must collect PII by lawful and fair means and, where appropriate, with the knowledge or consent of the individual (Section 4.2.1, *2004 HMIS Data and Technical Standards*).

Procedure: A CHO must post a copy of the HMIS Client Notice of Uses and Disclosures form at each intake desk (or comparable location) that explains generally the reasons for collecting any and all information. Data allowable includes all HUD mandated data as well as any other data deemed necessary and approved by the CHO which complies with federal regulations and the policies and procedures of this document.

Additional Privacy Protections

Policies and Procedures Manual

1. Client Confidentiality

Policy: The CHO will ensure the confidentiality of all client data. No identifiable client data will be entered into the HMIS without client consent, and no identifiable client data will be shared outside of the limits of that consent or applicable law.

Procedure: Access to client data will be tightly controlled using security technology and restrictive access policies. Only individuals authorized to view or edit individual client data will have access to that data.

2. Informed Consent

Policy: CHOs will collect and retain signed client consent forms before any client data will be entered into the HMIS. CHO staff will thoroughly explain the client consent to each client.

Procedure: Client consent forms must be completed with each individual or household accessing services before any information is entered into the HMIS. Consent forms should be stored in a secure place and made available to the HMIS Lead Agency upon request. Storing the consent form in the HMIS, via the import feature in the HMIS for client document storage, is allowable.

3. Additional User Privacy Measures

Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

- Restricting collection of personal data, other than required HMIS data elements;
- Obtaining oral or written consent from the individual for the collection of personal information from the individual or from a third party (Section 4.2.1, *2004 HMIS Data and Technical Standards*).

Procedure: All additional privacy measures must comply with federal, state, and local, regulations and the policies and procedures of this document. Prior authorization from the HMIS Program Manager, in writing, is required prior to implementing any additional privacy measures.

B. Required Data Collection

Policy: CHOs will collect all required sets of data variables for each client as determined by HUD HMIS Data and Technical Standards, state and local funder requirements, and the HMIS Committee.

Procedure: Copies of all relevant data collection guidelines, training aids, and data collection templates, will be posted to www.spokanehmis.org. The HMIS Lead Agency will send out updates to HMIS users--via email and regularly offered training—on changes, best practices, and other information related to data collection.

C. Appropriate Data Collection

Policy: PII collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PII should be accurate, complete and timely. HMIS users will only collect client data relevant to the delivery of services to people experiencing a housing crisis, (Section 4.2.2, *2004 HMIS Data and Technical Standards*) or as determined by the HMIS Lead Agency.

Procedure: Users will refer to policies outlined in the Data Quality Plan for timelines, accuracy and completeness. Users will ask the HMIS Lead Agency System for any necessary clarification of appropriate data collection.

D. Privacy Notice -- Identifying Purpose and Use Limitation

Policy: A CHO must specify in its privacy notice the purposes for which it collects PII and must describe all uses and disclosures. A CHO may use or disclose PII only if the use or disclosure is allowed by this standard and is described in its privacy notice (Section 4.2.3, *2004 HMIS Data and Technical Standards*).

Procedure: Except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards, all uses and disclosures are permissive and not mandatory. Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law. A CHO must take immediate actions to notify the HMIS Lead Agency about all legal disclosures.

E. Anonymous Clients

Rationale: Anonymous clients in HMIS negatively affect data quality for the

Annual Homeless Assessment Report (AHAR) and other HUD reports. HUD does allow for anonymous clients, but they also count that data as missing, and

HUD funding is increasingly being tied to data quality. There is certainly a need to accommodate clients who need services, but who do not feel comfortable sharing their personally identifying information in HMIS. Having a clear understanding of the privacy policies and laws is a necessity when explaining to clients what purpose their data fills and how it is protected.

Policy: The CHO will ensure all clients are fully educated on their rights **and** the benefits to their identifiable information being entered into the HMIS.

Procedure: Prior to entering client data into the HMIS, the client will be presented with a copy of the current release of information document and posted privacy notice. The CHO will make every effort to explain the conditions in the release of information document, the potential risks and benefits to participation in the HMIS, and answer any questions the client might have.

