Spokane City/County CoC (WA502) Homeless Management Information System (HMIS) Policies and Procedures Manual

Overview

The Spokane Continuum of Care (CoC) develops policies and procedures to guide participation in and access to the local Homeless Management Information System (HMIS). This manual is intended to protect the confidentiality of personal information entered into the system and to establish clear standards for privacy, security, and the responsible use and sharing of data. All practices outlined in the manual align with federal regulations set by the Department of Housing and Urban Development (HUD) and comply with applicable state laws. While the manual provides important guidance for agencies in their day-to-day operations, it does not replace or override any federal or state regulations. Each agency remains responsible for maintaining its own compliance with all relevant laws, including the Health Insurance Portability and Accountability Act (HIPAA), when applicable.

Table of Contents

I. Roles and Responsibilities

A. Community, Housing, and Human Services Department (CHHS): the HMIS Lead Agency

The Community, Housing, and Human Services (CHHS) Department is the HMIS Lead agency and is responsible for system administration and project management of the CoC's HMIS database for WA-502.

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

- Respond to CoC and HMIS Committee concerns and needs.
- Oversee the day-to-day administration of HMIS.
- Work with chosen software vendor to ensure system integrity and availability.
- Provide guidance on issues, including ethics and client confidentiality.
- Secure and manage contracts with the software vendor and ongoing communications.
- Provide staffing and a budget for operation of the HMIS.
- Provide user training to participating agencies on all funder and CoC guidelines and requirements for the collection and entry of data.
- Educate the CoC and HMIS Committee leadership to enhance their participation in, and understanding of, the HMIS Program.
- Provide technical support to participating agencies. Maintain knowledge about respective program components and data usage in order to guide end users on program design to ensure the most efficient and accurate data is collected.
- Regularly review data quality and related system metrics and provide reports to the HMIS Committee for review.
- Monitor HMIS participating agencies to ensure compliance with established HMIS policies and procedures. Report violations to the HMIS Committee.
- Staff the HMIS Committee and support the CoC Subcommittees and Workgroups.

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

The Spokane City/County CoC Governance Board will provide oversight of the HMIS Program and support the operations of in the following ways:

- Promote and prioritize HMIS participation by requiring compliance for funding and positioning HMIS as the primary data repository for all local agencies.
- Regularly review data quality and other reporting updates submitted by the HMIS Committee.
- Regularly monitor the HMIS Lead and support their oversight of participating agencies to ensure compliance. Ensure that all CoC participating agencies work with HMIS Lead staff to maintain accurate data in the system and to meet federal, state, and local reporting requirements.

C. Covered Homeless Organization (CHO)

A Covered Homeless Organization (CHO) or 'Agency' (including all its employees, volunteers, affiliates, contractors, and associates) is any agency that accesses HMIS, the client records it contains, or uses information, including Protected Personal Information (PPI) of clients experiencing homelessness or those at risk of experiencing homelessness (Section 4.1.1, *2004 HMIS Data and Technical Standards*).

Each agency participating in the HMIS must have an active HMIS Agency Partner Agreement (APA). Agency Partner Agreements must be renewed every two years on the anniversary of their activation. It is the responsibility of the CHO to monitor the expiration date and ensure a new APA is in place to retain HMIS access.

All Contributing HMIS Organizations (CHOs) that participate in the HMIS must follow the policies and procedures outlined in this manual and in the HMIS Partner Agency Agreement. CHOs that have signed the agreement will be granted access to the HMIS database through trained HMIS users (see Section D: HMIS Users). CHOs are responsible for communicating any needs, questions, or issues related to the CoC's HMIS Lead.

Each CHO must develop and maintain a written copy of procedures for accepting and considering questions or complaints related to existing privacy and security policies. 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 that access client's records (including employees, volunteers, affiliates, contractors and associates) to sign annually 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).

Each CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to undergo (annually or otherwise) formal training in privacy requirements, including those outlined in this document for HMIS.

A CHO may, in its privacy notice, commit those who access clients' records to additional privacy protections consistent with HMIS requirements. Additional requirements may include, but are not limited to:

- Establishing a method, such as an internal audit, for regularly reviewing compliance with its privacy policy.
- Designating a staff member to supervise implementation of the CHO's privacy standards.

