Ohio BoSCoC and Mahoning County CoC Homeless Management Information System (HMIS) Policies and Procedures Manual

Overview

The Ohio Balance of State Continuum of Care (Ohio BoSCoC) and Mahoning County Homeless Continuum of Care (MCHCoC) have a shared Homeless Management Information System (HMIS) implementation. The CoCs have jointly developed these policy standards and procedures to guide use of HMIS for all End Users and User Agencies. This purpose of this manual is to guide and clarify federal regulations related to HMIS for CoC agencies in their daily operations. It in no way should serve as a substitute for any federal regulations outlined and updated by HUD in its HMIS Data and Technical Standards. All CoC agencies are responsible for maintaining their own compliance with federal regulations as well as any outside applicable regulations such as the Health Insurance Portability and Accountability Act (HIPAA) standards.

Table of Contents

1 Roles and Responsibilities 3

1.1 HMIS System Administrator 3

1.2 Joint HMIS Advisory Committee 3

1.3 HMIS Management Committee 3

1.4 Covered Homeless Organization (CHO) 3

1.5 HMIS End Users 4

1.6 HMIS Agency Administrators 4

2 Privacy Standards 4

2.1 Personally Identifying Information (PII) 4

2.2 HMIS Uses and Disclosures 5

2.3 Applying the Standard 5

2.4 Other Allowable Uses and Disclosures 5

2.5 R minor and R minor Elevated Access and Use 6

3 Privacy Standards 7

3.1 Privacy Requirements 7

3.2 Limits on Data Collection 7

3.3 Additional Privacy Protections 8

3.4 Required Data Collection 8

3.5 Appropriate Data Collection 8

3.6 Data Purge 9

3.7 Privacy Notice - Identifying Purpose, Use Limitation, and Disclosures 9

3.8 Anonymous Clients 10

3.9 Ethical Data 11

3.10 Termination 11

3.11 Access and Correction 11

3.12 Accountability 14

4 Security Standards 15

4.1 System Security 15

4.2 Hard Copy Security 18

4.3 Security Breaches 18

5 Data Quality 19

5.1 Data Entry 19

5.2 Data Quality Plan 19

5.3 Covered Homeless Organization (CHO) Data 19

6 HMIS Participation Fees 20

6.1 HMIS Fees 20

1 Roles and Responsibilities

1.1 HMIS System Administrator

Policy: The Coalition on Homelessness and Housing in Ohio (COHHIO) has been designated as the HMIS System Administrator (called System Administrator, or HMIS System Administrator in this document) for the Ohio BoSCoC and MCHCoC and as such is responsible for system administration and project management of the HMIS.

Procedure: COHHIO will serve as the HMIS System Administrator (referred to in this document as HMIS System Administrator[s] or System Administrator[s]) for the Ohio BoSCoC and MCHCoC HMIS. COHHIO will help agencies to gain access to the database system, strive to ensure high quality use and operation of the HMIS, and provide training and technical assistance to the HMIS participants.

1.2 Joint HMIS Advisory Committee

Policy: The Joint HMIS Advisory Committee serves as the advisory entity for the merged HMIS implementation. More details regarding membership of the Committee and its responsibilities can be found in the Joint HMIS Governance Charter on the Ohio BoSCoC HMIS policies page or the MCHCoC webpage.

1.3 HMIS Management Committee

Policy: The HMIS Management Committee supports the HMIS system administrators in the day-to-day work of managing the merged HMIS implementation. More details regarding membership of the Committee and its responsibilities can be found in the Joint HMIS Governance Charter.

1.4 Covered Homeless Organization (CHO)

Definition: Any organization (including all its affiliates and contractors) that records or uses or processes PII from clients experiencing homelessness or those at risk of experiencing homelessness for an HMIS.

Policy: Any agency participating in the HMIS will abide by all policies and procedures outlined in this manual.

