

## *The Ohio Balance of State Homeless Management Information System*

### **Policies and Procedures Manual**

#### ***Overview***

The Ohio Balance of State Continuum of Care (BOSCO) for its Homeless Management Information System (HMIS) Implementation develops these policy standards and subsequent procedures of data usage for all Balance of State HMIS (BOSHMIS) users and user agencies. This manual serves to better protect the confidentiality of all personal information entered into the Homeless Management Information System while identifying the reasonable, responsible, and limited uses and disclosures of data, which comply with federal regulations set by the Department of Housing and Urban Development (HUD). Its purpose is to guide and clarify federal regulations for BOSCO agencies in their daily operations. It in no way, however, should serve as a substitute for any federal regulations outlined and updated by HUD in its Data and Technical Standards. All BOSCO 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.

# Policies and Procedures Manual

## Table of Contents

I. Roles and Responsibilities.....	5
A. Ohio Development Services Agency .....	5
B. The Coalition On Homelessness and Housing In Ohio .....	5
C. Core Group .....	5
D. Covered Homeless Organization (CHO) .....	6
E. HMIS Users .....	7
F. HMIS Advisory Committee.....	7
II. Privacy Standards .....	8
A. Personally Identifying Information (PII) .....	8
B. HMIS Uses and Disclosures .....	8
C. Applying the Standard .....	9
D. Other Allowable Uses and Disclosures.....	9
1. Legal: .....	9
2. Health and Safety .....	10
3. Abuse, Neglect, Domestic Violence .....	10
4. Law Enforcement.....	11
III. Privacy Requirements.....	12
A. Limits on Data Collection .....	12
1. Client Confidentiality .....	12
2. Informed Consent.....	13
3. Additional User Privacy Measures .....	13
B. Required Data Collection .....	14

# Policies and Procedures Manual

C. Appropriate Data Collection .....	14
D. Privacy Notice -- Identifying Purpose and Use Limitation .....	14
E. Anonymous Clients .....	15
F. Ethical Data.....	16
G. Termination .....	16
H. Openness and Disclosures .....	17
I. Access and Correction .....	18
1. Covered Homeless Organization.....	19
2. System Administrator .....	19
3. Client .....	20
4. Public.....	20
5. Inter-Agency Data Sharing.....	20
6. Access to Core Database.....	21
7. On-Site Review .....	21
J. Accountability.....	21
K. Client Grievance .....	22
IV. Security Standards.....	23
A. System Security .....	23
1. Additional Security Protections .....	23
2. Hardware/Software Requirements.....	24
3. Data Access Location .....	24
4. User Access.....	24
5. Virus Protection.....	25
6. Firewalls .....	25

# Policies and Procedures Manual

7. User Licenses .....	25
8. HMIS User Agreements .....	26
9. Training .....	26
10. Data Retrieval .....	26
B. Hard Copy Security .....	27
C. Physical Access .....	27
1. CHO Technical Support Requirements .....	28
V. Data Quality.....	29
A. Data Entry.....	29
B. Data Quality Plan .....	29
C. New Provider Data.....	29

# Policies and Procedures Manual

## I. Roles and Responsibilities

---

### ***A. Ohio Development Services Agency***

*Policy:* The Ohio Development Services Agency Office of Community Development (ODSA/OCD) is responsible for system administration and project management of the OBOSHMIS.

*Procedure:* The duties of all external HMIS project staff and the System Administrator at ODSA/OCD will be a joint effort. The ODSA/OCD will act as lead agency for the BOSHISMIS.

### ***B. The Coalition On Homelessness and Housing In Ohio***

*Policy:* The Coalition on Homelessness and Housing in Ohio (COHHIO) HMIS Department will assist ODSA/OCD in the implementation of the OBOSHMIS.

*Procedure:* COHHIO will help agencies to gain access to the database system, assist ODSA/OCD in developing any necessary custom reports, assist with training and help provide technical assistance to the HMIS participants. COHHIO will assist ODSA/OCD with the implementation of the OBOSHMIS process as part of the Core Group. COHHIO will participate in the Core Group meetings and assist with duties in the HMIS implementation. COHHIO HMIS Department will oversee and monitor the purchase of hardware, Internet access and coordinate the reimbursement process.

### ***C. Core Group***

*Policy:* The Core Group will consist of staff members from both COHHIO and ODSA/OCD. The Core Group will work with the Advisory Committee and the ODSA/OCD Deputy Chief in setting and adhering to HMIS Policy.