F. Ethical Data

Policy: Data contained in the HMIS will only be used to support the delivery of homeless and housing services within the CoC (WA502). Each HMIS User will affirm the principles of ethical data use and client confidentiality contained in this document.

Procedure: All HMIS users will sign an HMIS User Agreement before being given access to the HMIS. Any individual or CHO misusing, or attempting to misuse HMIS data will be denied access to the database, and his/her/its relationship with the HMIS will be terminated.

G. Termination

Policy: All HMIS users and CHOs are subject to the privacy and confidentiality terms outlined in this document as well as the federal regulations in the HUD Data and Technical Standards and as stated in the Partner Agency Agreement. At any point, if a breach of rules and/or policies occurs the user may be penalized by loss of access to HMIS and may be liable for civil and/or criminal penalties under federal and state law.

Procedure: The CHO or HMIS User shall inform the HMIS Lead Agency in a timely manner of any breach to the privacy and security policies outlined in this document, the Partner Agency Agreement, the HMIS User Agreement, or the

HUD Data and Technical Standards. The HMIS Program Manager will investigate the issue and determine a proper course of action for correction. If a permanent resolution is unforeseen or the HMIS Program Manager deems it necessary, a CHO and/or user termination may occur:

- The Partner Agency will be notified in writing of the intention to terminate their participation in the HMIS.
- The HMIS Program Manager will revoke access of the HMIS User or CHO staff to the HMIS.
- The HMIS Program Manager will keep all termination records on file.

Voluntary Termination

Policy: Should the CHO or HMIS User decide not to comply with the rules and policies of this document, the Partner Agency Agreement, HMIS User Agreement, and regulations in the HUD Data and Technical Standards, for any reason, they may voluntarily terminate their user agreement.

Procedure: The CHO must use the following measures to terminate participation in the:

- The CHO or HMIS User shall inform the HMIS Program Manager in writing of their intention to terminate their agreement to participate in the HMIS.
- The HMIS Program Manager will inform partners and any other relevant parties of the change.
- The HMIS Program Manager will revoke access of the CHO and/or HMIS User in the HMIS.
- The HMIS Program Manager will keep all termination records on file.

H. Openness and Disclosures

Policy: A CHO must publish a privacy notice describing its policies and practices for the processing of PII and must provide a copy of its privacy notice to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page. A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. (Section 4.2.4, *2004 HMIS Data and Technical Standards*).

Procedure: All amendments to the privacy notice must be consistent with the requirements of these privacy standards. A CHO must maintain permanent

documentation of all privacy notice amendments. Copies of the current privacy notice must be available to all clients, including a sign stating the availability of its privacy notice to any individual who requests a copy. In addition, CHOs who receive federal financial assistance shall provide required information in languages other than English that are common in the community, if speaker of these languages are found in significant numbers and come into frequent contact with the program. *CHOs are also reminded that they are obligated to provide reasonable accommodations for persons with disabilities throughout the data collection process.

*Note: This obligation does not apply to CHOs who do not receive federal financial assistance and who are also exempt from the requirements of Title III of the Americans with Disabilities Act because they qualify as ''religious entities'' under that Act.

Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:
- Giving a copy of its privacy notice to each client on or about the time of first data collection.
- Adopting a policy for changing its privacy notice that includes advance notice of the change, consideration of public comments, and prospective application of changes (Section 4.2.4, *2004 HMIS Data and Technical Standards*).

Procedure: All additional privacy protections must remain consistent with current HUD requirements and be present on the privacy notice.

I. Access and Correction

Policy: A CHO must consider any request by an individual for correction of inaccurate or incomplete PII pertaining to the individual. A CHO can reject repeated or harassing requests for access or correction (Section 4.2.5, 2004 HMIS Data and Technical Standards).

Procedure: In its privacy notice, a CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PII:

- Information compiled in reasonable anticipation of litigation or comparable proceedings;
- Information about another individual (other than a health care or homeless

provider);

- Information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or
- Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial and make it available to the HMIS Lead Agency upon request

Below are the different parties' access levels to data and sharing capabilities. Any additional questions or concerns should be discussed with the HMIS Program Manager.