Procedure: Any agency, organization or group who has signed an HMIS Agency Agreement will be given access to the HMIS through trained HMIS End Users (see E. HMIS End Users below).
Procedure: Agencies that operate multiple programs, including those which are not dedicated to serving those experiencing homelessness, must not access or use client-level HMIS data to support activities of another program that is not entering client-level data into the HMIS, unless they have written client permission to do so.
Policy: CHOs are responsible for communicating needs and questions regarding the HMIS directly to the System Administrators.
Procedure: Users at CHOs will communicate needs, issues, and questions to HMIS System Administrators.

1.5 HMIS End Users

Policy: HMIS End Users adhere to policies and procedures in data collection and privacy and security practices, ensure quality, timely data entry, and correct errors as they become known.
Procedure: Any individual who uses Clarity must have a signed HMIS End User Agreement on file with the HMIS System Administrator and abide by all policies and procedures in this Manual.

Procedure: Directors or managers who do not wish to become an HMIS End User but who are ultimately responsible for their agency's HMIS data may attend HMIS trainings as desired and receive aggregate reporting from HMIS End Users they oversee. It is recommended that directors who wish to run reports out of HMIS either obtain an HMIS End User license or ensure their staff are able run and safely transmit reports as necessary. Any director or manager who will see client-level data MUST obtain an HMIS End User license.
Procedure: HMIS End Users must use an email address that is individualized to them for their HMIS End User license management. HMIS End Users cannot use an email address that is generic (e.g., executivedirector@hopehouse.org or casemanager@hopehouse.org) or that is intended to be shared among staff.
Additional details about HMIS End User Agreements and HMIS Agency Administrator Agreements can be found in Section 4.
Procedure: People who received assistance from an HMIS-participating CHO within the Ohio BoSCoC or MCHCoC may not become HMIS End Users until 12 months have elapsed from the end of their receipt of assistance from the CHO. Employees of a CHO who receive assistance from a CHO may, as appropriate, have their HMIS license temporarily suspended while waiting for the 12 months to lapse.

1.6 HMIS Agency Administrators

Policy: Every HMIS Participating Agency must have a designated HMIS Agency Administrator.

Procedure: An Agency Administrator is responsible for ensuring quality, timely data entry; staying knowledgeable about HUD and state funder regulations (such as Ohio Department of Development) as they change; being a point of contact to the System Administrators; notifying a System Administrator of any changes in HMIS End User access to HMIS, program/project information, or bed count data, if applicable; plus all the responsibilities listed for HMIS End Users. Each HMIS Agency Administrator must be an active HMIS End User.
Note: If an Agency Administrator is not assigned, an HMIS End User will assume the responsibilities of the Agency Administrator until one is assigned.

2 Privacy Standards

2.1 Personally Identifying Information (PII)

Definition: Any information maintained by or for a member of the Ohio BoSCoC or MCHCoC or other CHO about a living homeless client or homeless individual which:

- Identifies, either directly or indirectly, a specific individual; including but not limited to Client Name, Date of Birth, Social Security Number, Race, Ethnicity, and Gender.
- 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 (*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.

Procedure: All HMIS End Users will be trained in appropriate and accurate procedures for entering PII into the HMIS. This training is provided by the HMIS System Administrators.

2.2 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 carry out administrative functions, including but not limited to legal, audit/monitoring, personnel, oversight and management functions; or
- For creating de-identified PII

Procedure: All CHOs must consult HMIS System Administrators before providing any information outside of the above stated standards.

2.3 Applying the Standard

Policy: All standards described in this manual pertain to any homeless assistance organization that records, uses or processes personally identifiable information (PII) for the 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.

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.

2.4 Other Allowable Uses and Disclosures

Policy: Under certain circumstances, a CHO may be permitted to disclose or permit the use of HMIS data, per the HUD standards.

Procedure: 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. All other disclosures must first be approved by HMIS System Administrators.

2.4.1 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, in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena.

Procedure: A CHO must take immediate actions to notify an HMIS System Administrator about all legal disclosures. If uncertainty exists about the CHO's authority to disclose, or the action is not specified in this document, the CHO must contact an HMIS System Administrator before approving any disclosure.