Each CHO is responsible for providing its own hardware and connectivity for accessing HMIS. These systems must comply with the security standards, and best practices outlined in this manual, as well as (Section 4.3, 2004 HMIS Data and Technical Standards).

D. HMIS Users

Any individual who uses and views HMIS must have a signed HMIS User Agreement on file and abide by all policies and procedures in this Manual, HMIS User Agreement, and other standards and practices as adopted by the HMIS Lead and/or the HMIS Committee. If a user changes employment or begins working with a different participating organization, they must complete a new HMIS User Agreement specific to that organization before accessing the system.

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. Only authorized users will have access to the HMIS via a username and password.

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 and receive aggregate reporting from users they oversee will be required to receive HMIS training.

Directors and managers are responsible for notifying the HMIS Lead Agency to deactivate 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 Lead Agency reserves the right to revoke and/or reinstate a user at any time.

E. HMIS Committee

The CoC will have an HMIS Advisory Committee to provide community feedback on HMIS implementation related activities and issues. The HMIS Committee will engage in the following activities in support of the HMIS:

- Assists with determining the guiding principles and vision for the HMIS Program, including strategic planning and the administration and execution for HMIS.
- Assists with expanding HMIS participation, coordination of resources, coordination of data integration, and determination of policies and procedures.
- Reviews and proposes the minimum data requirements for HMIS participating projects.
- Defines criteria, standards, and parameters, for the release of aggregate data and reports out of the HMIS.
- Creates and ensures compliance with the provisions in the Privacy and Security Plan.
- Advises on HMIS trainings, including course content and training

options.
- Participates in the selection of the HMIS software used by the CoC.
- Sets and evaluates performance standards for the HMIS Lead agency.

Provides input to the RFP and evaluation process of Lead HMIS candidates or software should the CoC Board decide to put this project out to RFP.

II. Privacy and Security Plan

A. Protected Personal Information (PPI)

Protected Personal Information (PPI) is defined *as* any information maintained by or for a member of the Spokane City/County CoC or other Covered Homeless Organization (CHO) about a homeless client or homeless individual which:

- Identifies a specific individual either directly or indirectly;
- 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*).
- In small populations and certain programs, a single data point can be enough to identify an individual and can therefore be considered PPI.

All HMIS users must complete training provided by the HMIS Lead and follow the HMIS User Agreement as well as the consent provided in the client's signed HMIS Release of Information. All staff, including contract, part time, and internship staff, from any participating CHO must accurately enter all required client data, including universal and program-specific elements as outlined in this document, including HUD and locally determined UDE's. Clients who do not consent to sharing their PPI will be entered using the anonymous client process.

Personal Identification Number (PIN), defined as a permanent and unique number automatically generated by the HMIS application, which is unique to each client, may be disclosed between a CHO and the HMIS Lead Agency in the performance of contracted services. In all other

circumstances a Personal Identification Number is considered PPI.

The HMIS Lead Agency reserves the right to make a client anonymous at any time and to make the final decision on anonymous clients being served by multiple agencies at once.

B. HMIS Uses and Disclosures

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 may use or disclose PPI from an HMIS under the following circumstances:

- To provide or coordinate services to an individual in accordance with their signed consent;
- If compelled by legal action or court order;
- To carry out administrative functions, including but not limited to legal, audit, personnel, oversight, and management functions;
- For creating de-identified PPI (Section 4.1.3 and Section 4.2.3, 2004 HMIS Data and Technical Standards);
- A PIN may be disclosed for functions related to payment or reimbursement for services;
- In the event that datapoints or values must be preserved for data quality or analysis, values must be hashed or otherwise rendered anonymous before any data can be shared.

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

CHO’s may be obligated to share the information (including PPI) about the individual:

- With the individual (first party),
- As required by law,
- As part of necessary disclosures to ensure that privacy and security

rules and funding requirements are being (e.g. audits or oversight, like desk monitorings).

Otherwise, a CHO may only share information about the individual (first party) if the individual/client provides consent, and as provided for in the following CHO Access levels:

1. Covered Homeless Organization

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 by MOU, Data Sharing Agreement, or other formal partnership with another CHO.

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

The HMIS Lead Agency will have access to retrieve all data in the HMIS. The HMIS Lead Agency staff shall be responsible for investigating and correcting any breach of the data use and privacy policies as outlined in this manual, or state and federal statutes.