1. Covered Homeless Organization

Policy: CHOs will have access to retrieve any individual and aggregate data entered into the HMIS entered by the CHO. When generating reports, users will be able to generate data from any records entered by the CHO or that the CHO has permission to use.

Procedure: the HMIS is an 'open system', meaning that a signed HMIS Client Release of Information form must be signed by each client in order for personally identifiable information to be entered All client acknowledgement of data collection and consent to share data forms used by CHOs must indicate that the data entered into the HMIS is viewable by all users of the system.

2. HMIS Lead Agency

Policy: The HMIS Lead Agency will have access to retrieve all data in the HMIS. Staff will not access individual client data for purposes other than maintenance, checking for data integrity, or other relevant business needs. Client data will only be reported in aggregate form.

Procedure: The HMIS Lead Agency staff will be responsible for ensuring that no individual client data is retrieved for purposes other than

maintenance and performing data quality checks.

3. Client

Policy: Any client will have access on demand to view, or keep a printed copy of, their own records contained in the HMIS. All requests for client information will follow agency policy guidelines for release of information. The client will also have access to a logged audit trail of changes to those records. No client shall have access to another client's records in the HMIS.

*Procedure***:** A client will submit an oral or written request to a case manager, at the CHO that collected the data, requesting access to their records in the HMIS. The case manager, or any available staff person with access, will verify the client's identity and print all requested information. The case manager can also request a logged audit trail of the client's record from the HMIS Lead Agency. The HMIS Lead Agency will provide the requested audit trail information to the requesting case worker electronically for dissemination to the client requesting the data.

4. Public

Policy: The HMIS Lead Agency staff, on behalf of the HMIS Committee, will address all requests for data from entities other than CHOs or clients. No individual client data will be provided to any group or individual that is neither the CHO, which entered the data, nor the client without proper authorization or consent.

Procedure: All requests for data from anyone other than a CHO or client will be directed to the HMIS Lead Agency staff. As part of the HMIS Program Manager's regular employment functions, periodic public reports about homelessness and housing issues will be published and posted electronically to the HMIS Lead Agency's website at: www.spokanehmis.org. No PII data will be released in any of these reports.

5. Inter-Agency Data Sharing

Policy: All client data entered into the HMIS, except Case Notes and

records restricted to the entering User/CHO, is viewable by all users and CHOs that are party to the HMIS Partner Agency Agreement.

Procedure: All client acknowledgements of data collection and consent to share data forms used by CHOs must indicate that the data entered into the HMIS is viewable by all users of the system

6. Access to Physical Database

Policy: No one will have direct access to the HMIS database unless explicitly given permission by the HMIS Program Manager.

Procedure: In contract with the HMIS Lead Agency, Eccovia Solutions, Inc. will monitor access of the database server and employ security methods to prevent unauthorized database access.

7. On-Site Review

Policy: The HMIS Lead Agency may perform annual on-site reviews at each CHO of data, security, and privacy, processes related to the HMIS.

*Procedure***:** The CHO will be provided advance notice before each onsite review, a list of the documents or processes that are being reviewed, key staff needed to complete the review, and expectations regarding outcomes.

J. *Accountability*

Procedure: Each CHO must develop and maintain a written copy of procedures for accepting and considering questions or complaints. This must be accessible to all staff members and updated as needed to comply with all HUD regulations. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice (Section 4.2.6, 2004 HMIS Data and Technical Standards).

Additional Protections
Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements. Additional corrections

include but are not limited to:

- Establishing a method, such as an internal audit, for regularly reviewing compliance with its privacy policy;
- Establishing an internal or external appeal process for hearing an appeal of a privacy complaint or an appeal of a denial of access or correction rights; and/or
- Designating a chief privacy officer to supervise implementation of the CHO's privacy standards.

Procedure: Any additional privacy protections should comply with all federal HUD HMIS Data and Technical Standards and policies in this document. Additional protections must be written out in each CHO's policies and procedures documents.