2.4.2 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 an HMIS System Administrator about all legal disclosures. If uncertainty exists about the CHO's authority to disclose, or the action is not specified in this document, the CHO must contact an HMIS System Administrator before approving any disclosure.

2.4.3 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 HMIS System Administrators about all legal disclosures. If uncertainty exists about the CHO's authority to disclose, or the action is not specified in this document, the CHO must contact HMIS System Administrators before approving any disclosure.

2.5 R minor and R minor Elevated Access and Use

Background: The Ohio BoSCoC and MCHCoC use the custom reporting platforms R minor (Rm) and R minor elevated (Rme) for system and project-level reporting. Rm is

publicly accessible, contains no client-level data, and does not require log-in to access it. Rme houses more detailed performance reporting along with HMIS data quality reporting and prioritization reports. This site requires a login because more detailed client-level data is shown, such as client unique IDs.

Policy: CHO's will prohibit access to Rme or Rme data for anyone who does not have their own log-in or who has not been granted Rme access permission by the HMIS System Administrators.

Procedure: HMIS End Users do not share their Rme log-in or share view of data from Rme with anyone who does not have their own Rme log-in. The exception to this is for sharing of the Veterans Active List and the Prioritization Report, both of which are housed in Rme, do not have PII, and can be exported out of Rme for purposes of providing data for coordination of permanent housing resources and case conferencing.
Procedure: Rme or Rme data may be shared in meetings of providers where the focus is coordination of services for clients, as outlined in policy II.B. above and in the Privacy Notice.
Procedure: In other meetings not focused on service coordination or where some participants do not have an Rme log-in, Rme may not be displayed and Rme data may not be shared, excluding the Veterans Active List and Prioritization Report noted above.
Procedure: On a case-by-case basis, HMIS System Administrators may grant Rme access to non-HMIS End Users. In these instances, staff should contact HMIS System Administrators to request access. Upon approval by the appropriate CoC, the staff person will be required to sign an Rme Privacy and Confidentiality Agreement.

3 Privacy Standards

3.1 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.

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.

3.2 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.

Procedure: A CHO must post a sign 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.

3.3 Additional Privacy Protections

3.3.1 Client Confidentiality

Policy: The HMIS System Administrators and CHOs 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.

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.

3.3.2 Informed Consent

Policy: CHOs only enter client PII into the HMIS with client consent.

Procedure: CHO staff explain to clients why their data is being collected, who has access to the data in HMIS, and how the data is protected and kept private, as outlined in the posted Privacy Notice (described in section D below).
Procedure: Upon receiving client verbal consent to collect their data and enter into the HMIS, CHO staff sign a form verifying they asked the client for their consent to collect and enter data into the HMIS and that the client consented.

3.4 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.

Procedure: HUD HMIS Data and Technical Standards identify the data elements to be collected for each client contact. These data elements may change as HUD HMIS Data and Technical Standards are revised and updated. For consistency in data collection and more accurate reporting, all HMIS Participating Programs may be held to the most stringent program-specific data collection requirements. The decision to add a data element will be made by the Joint HMIS Advisory Committee, with input from the HMIS Management Committee.

3.5 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 End Users will only collect client data relevant to the delivery of services to people experiencing a housing crisis in the Ohio BoSCoC or MCHCoC.

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

3.6 Data Purge

Policy: COHHIO HMIS must dispose of client PII that is not in current use seven years after the PII was created or last changed.

Procedure: COHHIO HMIS will work with the vendor to dispose of client PII annually based on the criteria outlined in the Homeless Management Information Systems (HMIS); 2004 Data and Technical Standards.

3.7 Privacy Notice - Identifying Purpose, Use Limitation, 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.

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 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, if they receive federal funding. 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.
Procedure: All additional privacy protections must remain consistent with current HUD requirements and be present on the Privacy Notice.

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.

Procedure: A CHO may infer its ability to consented use and disclosure of any item specified in the notice. 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 HMIS System Administrators about all legal disclosures.
Policy: To ensure accurate information is communicated to clients via the HMIS privacy notice, HMIS System Administrators will make available a sample privacy notice for use by all CHOs in the Ohio BoSCoC and MCHCoC.