3. Public

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 unless required to do so by legal obligation. All requests for data from anyone other than a CHO or client will be directed to the HMIS Lead Agency staff. No PPI data will be released in any of these reports.

On behalf of the CoC and HMIS committee, Lead agency staff shall facilitate the creation and distribution or publication of the yearly, periodic and one-time reports on homelessness, housing and other

system information.

4. Inter-Agency Data Transparency

All client data entered into the HMIS is viewable by all users and CHOs that are covered by HMIS Partner Agency Agreements.

5. Access to Database

The HMIS vendor will monitor access to the database server and employ security methods to prevent unauthorized database access.

6. On-Site Review

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

For any additional questions or concerns, please contact the HMIS Lead Agency.

C. Applying the Standard

All standards described in this manual pertain to any homeless assistance organization that records, uses, or processes protected personal information (PPI) for a HMIS and/or identifies as a CHO. If a CHO is a HIPAA covered entity as defined by 45 CFR 160 and 164, the CHO is required to follow HIPAA regulations which supersedes the above stated standards and the 2004 HMIS Data and Technical Standards (Section VII, 2004 HMIS Data and Technical Standards).

D. Other Allowable Uses and Disclosures

Additional uses and disclosures are permitted as detailed below and in Section 4.1.3 of the 2004 HMIS Data and Technical Standards.

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).

A CHO must comply with below standards for additional disclosure to applicable entities. By sharing, or releasing, information CHO is acknowledging that it 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 Lead Agency before approving any disclosure.

1. Legal:

A CHO may use or disclose PPI when required by law to the extent that the disclosure complies with and remains within the boundaries of said law. A CHO must take immediate actions to notify the HMIS Lead Agency about all legal disclosures.

2. Health and Safety:

A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PPI 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.

3. Abuse, Neglect, Domestic Violence:

A CHO may disclose PPI about an individual whom the CHO reasonably believes to be a victim of abuse, neglect, or domestic violence to any government authority (including but not limited to 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 PPI 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.

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:

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

- In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
- If the law enforcement official makes a written request for protected personal information that:
    1) Is signed by a supervisory official of the law enforcement agency seeking the PPI;
    2) States that the information is relevant and material to a legitimate law enforcement investigation;
    3) Identifies the PPI sought;
    4) Is specific and limited in scope to the extent reasonably

practicable in light of the purpose for which the information is sought; and
5) States that de-identified information could not be used to accomplish the purpose of the disclosure.

- If the CHO believes in good faith that the PPI constitutes evidence of criminal conduct that occurred on the premises of the CHO;
- In response to a request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person, the PPI 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 PPI for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

5. Academic Research Purposes:

A CHO may use or disclose PPI for academic research conducted by an individual or institution that has a formal relationship with the CHO if the research is conducted either:

- By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the CHO; or
- By an institution for use in a research project conducted under a written research agreement approved in writing by a program administrator designated by the CHO. A written research agreement must:
  1) Establish rules and limitations for the processing and security of PPI in the course of the research;
  2) Provide for the return or proper disposal of all PPI at the conclusion of the research;

3) Restrict additional use or disclosure of PPI, except where required by law; and
4) Require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board, or other applicable human subjects' protection institution.

If the information being used in the course of the research is coming from, or being obtained through HMIS, each party involved in the research agreement must have separate agreements with the HMIS Lead, and the HMIS committee must be informed of the extent of the activities.

III. Privacy Requirements

All CHOs must at minimum comply with the baseline privacy requirements described in the 2004 HMIS Data and technical standards as well as state law, including RCW 43.185C.180. In addition, all CHOs must comply with all applicable federal, state, and local laws that require additional confidentiality protections. A CHO may adopt additional policies, so long as they do not conflict, or decrease the protections as described below. A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PPI. When PPI is shared between organizations, responsibilities for privacy and security must be allocated between the organizations (Section 4.2, *2004 HMIS Data and Technical Standards)*.

Selected sections of the 2004 HMIS Data and Technical Standards are printed below, these are not the full text of the guidelines.

A. Limits on Data Collection

A CHO may collect PPI only when appropriate to the purposes for which the information is obtained or when required by law. A CHO must collect PPI by lawful and fair means and, where appropriate, with the knowledge or consent of the individual (Section 4.2.1-2, *2004 HMIS Data and Technical Standards*). HMIS users will only collect client data relevant to

the delivery of services to people experiencing a housing crisis.