K. Client Grievance

Policy: Clients will contact the CHO with which they have a grievance for resolution of HMIS problems. CHOs will report all HMIS-related client grievances to the HMIS Lead Agency.

Procedure: Clients will bring HMIS complaints directly to the CHO with which they have a grievance. CHOs will provide a copy of the HMIS Policies and Procedures Manual upon request, and respond to the client grievance. CHOs will send email notification to the HMIS Lead Agency of any HMIS-related client grievance and the outcome. The HMIS Lead Agency staff will record all grievances and will report these complaints to the HMIS Committee.

Policy: If the client is not satisfied with the results of the grievance with the CHO, the client may contact the HMIS Lead Agency staff for further assistance.

Procedure: Clients bringing HMIS complaints to the HMIS Lead Agency will be provided a copy of the HMIS Policies and Procedures Manual upon request. The HMIS Lead Agency staff will work to resolve the client grievance, consulting with the CHO as necessary.

L. User Grievance

Policy: Users will contact the HMIS Lead Agency with any grievance regarding HMIS. The HMIS Lead Agency will report all HMIS-related user grievances to the HMIS Committee for review and resolution.

Procedure: Users will bring HMIS complaints directly to the HMIS Lead Agency. The HMIS Lead Agency will provide a copy of the HMIS Policies and Procedures Manual upon request, and respond to any user issues. The HMIS Lead Agency will notify the HMIS Committee of any HMIS-related user grievance. The HMIS Lead Agency will record all grievances and review these complaints with the HMIS Committee.

IV. Security Standards

A. System Security

Policy: A CHO must apply system security provisions to all the systems where personally identifying information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mainframes and servers (Section 4.3.1, 2004 HMIS Data and Technical Standards).

Procedure: Each CHO must apply and maintain security provisions in the form of virus protection, firewalls, and other provisions listed below in this section to ensure the confidentiality of its clients.

1.   Additional Security Protections

*Policy***:** A CHO may commit itself to additional security protections consistent with HMIS requirements by applying system security provisions to all electronic and hard copy information that is not collected specifically for the HMIS. A CHO may also seek an outside organization to perform an internal security audit and certify system security (Section 4.3.1, 2004 HMIS Data and Technical Standards).

Procedure: Additional security protections may be utilized as each CHO believes necessary, but must be compliant with HMIS requirements.

2.   Hardware/Software Requirements

Policy: CHOs will provide their own computer and method of reliably connecting to the Internet, and thus the HMIS.

Procedure: It is the responsibility of the CHO to provide a computer and connection to the Internet. If desired by the CHO, the HMIS Program Manager will provide advice as to the type of computer and connection.

3. Data Access Location

*Policy***:** Users will ensure the confidentiality of client data, following all security policies in this document and adhering to the standards of ethical data use, regardless of the location of the connecting computer.

Procedure: All Policies and Procedures and security standards will be enforced regardless of the location of the connecting computer.

4. User Access

Policy: Only authorized users will have access to the HMIS via a user name and password. Users will keep their access information confidential.

Procedure:
The HMIS Lead Agency will provide user names and initial passwords to each user upon completion of training and signing of user agreements. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. User names will be unique for each user and will not be exchanged with other users. The sharing of username and passwords will be considered a breach of policy resulting in access being revoked. Agencies will notify the HMIS Program Manager immediately of employee reassignment to non-HMIS job responsibilities or termination so the login can be inactivated within 24 hours of the personnel action. Users not accessing the HMIS within three months may have their login inactivated.

5. Virus Protection

Policy: A CHO must protect systems that access HMIS from viruses by using commercially available virus protection software. It may also commit

itself to additional security measures beyond this standard if in line with HMIS regulations.

Procedure: A CHO must regularly update virus definitions from the virus software vendor. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is accessed.

6. **Firewalls**

Policy: A CHO must protect systems the access HMIS from malicious intrusion behind a secure firewall. It may also commit itself to additional security measures beyond this standard if in line with HMIS regulations.

Procedure: Each CHO must maintain its own up to date firewall, however, 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 of the organization.

7. **User Licenses**

Policy: User licenses are controlled by the HMIS Lead Agency regardless of program access.