*Procedure:* The Core Group will meet on a routine basis to plan for trainings and HMIS implementation, discuss issues from end-users or covered homeless organizations (CHO) and trouble shoot problems with the database system. The HMIS Department

## Policies and Procedures Manual

will report to the OCD Office Chief and will be involved with the project throughout its implementation.

*Policy:* The Core Group is responsible for relevant and timely communication with each CHO regarding the OBOSHMIS.

*Procedure:* General communications from the Core Group will be directed towards the Agency Administrator. Specific communications will be addressed to the person or people involved. The Core Group will be available via email, phone, and mail. The ServicePoint “System News” feature will also be used to distribute HMIS information. The Core Group will review all broadcast email. In addition, all documents, manuals, and web postings will be reviewed first by the Core Group and then final review will be completed by the Office of Community Development (OCD) Supportive Housing Manager, prior to distribution to the OBOSHMIS System Administrators, HMIS Users or members of the Advisory Group.

### ***D. Covered Homeless Organization (CHO)***

*Definition:* Any organization (including all its affiliates) that records, uses or processes\* PII on clients experiencing homelessness or those at risk of experiencing homelessness for an HMIS (Section 4.1.1, *2004 HMIS Data and Technical Standards*).

\*Processing refers to any and all operations performed on the PII (i.e. collection, maintenance, etc.).

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

*Procedure:* Any agency, organization or group who has signed an HMIS Agency Agreement with the ODSA/OCD will be given access to the OBOSHMIS database through trained HMIS Users (see E. HMIS Users below).

*Policy:* CHOs are responsible for communicating needs and questions regarding the OBOSHMIS directly to the Core Group.

*Procedure:* Users at CHOs will communicate needs, issues and questions to the COHHIO HMIS Department. If the CHO is unable to resolve the issue, he/she will contact the ODSA/OCD.

# Policies and Procedures Manual

## **E. HMIS Users**

*Policy:* Any individual who uses ServicePoint must have a signed HMIS User Agreement on file with ODSA/OCD and abide by all policies and procedures in this Manual. The OBOSH MIS will grant the following permissions to HMIS users according to the below hierarchy:

NOTE: These user permission levels are specific to ServicePoint and do not necessarily relate to agency positions.

1. System Administrator
2. Executive Director
3. Agency Administrator
4. Case Manager

*Procedure:*

At each new user training, CHOs are responsible for identifying the employee's role in regard to permissions within the HMIS system.

*Procedure:* System Administrator and Executive Director access levels are limited to COHHIO or ODSA staff only.

*Procedure:* An Agency Administrator is responsible for ensuring quality, timely data entry; staying knowledgeable about HUD and ODSA regulations as they change; being a point of contact to System Administrator; notifying a System Administrator of any changes in user access to HMIS, provider address, contact information, or bed count data, if applicable; plus all the responsibilities listed for Case Manager.

*Procedure:* A Case Manager is 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. Note: if an Agency Administrator is not assigned the Case Manager will assume the responsibilities of the Agency Administrator until one is assigned.

## **F. HMIS Advisory Committee**

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

# Policies and Procedures Manual

*Procedure:* The Core Group will solicit names of particularly skilled candidates for this committee and will invite them to join. The Core Group will elicit advice and convene meetings of this group as necessary.

## II. Privacy Standards

---

### ***A. Personally Identifying Information (PII)***

*Definition:* Any information maintained by or for a member of the BOSCO or other Covered Homeless Organization about a living homeless client or homeless individual which:

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

*Policy:* A CHO will enter into the OBOSHMIS a required set of data variables for each client, including all universal and program specific data elements, which are specified in the HUD HMIS Data and Technical Standards (see Appendix A for list of Data Elements).

*Procedure:* All HMIS users will be trained in appropriate and accurate procedures for entering PII into HMIS. This training is provided by the HMIS Department.

### ***B. HMIS Uses and Disclosures***

*Policy:* A CHO may use or disclose PII from an HMIS under the following circumstances:

- To provide or coordinate services to an individual;
- For functions related to payment or reimbursement for services;
- To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or
- For creating de-identified PII (Section 4.1.3, *2004 HMIS Data and Technical Standards*).

# Policies and Procedures Manual

*Procedure:* All CHOs must comply with or consult COHHIO or ODSA before providing any information outside of the above stated standards. Disclosure questions should be addressed and documented with ODSA.