Procedure: Sample privacy notices are posted on the Ohio BoSCoC and MCHCoC websites.

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 written consent from the individual for the collection of personal information from the individual or from a third party
- Seeking either oral or written consent for some or all processing when individual consent for a use, disclosure or other form of processing is appropriate;
- Agreeing to additional restrictions on use or disclosure of an individual's PII at the request of the individual if the request is reasonable. The CHO is bound by the agreement, except if inconsistent with legal requirements;
- Limiting uses and disclosures to those specified in its privacy notice and to other uses and disclosures that are necessary for those specified;
- Committing that PII may not be disclosed directly or indirectly to any government agency (including a contractor or grantee of an agency) for inclusion in any national homeless database that contains personal protected information unless required by statute;
- Committing to maintain an audit trail containing the date, purpose and recipient of some or all disclosures of PII;
- Committing to make audit trails of disclosures available to the homeless individual; and
- Limiting disclosures of PII to the minimum necessary to accomplish the purpose of the disclosure
- 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

Procedure: Additional privacy protections beyond the baseline requirements are permissible, as exemplified in this policy. Protections should, however, be documented in the Privacy Notice at all times and approved by HMIS System Administrators if potentially beyond reasonable scope of authority.
Procedure: All End User policies must be available to staff members and clients. Changes to Privacy Notices should be given in advance to all clients and employees using a procedure developed by the CHO.

3.8 Anonymous Clients

Rationale: Anonymous clients in HMIS negatively affect data quality for the Longitudinal System Analysis (LSA) and other HUD reports. HUD does allow for anonymous clients; however, anonymous client data is considered missing data and HUD funding is increasingly tied to data quality. There is certainly a need to accommodate clients who need services, but who do not feel comfortable sharing their personally identifiable information in the HMIS. Having a clear understanding of the privacy policies outlined in this Manual is a necessity when explaining to clients what purpose their data fills and how it is protected.

Policy: The CHO's current year (October to September) percentage of anonymous clients not currently fleeing domestic violence shall not exceed 1% of its total clients served during the same period.

3.9 Ethical Data

Policy: Data contained in the HMIS will only be used to support the delivery of homeless and housing services in Ohio BoSCoC and MCHCoC. Each HMIS End User will affirm the principles of ethical data use and client confidentiality contained in this document.

Procedure: All HMIS End Users will sign an HMIS End 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.

3.10 Termination

Policy: All HMIS End 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. At any point if a breach of rules and/or policies occurs the user may be penalized by loss of access and/or participation in the HMIS.

Procedure: The CHO or HMIS End User shall inform an HMIS System Administrator in a timely manner of any breach to the privacy and security policies outlined in this document or the HUD Data and Technical Standards. The HMIS System Administrator will investigate the issue and determine a proper course of action for correction. If a permanent resolution is unforeseen or the HMIS System Administrator 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 System Administrator will revoke access of the HMIS End User or CHO staff to HMIS.
- The HMIS System Administrator will keep all termination records on file.

3.10.1 Voluntary Termination

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

Procedure: The CHO or HMIS End User must use the following measures to terminate participation in the HMIS:

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

3.11 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 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. A CHO can reject repeated or harassing requests for access or correction.

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 must document requests for changes to an individual's PII.
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.
Below are the different parties' access levels to data and sharing capabilities. Any additional questions or concerns should be discussed with the HMIS System Administrator.

3.11.1 Covered Homeless Organization

Policy: CHOs will have access to retrieve any individual and aggregate data entered into the HMIS. When generating reports, HMIS End Users will be able to generate data from any records. All client data entered into the HMIS except Client Case Notes and private records are viewable by all users.

Procedure: The HMIS is a system with shared visibility between all participating providers. Posted HMIS Privacy Notices at CHOs must indicate that the data entered into the HMIS is viewable by all users of the system.

Policy: The HMIS Management Committee may perform on-site reviews at CHOs of data processes related to the HMIS.