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, including PPI. Data allowable includes all HUD mandated data as well as any other data deemed necessary and approved by the CoC Board which complies with federal regulations and the policies and procedures of this document. A CHO may collect additional data elements in order to comply with funding requirements so long as the additional elements are relevant to the service being provided and comply with federal regulations and this document.

Additional Privacy Protections:

1. Client Confidentiality

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. 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

RCW 43.185C.180 (a) Personally identifying information about homeless individuals for the Washington homeless client management information system may only be collected after having obtained informed, reasonably time limited (i) written consent from the homeless individual to whom the information relates, or (ii) telephonic consent from the homeless individual, provided that written consent is obtained at the first time the individual is physically present at an organization with access to the Washington homeless client management information system.

Safeguards consistent with federal requirements on data collection must be in place to protect homeless individuals' rights regarding their personally identifying information.

Consent may be obtained via signature in person (wet-ink) or through digital means, so long as those means comply with the U.S. Electronic Signatures in Global and National Commerce (E-Sign) Act

and the Uniform Electronic Transactions Act (UETA), and RCW 1.80.060, and they collect:

- The individual's intent to sign or agree
- Clear attribution and identity
- Integrity of the agreement being signed
- Notice and opportunity to review
- Record retention and accessibility

Affirmative, informed consent by the client must be collected by the CHO prior to entry of that client's information into HMIS. Each client should have the opportunity to thoroughly review the client consent and, as needed, CHO staff should explain the meaning of that consent and their rights to each client.

Documentation of client consent shall be securely retained by the CHO and made available to the HMIS Lead Agency upon request. Consent forms may additionally be stored in HMIS via the import feature in the HMIS for client document storage.

A CHO has the option to inquire if the client has been entered into the system at some point in the past to ensure that duplicated information is not being entered. A client's written consent should be recorded for the cross-collaboration of CHOs.

3. Additional User Privacy Measures

A CHO can implement extra privacy protections, adding them to their privacy notice if they do so, as long as those additions comply with federal, state, and local regulations and the policies and procedures of this document.

B. Required Data Collection

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 CoC. Copies of all relevant data collection guidelines will be posted on the HMIS Leads website. The HMIS Lead Agency will send out updates to HMIS users and the CoC related to data collection.

C. Anonymous Clients

HUD guidelines and Washington code provide clear standards for clients who, after being informed of their privacy rights, wish to be entered anonymously. It is the responsibility of every CHO and all staff performing data collection and input to make every effort to provide a clear explanation of the purpose of HMIS, the role and limits of client consent, and the conditions of the Release of Information.

D. Ethical Data

Both CHO's and users are responsible for maintaining privacy when collecting, accessing and handling client data. This includes limiting data access, maintaining confidentiality, complying with security policies, respecting and documenting client sharing preferences, and allowing clients to change those preferences. All users must adhere to requirements for data accuracy, legitimate use, and respecting client rights to access their information and file complaints without retaliation. CHO's may not deny services based on a client's HMIS participation.

Any individual or CHO misusing or attempting to misuse HMIS data will be denied access to the database and their relationship with the HMIS will be terminated.

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

A. Users will not access individual client data for purposes other than maintenance, checking for data integrity, or other relevant business needs.
B. 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. All policies and procedures and security standards will be enforced regardless of the location of the connecting computer.
C. Users must be prepared to answer client questions regarding HMIS.
D. Users must faithfully respect client preferences with regard to the entry into and the sharing of client information within HMIS. Users

must accurately record a client's preferences by making the proper designations as to sharing of client information and/or any restrictions on the sharing of client information.

E. Users must allow a client to change his or her information sharing preferences at the client's request.
F. Users must not decline services to a client or potential client if that person refuses to allow entry of information into HMIS or to share their personal information with other agencies via HMIS.
G. The User has primary responsibility for information entered by the User. Information entered into HMIS by a User must be truthful, accurate, complete and timely to the best of User's knowledge.
H. Users will not solicit from or enter information about clients into HMIS unless the information is required for a legitimate business purpose such as to provide services to the client.
I. Users will not use the HMIS database for the violation of any law, to defraud any entity, or to conduct any illegal activity.
J. Upon client written request, Users must allow a client to inspect and obtain a copy of the client's own information maintained within HMIS. Information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding need not be provided to the client.
K. Users must permit clients to file a written complaint regarding the use or treatment of their information within HMIS. Clients may file a written complaint with either the CHO or with the City of Spokane's Community Housing and Human Services (CHHS) Department at 808 W. Spokane Falls Blvd. Spokane, WA, 99201. Clients may not be retaliated against for filing a complaint.