## ***C. Applying the Standard***

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

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

## ***D. Other Allowable Uses and Disclosures***

*Policy:* Provided below are additional uses and disclosures of information allowable by HUD standards. It should be noted that these additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards). However, nothing in this standard modifies an obligation under applicable law to use or disclose personal information (Section 4.1.3, *2004 HMIS Data and Technical Standards*).

*Procedure:* A CHO must comply with below standards for additional disclosure to applicable entities. All other disclosures must first be approved by ODSA.

### **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. The following are allowable uses but not a comprehensive list:

# Policies and Procedures Manual

- 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 CHO believes in good faith that the PII constitutes evidence of criminal conduct that occurred on its premises

*Procedure:* A CHO must take immediate actions to notify ODSA 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 the Chief Deputy at ODSA before approving any disclosure.

## 2. Health and Safety

*Policy:* A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PII if:

- The CHO, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
- The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

*Procedure:* A CHO must take immediate actions to notify ODSA 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 ODSA administration before approving any disclosure.

## 3. Abuse, Neglect, Domestic Violence

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

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

## Policies and Procedures Manual

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

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

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

#### 4. Law Enforcement

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

- In response to a request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PII disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics.
- If the official is an authorized federal official seeking PII for the provision of protective services to the President or other authorized persons OR for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others).

*Procedure:* A CHO must take immediate actions to notify ODSA 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 ODSA administration before approving any disclosure.

## III. Privacy Requirements

---

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

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

### **A. Limits on Data Collection**

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

*Procedure:* A CHO must post a 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. Consent of the individual for data collection may be inferred from the circumstances of the collection.

### **Additional Privacy Protections**

#### **1. Client Confidentiality**

*Policy:* The OBOSHMIS System Administrator and CHOs will ensure the confidentiality of all client data. No identifiable client data will be entered

## Policies and Procedures Manual

into the OBOSHMIS 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.

### 2. Informed Consent

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

*Procedure:* Client consent forms must be completed with each individual or household accessing services before any information is entered into the OBOSHMIS. Consent forms should be stored in a secure place.

### 3. Additional User Privacy Measures

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

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

*Procedure:* All additional privacy measures must comply with federal regulations and the policies and procedures of this document.

*Policy:* OBOSHMIS users will be responsible for maintaining updated and accessible privacy notices and other procedures.

*Procedure:* All 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 designated procedure developed by the CHO.

# Policies and Procedures Manual

## ***B. Required Data Collection***

*Policy:* CHOs will collect all required sets of data variables for each client as determined by HUD HMIS Data and Technical Standards (see Appendix A for Required Data Elements).

*Procedure:* Appendix A will contain a listing of data elements to be collected for each client contact in accordance with federal regulations. These data elements may change as HUD HMIS Data and Technical Standards are revised and updated.

## ***C. Appropriate Data Collection***

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

*Procedure:* OBOSHISMIS users will refer to policies outlined in the Data Quality Plan (see Appendix B) for timelines, accuracy and completeness. Users will ask the COHHIO System HMIS Department for any necessary clarification of appropriate data collection.

## ***D. Privacy Notice -- Identifying Purpose and Use Limitation***

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

*Procedure:* 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 ODSA about all legal disclosures.

## **Additional Uses**

## Policies and Procedures Manual

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

- 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 (Section 4.2.3, *2004 HMIS Data and Technical Standards*).

*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 ODSA if potentially beyond reasonable scope of authority.

### ***E. Anonymous Clients***

*Rationale:* Anonymous clients in HMIS negatively affect data quality for the Annual Homeless Assessment Report (AHAR) and other HUD reports. HUD does allow for anonymous clients, but they also count that data as missing, and HUD funding is increasingly being tied to data quality. There is certainly a need to accommodate clients who need services, but who do not feel comfortable sharing their personally identifying information in HMIS. Having a clear understanding of the Balance of State

## Policies and Procedures Manual

Privacy Policies is a necessity when explaining to clients what purpose their data fills and how it is protected. Based on previous years' data, the Balance of State CoC HMIS providers have an average of less than 1% of clients not fleeing domestic violence being entered as anonymous.

*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.

*Procedure:* Refer to the Data Quality Standards for information on how to find the percentage of anonymous clients not currently fleeing domestic violence for a given CHO.

### ***F. Ethical Data***

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

*Procedure:* All HMIS users will sign an HMIS User Agreement before being given access to the OBOSHMIS. 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 OBOSHMIS will be terminated.