*Procedure***:** This review may be done as part of the renewal of the HMIS Agency Agreement or End User Agreements.

3.11.2 HMIS System Administrator

Policy: The HMIS System Administrators will have access to retrieve all data in the HMIS. The HMIS System Administrators will not access individual client data for purposes other than maintenance and checking for data integrity. Any client-level data submitted to the Ohio Human Services Data Warehouse or to other parties for data analysis will be de-identified and/or encrypted. All other HMIS data submitted to funders or published will be aggregated.

Procedure: System Administrators will only publish or submit to funders aggregate data from the HMIS.

3.11.3 Client

Policy: Any client may request to view, or keep a printed copy of, their own records contained in the HMIS.

Procedure: Clients should submit requests for their own client information to the CHO they are seeking data from. CHOs will follow their own policy guidelines for release of information. No client shall have access to another client's records in the HMIS.
*Procedure***:** Upon receipt of a client request for their own data, the case manager, or any available staff person within HMIS access, will verify the client's identity and print PII, as defined by HUD's HMIS Data Standards. This data will be provided to the client by the Agency HMIS Administrator per the CHO's procedures.
Procedure: CHOs are only required to provide clients with their own PII from HMIS, as defined by HUD's HMIS Data Standards.
Procedure: CHO's may decline to provide clients with their own PII from HMIS per the reasons outlined in policy 3.11 above. Additionally, upon responding to an initial request for client's own PII, a CHO may decline to respond to further requests if those requests are duplicative or harassing. CHOs must notify the HMIS System Administrator if they are declining to respond to a client's request for their own PII from HMIS.
Procedure: If the CHO is non-responsive to client requests for their own PII, clients may contact the HMIS System Administrator and/or the respective CoC Director for possible further assistance.
Procedure: PII of minors is not entered into the HMIS without the consent of a parent. In cases where a parent provides consent to share the PII of a minor, but the minor disagrees with that consent, the wishes of the minor to keep their data private will be honored. Upon turning 18, an individual served by a CHO as a minor may choose to begin sharing previously unshared data or to relinquish consent to further sharing of data collected on them in the past. Should the parent of an individual who was served by a CHO as a minor request a copy of that data, COHHIO will obtain consent from the individual before releasing any historical data to their parent.

3.11.4 Public

Policy: The HMIS Management 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 HMIS System Administrators. As part of the HMIS System Administrators' regular employment functions, periodic public reports about homelessness and housing issues in the CoCs may be issued. No PII data will be released in any of these reports.
Procedure: CHO's are not permitted to share individual client data from HMIS with any research or evaluation entity with which they are working unless they request and receive permission from the HMIS System Administrator.

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

Procedure: In contract with COHHIO, Bitfocus will monitor access of the database server and employ security methods to prevent unauthorized database access.

3.12 Accountability

Policy: A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices.

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.

3.12.1 Client Grievance

Policy: CHO's have a procedure to receive and respond to a grievance from a client for resolution of HMIS problems.

Procedure: Clients will bring HMIS grievances 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 client issues. CHOs will send written notice to the HMIS System Administrators of any HMIS-related client grievance. HMIS System Administrators will record all grievances and will report them to the HMIS Management Committee.
Procedure: If the client is not satisfied with the results of the grievance with the CHO, the client may contact HMIS System Administrators for further assistance. Clients bringing HMIS complaints to HMIS System Administrators will be provided a copy of the HMIS Policies and Procedures Manual upon request. HMIS System Administrators will record all complaints and report them to the HMIS Management Committee.

3.12.2 HMIS End User Complaints

Policy: HMIS System Administrators are available to receive and respond to any complaint regarding HMIS from an HMIS End User.
Procedure: HMIS End Users will bring HMIS complaints directly to HMIS System Administrators. HMIS System Administrators will provide a copy of the HMIS Policies and Procedures Manual upon request and respond to any user issues. HMIS System Administrators will record and report all HMIS-related user complaints to the HMIS Management Committee.
Procedure: If the HMIS End User is not satisfied with the results of the complaint with HMIS System Administrators, the user may contact the appropriate CoC Director for further assistance.