Procedure: Licenses are assigned once training is completed successfully.

8. **HMIS User Agreements**

Policy: Each User will sign an HMIS User Agreement before being granted access to the HMIS.

Procedure:
Each year, the HMIS Lead Agency will instruct HMIS users on the process for completing the annual privacy training. These instructions will be sent to HMIS users via email.

The annual privacy training will be followed by a quiz that tests users on their understanding of Spokane City/County CoC HMIS privacy and security issues, policies, and requirements. All users will be required to

pass the quiz in order to maintain access rights to the HMIS.

Users who do not attend the required training and/or fail the quiz will have their accounts suspended until compliance is achieved.

9. HMIS Partner Agency Agreement

Policy: Each agency participating in the Balance of State HMIS will sign the HMIS Partner Agency Agreement before any data may be entered for its clients. This agreement will be reviewed annually.

Procedure: Each year, the HMIS Program Manager will review the HMIS Partner Agency Agreement with the HMIS Committee for possible revision.

An original signed copy of the Agency Agreement must be sent directly to the HMIS Program Manager. An electronic copy will be returned to each signatory.

Any agency that fails to send the updated Agency agreement by the date specified in the instructions will lose access to HMIS at the user level until the agreement is received.

10. Training

Policy: All users must be trained by the HMIS Lead Agency and sign an HMIS User Agreement prior to receiving a login to the HMIS. Also all users must complete an Annual Privacy Training and renew any agreements in order to maintain access to the HMIS.

Procedure: New or current users can sign up for HMIS training by registering through the HMIS Lead Agency website: www.spokanehmis.org. HMIS Lead Agency staff will provide training to all new users.

11. Data Retrieval

Policy: Users will maintain the security of any client PII data extracted from the database and stored locally, including all data used in reporting. Users will not electronically transmit any PII client data across

a public network.

Procedure: PII data extracted from the database and stored locally will be stored in a secure location and will not be transmitted outside of the private local area network. Security questions will be addressed to the HMIS Program Manager.

B. Hard Copy Security

Policy: A CHO must secure any paper or other hard copy containing PII that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms. CHO may commit itself to additional security protections consistent with HMIS requirements by applying hard copy security provisions to paper and hard copy information that is not collected specifically for the HMIS (Section 4.3.2, 2004 HMIS Data and Technical Standards).

Procedure: A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PII when the hard copy is in a public area. When CHO staff is not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location.

C. Physical Access

Policy: A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff is not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. A CHO may commit itself to additional security protections consistent with HMIS requirements.

Procedure: A CHO must take steps to secure each computer by automatically turning on a password protected screen saver when the workstation is temporarily not in use. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system.

1. **CHO Technical Support Requirements**

Policy: CHOs will provide their own technical support for all hardware and software used to connect to the HMIS.

Procedure: CHOs will provide technical support for the hardware, software and Internet connections necessary to connect to the HMIS according to their own organizational needs.

V.   Data Quality

A. Data Entry

Policy: HMIS users and CHOs will be responsible for the accuracy of their data entry.

Procedure: The CHO must maintain standards for periodically checking data for completeness, accuracy and timeliness. The HMIS Lead Agency maintains Data Quality Standards to help all CHOs manage the monitoring of their data quality. CHO staff will perform regular data quality checks on the data entered into the HMIS using the processes identified in the HMIS Data Quality Plan. When patterns of error have been discovered, users will be required to correct the data, data entry processes (if applicable) and will be monitored for compliance.

B. Data Quality Plan

Policy: The Data Quality Plan, designed by the HMIS Lead Agency in collaboration with the HMIS Committee, is the official document pertaining to all data quality measures including but not limited to accuracy, completeness, and timeliness. This should be referenced for all data quality standards. Any questions about materials in this document or items that are unclear should be addressed with the HMIS Program Manager.

Procedure: The Data Quality Standards should be referenced and followed for all data quality procedures. Each CHO must retain copies of this document and have available for all relevant staff members. If questions are left unaddressed, they should be brought to the attention of the HMIS Lead Agency in a timely manner.