### ***G. Termination***

*Policy:* All HMIS users and CHOs are subject to the privacy and confidentiality terms outlined in this document as well as the federal regulations in the HUD Data and Technical Standards. At any point if a breach of rules and/or policies occurs the user may be penalized by loss of access and/or membership in the OBOSHMIS.

*Procedure:* The CHO or HMIS User shall inform the 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 System Administrator will investigate the issue and determine a proper course of action for correction. If a permanent resolution is unforeseen or the 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 OBOSCO.

## Policies and Procedures Manual

- The OBOSHMIS System Administrator will revoke access of the HMIS User or CHO staff to OBOSHMIS.
- The OBOSHMIS System Administrator will keep all termination records on file.

### **Voluntary Termination**

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

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

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

### ***H. Openness and Disclosures***

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

*Procedure:* All amendments to the privacy notice must be consistent with the requirements of these privacy standards. A CHO must maintain permanent documentation of all privacy notice amendments. Copies of the current privacy notice must be available to all clients, including a sign stating the availability of its privacy notice to any individual who requests a copy. In addition, CHOs who receive federal

## Policies and Procedures Manual

financial assistance shall provide required information in languages other than English that are common in the community, if speaker of these languages are found in significant numbers and come into frequent contact with the program. \*CHO's are also reminded that they are obligated to provide reasonable accommodations for persons with disabilities throughout the data collection process.

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

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

- Giving a copy of its privacy notice to each client on or about the time of first data collection.
- Adopting a policy for changing its privacy notice that includes advance notice of the change, consideration of public comments, and prospective application of changes (Section 4.2.4, *2004 HMIS Data and Technical Standards*).

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

### ***I. Access and Correction***

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

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

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

## Policies and Procedures Manual

- 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 System Administrator.*

### **1. Covered Homeless Organization**

*Policy:* CHOs will have access to retrieve any individual and aggregate data entered by their own programs. CHOs will not have access to retrieve individual records entered by other programs except when data is explicitly shared through the HMIS Agency Agreement, a written agreement between organizations or with the explicit consent of the client. When generating reports, users will only be able to generate data from those records for which they have access.

*Procedure:* CHOs will create written memorandum of understandings (MOU) between each other when they wish to share client data beyond the default level of sharing in the HMIS system. MOU's should be provided to the Core Team for review.

### **2. System Administrator**

*Policy:* The System Administrator will have access to retrieve all data in the OBOSHMIS. The System Administrator will not access individual client data for purposes other than maintenance and checking for data integrity. The System Administrator will only report client data in aggregate form.

## Policies and Procedures Manual

*Procedure:* The System Administrator will be responsible for ensuring that no individual client data is retrieved for purposes other than maintenance and performing data quality checks.

### **3. Client**

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

*Procedure:* A client will provide a signed written request to a case manager to see the client's own record. The case manager, or any available staff person within OBOSHMIS access, will verify the client's identity and print all requested information. The case manager can also request a logged audit trail of the client's record from the Agency Administrator. The Agency Administrator will contact the System Administrator who will print this audit trail and with agency approval forward to the Agency Administrator for distribution to the client.

### **4. Public**

*Policy:* The ODSA staff, on behalf of the HMIS Advisory 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 ODSA staff. As part of the System Administrator's regular employment functions, periodic public reports about homelessness and housing issues in Ohio Balance of State will be issued. No PII data will be released in any of these reports.

### **5. Inter-Agency Data Sharing**

*Policy:* Data included in the Profile section of a client record will be viewable by all users; in addition, any entry/exits will be viewable by all users as well. CHOs

## Policies and Procedures Manual

will specify other CHOs with which it will share any other data, and the data sections that will be shared in an HMIS Agency Agreement.

*Procedure:* CHOs will create written memorandum of understandings (MOU) between each other when they wish to share client data beyond the default level of sharing in the HMIS system. MOU's should be provided to the Core Team for review.

### **6. Access to Core Database**

*Policy:* No one will have direct access to the OBOSHMIS database through any unless explicitly given permission by the ODSA/OCD.

*Procedure:* In contract with ODSA/OCD, Bowman Systems will monitor access of the database server and employ security methods to prevent unauthorized database access.

### **7. On-Site Review**

*Policy:* The Core Group may perform annual on-site reviews at each CHO of data processes related to the OBOSHMIS.

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

## ***J. Accountability***

*Policy:* A CHO must adhere to confidentiality, privacy and security standards. 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 require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that

## Policies and Procedures Manual

acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice (Section 4.2.6, 2004 HMIS Data and Technical Standards).