3.12.3 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.

4 Security Standards

4.1 System Security

Policy: A CHO must apply system security provisions to all the systems where Personally Identifying Information (PII) is stored, including, but not limited to, a CHO's networks, desktops, laptops, mainframes and servers.

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.

4.1.1 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.

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

4.1.2 Hardware/Software Requirements

Policy: CHOs will provide their own computer and method of 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 System Administrator will provide advice as to the type of computer and connection.

4.1.3 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. All HMIS End Users are prohibited from accessing the HMIS database from any location other than the designated and approved work site.

Procedure: All Policies and Procedures and security standards will be enforced regardless of the location of the connecting computer. All HMIS related data entry will be processed at a designated and approved work site. A System Administrator will provide any additional clarification.

Procedure: 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, 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.
Procedure: A CHO may commit itself to additional security protections consistent with HMIS requirements.

4.1.4 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.

4.1.5 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.

4.1.6 HMIS End User Licenses

Policy: HMIS End User licenses are controlled by HMIS System Administrators regardless of program access.

Procedure: Licenses are assigned once training is completed successfully and HMIS End User Agreements signed.

4.1.7 HMIS End User Agreements

Policy: Each HMIS End User will sign an HMIS End User Agreement before being granted access to the HMIS. HMIS End User Agreements must be updated annually in order to retain access to the HMIS.

Procedure: HMIS System Administrators instruct HMIS End Users on the process for completing the annual privacy training and submitting an HMIS End User Agreement.

4.1.8 HMIS Agency and Agency Administrator Agreements

Policy: Each agency participating in the HMIS signs an HMIS Agency Agreement and HMIS Agency Administrator Agreement before any data may be entered for its clients. These Agreements are updated annually.

Procedure: Each year, System Administrators instruct agencies on the process for completing and submitting an updated HMIS Agency Agreement and HMIS Agency Administrator Agreement to HMIS System Administrators.
Any agency that fails to send the updated Agency Agreements by the date specified in the instructions will lose access to HMIS at the HMIS End User level until the agreement is received.

4.1.9 HMIS End User Access

Policy: Only authorized users will have access to the HMIS via a user name and password. End Users will keep their access information confidential.
Procedure: System Administrators communicate log-in information to each user upon completion of training.

Procedure: User names and passwords are not to be written down and may not be stored or displayed in any publicly accessible location. User names are 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 HMIS access being revoked (see Section 4.3 Security Breach).
Procedure: HMIS Agency Administrators will notify an HMIS System Administrator immediately of employee reassignment to non-HMIS job responsibilities or termination so the login can be inactivated.
Procedure: HMIS End Users not accessing HMIS within three months may have their login inactivated.

4.1.10 Training

Policy: All HMIS End Users receive appropriate training in order to be able to accurately enter and maintain data in HMIS and to abide by all security and privacy policies outlined in this Manual

Procedure: HMIS System Administrators provide training to all HMIS End Users prior to them entering and viewing data in HMIS.
Procedure: HMIS End Users sign an HMIS End User Agreement prior to entering and viewing data in the HMIS.
Procedure: CHO's may register new or current HMIS End Users for HMIS training via the Register for Training form on the Ohio BoSCoC website. HMIS System Administrators provide training to all new HMIS End Users. HMIS System Administrators provide periodic training updates for all HMIS End Users. The HMIS Management Committee is responsible for ensuring that training includes content related to both HMIS policies and security.
Procedure: HMIS End Users are required to complete an annual HMIS End User License renewal. Failure to complete this training may result in revocation of access to the HMIS.
The annual HMIS End User License renewal includes a quiz that tests users on their understanding of HMIS policies and procedures, data standards, and privacy and security. All HMIS End Users will be required to pass the quiz in order to maintain HMIS access.

4.1.11 Data Retrieval

Policy: HMIS End Users will maintain the security of any client PII data extracted from the database and stored locally, including all data used in custom reporting. HMIS End

Users will not electronically transmit any PII client data across a public network. Emailing of client data may be permitted provided a secure IntraMail, or a third party encrypted email product is used. CHO's are responsible for ensuring any secure email software or products are sufficiently secure.