E. Termination

All HMIS users and CHOs are subject to the privacy and confidentiality terms outlined in this document as well as the federal regulations contained in the HUD Data and Technical Standards, as stated in the Agency Partnership Agreement (APA), and by Washington State law. 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.

F. Responsibility to Report

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 Agency Partnership Agreement, the HMIS User Agreement, or the HUD Data and Technical Standards, and Washington State law. The HMIS Lead Agency will investigate the issue and determine a proper course of action for correction. If the HMIS Lead Agency deems it necessary, a CHO and/or user termination may occur and:

- The Partner Agency (CHO) will be notified in writing of any decisions that affect their participation in the HMIS, or actions taken concerning their staff.
- The HMIS Lead Manager shall retain record of all access changes affecting CHOs and users as a result of any investigation.

G. Openness and Disclosures

A CHO must publish a privacy notice (additional policies cannot override or supersede existing privacy requirements and notices, it can only act as an addition to those, if CHO has additional policies) describing its policies and practices for the processing of PPI 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 as well. 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*).

All amendments to the privacy notice must be consistent with the requirements of these privacy standards, all State and Federal privacy regulations. 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 shall provide required information in languages other than English that are common in the community, if speakers 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.

H. Client Data Access and Correction Requests

A CHO must allow an individual to inspect and obtain a copy of their own PPI and records. Access to another individual's PPI is strictly prohibited, unless the requesting party is the custodial parent or legal guardian of that individual. All requests for client information will follow agency policy guidelines for release of information and policies and procedures outlined in this document, as well as applicable Federal and State laws.

A CHO must offer to explain any information that the individual may not understand. A CHO must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information. (Section 4.2.5, 2004 HMIS Data and Technical Standards)

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 PPI:

> (1) Information compiled in reasonable anticipation of litigation or comparable proceedings;
>
> (2) Information about another individual (other than a health care or homeless provider);
>
> (3) 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
>
> (4) Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

A CHO can reject repeated or harassing requests for access or correction. 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 as part of the protected personal information about the individual.

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

(1) Accepting an appeal of a denial of access or correction by adopting its own appeal procedure and describing the procedure in its privacy notice;

(2) Limiting the grounds for denial of access by not stating a recognized basis for denial in its privacy notice;

(3) Allowing an individual whose request for correction has been denied to add to the individual's information a concise statement of disagreement. A CHO may agree to disclose the statement of disagreement whenever it discloses the disputed PPI to another person. These procedures must be described in the CHO's privacy notice; and/or

(4) Providing to an individual a written explanation of the reason for a denial of an individual's request for access or correction.

I. Client Grievance

Clients have the right to raise concerns regarding the privacy, security, or accuracy of their information in the HMIS. Concerns should first be addressed with the CHO, and if unresolved, escalated to the HMIS Lead Agency.

1. Initial Complaint (Grievance):

    - Clients should contact the CHO with which they have a grievance.
    - The CHO must:
        - Acknowledge the complaint.
        - Provide the client a copy of the HMIS Policies and Procedures Manual upon request.
        - Investigate and respond in a timely manner.
        - Document the complaint and outcome.
        - Notify the HMIS Lead Agency via email of the grievance and the outcome.

2. Escalation (Appeal):

    - If a client is dissatisfied with the CHO's response, they may file an appeal in writing with the HMIS Lead Agency.

- The HMIS Lead Agency must:
    - Provide the client a copy of the HMIS Policies and Procedures Manual upon request.
    - Consult with the CHO to assess the issue.
    - Attempt to mediate and resolve the issue fairly.
    - Record the grievance, appeal, and resolution steps.
    - Report all appeals to the HMIS Committee for review and oversight.