### **Additional Protections**

*Policy:* A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements. Additional protections include but are not limited to:

- Requiring each member of its staff to undergo (annually or otherwise) formal training in privacy requirements;
- Establishing a method, such as an internal audit, for regularly reviewing compliance with its privacy policy;
- Establishing an internal or external appeal process for hearing an appeal of a privacy complaint or an appeal of a denial of access or correction rights; and/or
- Designating a chief privacy officer to supervise implementation of the CHO's privacy standards.

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

### **K. Client Grievance**

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

*Procedure:* Clients will bring HMIS complaints directly to the CHO with which they have a grievance. CHOs will provide a copy of the OBOSH MIS Policies and Procedures Manual upon request, and respond to client issues. CHOs will send written notice to the COHHIO HMIS staff of any HMIS-related client grievance. The COHHIO HMIS staff will record all grievances and will report these complaints to the Core Group.

# Policies and Procedures Manual

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

*Procedure:* Clients bringing HMIS complaints to the COHHIO HMIS Staff will be provided a copy of the OBOSHMIS Policies and Procedures Manual upon request. COHHIO HMIS staff will send written notice to the Core Team of any HMIS-related client grievance. The COHHIO HMIS staff will record all grievances and will report these complaints to the Core Group.

## IV. Security Standards

---

### ***A. System Security***

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

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

#### **1. Additional Security Protections**

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

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

# Policies and Procedures Manual

## 2. Hardware/Software Requirements

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

*Procedure:* It is the responsibility of the CHO to provide a computer and connection to the Internet. If desired by the CHO, the OBOSHMIS System Administrator will provide advice as to the type of computer and connection. Should the agency need additional equipment, COHHIO's HMIS staff will work with the agency to identify the need and issue reimbursement if appropriate. The Agency must contact COHHIO HMIS staff prior to the purchase of any HMIS related equipment to assure adequate reimbursement.

## 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 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.

## 4. User Access

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

*Procedure:*

System Administrators will provide user names and initial passwords to each user upon completion of training and signing of user agreements and receipt of this Security and Privacy Policies and Procedures document. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. User names will be unique

## Policies and Procedures Manual

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. Passwords will be reset every 45 days. Agencies will notify a System Administrator immediately of employee reassignment to non-HMIS job responsibilities or termination so the login can be inactivated. Users not accessing OBOSHMIS within three months may have their login inactivated.

### 5. Virus Protection

*Policy:* A CHO must protect systems that access HMIS from viruses by using commercially available virus protection software. It may also commit itself to additional security measures beyond this standard if in line with HMIS regulations.

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

### 6. Firewalls

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

*Procedure:* Each CHO must maintain its own up to date firewall, however, each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization.

### 7. User Licenses

*Policy:* User licenses are controlled by COHHIO regardless of program access. CHOs may be limited to two licenses per agency for CoC-funded programs. Non CoC-related programs must purchase licenses from Bowman Internet Systems.

# Policies and Procedures Manual

*Procedure:* Licenses are assigned once training is completed successfully. CHOs wishing to purchase additional user licenses will purchase licenses directly from Bowman and inform a System Administrator of their intent to acquire additional User Licenses. A System Administrator will assign additional user names and passwords upon Bowman's receipt of payment for additional user licenses.

## **8. HMIS User Agreements**

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

*Procedure:* A System Administrator will distribute HMIS User Agreements to new HMIS Users for signature. The user will sign the HMIS User Agreement. A System Administrator will collect and store signed HMIS User Agreements for all users. A copy of all signed user agreements must be forwarded to ODSA/OCD for the permanent HMIS file.

## **9. Training**

*Policy:* All users must be trained by COHHIO and sign an End User Agreement prior to receiving a login to the HMIS.

*Procedure:* CHO Agency Administrators or Executive Directors can sign up new or current users for HMIS training by emailing [hmis@cohhio.org](mailto:hmis@cohhio.org). COHHIO HMIS staff will provide training to all new users. Agency Administrators will be given additional training relevant to their position. The System Administrator will provide periodic training updates for all users. The Core Team will be responsible for ensuring that users are instructed in both policies and security.

*Procedure:* All users are required to complete an annual security and privacy training. Failure to complete this training may result in revocation of access to OBOHMIS.

## **10. Data Retrieval**

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

## Policies and Procedures Manual

reporting. OBOSHMIS users will not electronically transmit any PII client data across a public network.