Procedure: PII data extracted from the database and stored locally will be stored in a secure location and appropriately disposed of. Security questions will be addressed to a System Administrator.

4.2 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 client consent forms. A 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.

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.

4.2.1 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.

4.3 Security Breaches

Policy: This process specifically applies to HMIS Security Breaches, though depending on the gravity of the breach, the HMIS Management Committee may opt to immediately and permanently revoke licensure, as specified later in this Policy. Breaches of these standards, including, but not limited to, sharing of username and passwords and emailing Personally Identifying Information (PII), are cause for serious concern and could potentially jeopardize client confidentiality. This protocol outlines the process that the HMIS Management Committee will use to respond to HMIS security breaches. For further information about what may be considered PII or security breaches, refer to the HUD Data Standards, Section 4, Standards for Data Confidentiality and Security, or the HMIS User – HMIS Privacy and Security Video content on the COHHIO eLearning system.

Procedure: Any type of security breach will be deemed an offense for response via this protocol. The following information provides a description of what will occur once any breach has been detected:

- **First Offense:**
  - Inactivate login immediately.
  - User will be asked to complete an online security breach course including an information section, review of the policies and procedures, a security quiz, and a Security Breach Acknowledgment form.

- **Second Offense**:
  - Inactivate login immediately.
  - Notify the user's supervisor and Executive Director or equivalent.
  - Notify the HMIS Lead Agency (COHHIO)
  - May notify ODOD, HUD, or VA, who may withhold funding or take other action due to violation of the agency's grant agreement, at HMIS Lead Agency's (COHHIO) discretion.
  - License may be reactivated at HMIS Lead Agency's (COHHIO) discretion.
- **Third Offense**:
  - License revoked permanently.
  - Further actions taken as necessary, such as reporting to funder or notifying clients of the data breach.

5 Data Quality

5.1 Data Entry

Policy: HMIS End Users are 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 maintains Data Quality Standards to help all CHOs manage the monitoring of their data quality.

Procedure: HMIS System Administrators will develop and implement a data quality plan to help ensure accuracy of data in HMIS.
Procedure: If the End Users do not respond when contacted by HMIS System Administrators to address data quality issues, as part of the HMIS data quality plan, HMIS System Administrators will reach out to the HMIS Agency Administrators and/or Executive Director of the agency. If an agency does not adequately respond to the request for improvement, the issue will be raised with the HMIS Management Committee and an action plan determined. If the agency still does not adequately respond to the request for improvement, the CoC Staff Lead may contact the appropriate funding agency regarding the issue and continued access to the HMIS may be jeopardized.

5.2 Data Quality Plan

Policy: The Data Quality Standards are 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 HMIS System Administrators.

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 System Administrators in a timely manner.

5.3 Covered Homeless Organization (CHO) Data

Policy: All agency and program information is correct and up to date in HMIS.

Procedure: CHOs submit information about newly operating agencies or programs to the appropriate CoC via ohioboscoc@cohhio.org (for the Ohio BoSCoC) or to colleen.kosta@mahoningcountyoh.gov (for MCHCoC). CHOs use the New Project Form to convey the information. Once approved, HMIS System Administrators will enter the appropriate data into the HMIS.
Procedure: CHO's submit changes to agency or program data to the appropriate CoC via ohioboscoc@cohhio.org (for the Ohio BoSCoC) or to colleen.kosta@mahoningcountyoh.gov (for MCHCoC). CHO's use the Housing Inventory Verification Report, or other method as directed by the HMIS System Administrators, to convey the information. Once approved, System Administrators will enter the appropriate data into the HMIS.

6 HMIS Participation Fees

6.1 HMIS Fees

Policy: All CHOs participating in the HMIS may be required to pay HMIS participation fees. Refer to the CoC's current HMIS Participation Fee Policy for details.

Procedure: CHO's will pay for their HMIS participation as outlined in the participation fee policy referenced above.