IV. Security Standards

These rules apply to any system or location where client data is stored, whether it's inside the HMIS application or elsewhere (including but not limited to agency computers, cloud storage, or hard copies). This section refers to HMIS systems, but applies to any system of collecting, using and maintaining client data. 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. HMIS is a web-based application which requires reliable and secure Internet access.

A CHO may implement other best practice security measures in addition to those listed below, such as:

- Policies that prevent staff from accessing HMIS from personal devices.
- Configuring systems to prevent USB or external drive read/write permissions
- Local machine encryption.
- Policies surrounding the secure transmission and reception of client data between CHOs (such as needed for coordinated entry referrals).
- Policies surrounding secure disposal of drives and machines that have been used to access HMIS, such as though a certified destruction company.

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

1. Protect All Systems with PPI

All CHOs must protect any device or system that stores client information, including but not limited to:

- Desktops, laptops, servers, mainframes
- Network drives, cloud storage
- USB drives or paper files.

2. User Login Requirements

Only authorized users will have access to the HMIS via a username and password. Users will keep their access information confidential.

All digital systems must be protected with a username and password. Passwords must be at least 8 characters long and adhere to these requirements:

- Include upper and lowercase letters, at least one symbol, and at least one number.
- Never include part of the username, system name, or vendor name.
- Not be a dictionary word or simple phrase.
- Users should not be logged in on multiple computers at once.
- Usernames 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.
- Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location.
- Users not accessing the HMIS for 30 days or more will have their login inactivated.

3. Antivirus Software

- All systems with HMIS data and which access HMIS must have active antivirus software.
- It must automatically scan files when opened or downloaded.
- Keep antivirus updated regularly.

4. Use Firewalls

- All systems accessing HMIS must do so through a firewall.
- A central firewall, such as a network or server-side firewall may cover multiple computers.
- Older computers must be updated with secure firewall software.

5. Secure Public Access Systems

If the CHO collects data using public systems (like kiosks or tablets), it must:

- Restrict access using certificates or approved IP addresses.
- Ensure public devices can't reach data that isn't meant to be public.

6. Control Physical Access

- Computers in public areas must be monitored by staff.
- If staff step away, systems must:
    - Log out of HMIS and lock their computer.
    - Lock automatically with a password-protected screen saver.
    - Be shut down for long absences.
- Systems must be stored securely when not in use.
- Access to static systems such as servers must be secured by both two physical locks and digital access controls.
- All Policies and Procedures and security standards will be enforced regardless of the location of the connecting computer.

7. Secure Transfer of Client Data

- Any transfer of Personally Protected Information client data between a CHO and HMIS, or between two CHO's (such as required by coordinated entry) must take place via Secure File Transfer Protocol, HMIS approved encrypted mail.
- If the situation requires, client data may be transferred in secure media, such as an AES encrypted external drive, in which case the password for that drive must be transferred via other secure means.

8. Backups and Disaster Recovery

- If a CHO chooses to back up their own client data, the backups must:
- Meet the same privacy and security and encryption standards.
- Servers and backups maintained by any CHO must be protected from heat, fire, power surges, unauthorized access.
    - It is advised that backups follow the 3-2-1 rule: 1 original, and at least two copies on different media, and the copies should not be kept on the same site.

9. Proper Disposal of Data

- Remove all data from a device or storage media:
    - Media must be sanitized in compliance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization, Special Publication 800-88
- Disposal of physical media or devices containing PII.
    - If disposing of physical storage media, use a bonded shredding or data destruction service.
- If electronic devices containing client data are to be redistributed or repurposed, all storage media such as hard drives must be sanitized or removed.

10. Monitor Your Systems

- Maintain a log of who accesses client data systems and review it regularly.
- Use tools that alert you to:
    - Unauthorized access.
    - Changes to files.
    - Potential security breaches.

11. Hard Copy Security

A CHO must secure any paper or other hard copy containing PPI that is either generated by or for HMIS, including, but not limited to reports, data entry forms, and signed consent forms. CHO must apply security protections consistent with HMIS requirements by applying hard copy security provisions to paper and hard cop information that is not collected specifically for the HMIS (Section

4.3.2, 2004 HMIS Data and Technical Standards). A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PPI 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.

V. Data Quality

A. Data Entry

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

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 (Attachment)

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 Lead Agency. The Data Quality Standards should be referenced and followed for all data quality procedures. Each CHO must retain copies of this document and make it 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.