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

### ***B. Hard Copy Security***

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

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

### ***C. Physical Access***

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

*Procedure:* A CHO must take steps to secure each computer by automatically turning

## Policies and Procedures Manual

on a password protected screen saver when the workstation is temporarily not in use. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system.

### **1. CHO Technical Support Requirements**

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

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

## V. Data Quality

---

### **A. Data Entry**

*Policy:* OBOSHMIS users will be responsible for the accuracy of their data entry.

*Procedure:* The CHO must maintain standards for periodically checking data for completeness, accuracy and timeliness. The OBOSHMIS will also define and maintain a data quality plan to help all CHOs monitor data quality. The Systems Administrator will perform regular data quality checks on the OBOSHMIS using the Data Quality Plan (see Appendix B for Data Quality Plan). Any patterns of error will be reported to the Agency Administrator. When patterns of error have been discovered, users will be required to correct the data, data entry processes (if applicable) and will be monitored for compliance.

### **B. Data Quality Plan**

*Policy:* The Data Quality Plan designed by ODSA in collaboration with the OBOSCO 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 ODSA.

*Procedure:* The Data Quality Plan (see Appendix B) 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 ODSA in a timely manner.

### **C. New Provider Data**

*Policy:* All new programs, projects or providers are to be entered into HMIS by a System Administrator.

*Procedure:* New programs, projects or providers are to contact COHHIO HMIS staff to inform of the intent for new information in HMIS. COHHIO HMIS staff will verify the information and then enter the appropriate data into the OBOSHMIS.

## Policies and Procedures Manual

*Policy:* All provider data including but not limited to name, project type, bed counts, address, and contact information in HMIS must be kept up to date.

*Procedure:* Any changes to a provider's data should be reported immediately to COHHIO HMIS staff.

# Policies and Procedures Manual

## Appendix A: Data Elements

### Universal

1. Name
2. Social Security Number
3. Date of Birth
4. Race
5. Ethnicity
6. Gender
7. Veteran Status
8. Disabling Condition
9. Residence Prior to Project Entry
10. Project Entry Date
11. Project Exit Date
12. Destination
13. Personal Identification Number
14. Household Identification Number
15. Head of Household
16. Length of Time Homeless

### Program-Specific Data Elements

1. Zip Code of Last Permanent Address
2. Housing Status
3. Income and Sources
4. Non-Cash Benefits
5. Health Insurance / Medical Assistance
6. Employment Status
7. Physical Disability
8. Developmental Disability
9. Chronic Health Condition
10. HIV/AIDS
11. Mental Health Problem
12. Substance Abuse
13. Domestic Violence
14. Contact
15. Dates of Engagement and Enrollment

## Policies and Procedures Manual

16. Veterans Information
17. Services Provided
18. Financial Assistance Provided
19. Area Median Income (AMI) Percentage Used for Eligibility
20. Sexual Orientation
21. Last Grade Completed
22. School Status
23. General Health Status
24. Pregnancy Status
25. Funding Source for Residence Prior to Project Entry
26. Funding Source for Destination
27. Referrals Provided
28. Reason for Leaving
29. Project Transition
30. Formerly a Ward of Child Welfare / Foster Care Agency
31. Formerly a Ward of Juvenile Justice System
32. Young Person's Critical Issues
33. Referral Source
34. Transitional, Exitcare, or Aftercare Plans and Actions
35. Project Completion Status
36. Family Reunification Achieved
37. Physical Health Status
38. Dental Health Status
39. Mental Health Status
40. Housing Category
41. Percent of AMI
42. Formerly Chronically Homeless
43. Federal Funding Source for Project Enrollment
44. Worst Housing Situation

# Policies and Procedures Manual

## Appendix B: Data Quality Plan Outline

### I. Introduction

- A. Applicability of the HMIS Data Quality Standards
- B. What is an HMIS
- C. HMIS Data and Technical Standards
- D. What is Data Quality?
- E. What are Data Quality Standards?
- F. What is a Data Quality Monitoring Plan?

### II. Data Quality Standards

- A. Data Timeliness
  - 1. Data Timeliness Standard
- B. Data Completeness
  - 1. Data Completeness Standard
- C. Data Accuracy
  - 1. Data Accuracy Standard:
- D. Bed/Unit Utilization Rates

### III. Data Quality Monitoring Plan

- A. Roles and Responsibilities
- B. Data Quality Monitoring
- C. Compliance