Toledo Homeless Management Information System (HMIS) Consolidated Policies and Procedures

Purpose of HMIS

The purpose of the Toledo HMIS project is to provide a robust and comprehensive system for collecting and disseminating information about persons experiencing homelessness and the homelessness service system in support of the Toledo-Lucas County Continuum of Care's goal to prevent, reduce, and eliminate homelessness.

We do this by assisting homelessness service providers in generating reports to the U.S. Department of Housing and Urban Development, the Toledo Lucas County Continuum of Care, and other funders, as well as streamlining and consolidating their internal tracking and record-keeping requirements.

I. Roles and Responsibilities

1. **Project Management**
   The Toledo Lucas County Homelessness Board (TLCHB) is responsible for the HMIS project under the auspices of a TLCHB/HMIS Administrator. The HMIS Administrator is employed and supervised by TLCHB.

2. **Project Staffing**
   The HMIS Administrator has primary responsibility for coordination and administration of the Toledo HMIS and reports to the TLCHB Chief Executive Officer (CEO).

3. **Contributory HMIS Organizations**
   Any agency, group, or other entity that has completed an Agency Agreement with the HMIS Administrator is a Contributory HMIS Organization (CHO). All CHO's must abide by all policies and procedures outlined in this manual, which are subject to change. CHO's must complete a CHO Agreement with the HMIS Administrator on an annual basis. CHO's with expired CHO Agreements may have their End User accounts locked or removed to maintain the security, confidentiality, and integrity of the system. CHO's are responsible for the conduct of their End Users and the security of End User Accounts.

4. **Project Agency Administrators**
   Each CHO will designate an HMIS Agency Administrator to serve as primary contact between the HMIS Administrator and the CHO, and each HMIS Agency Administrator must have a valid email address with the CHO. Each CHO should choose its HMIS Agency Administrator and send that person's name and contact information to the HMIS Administrator. Changes to that information should be promptly reported to the HMIS Administrator.

5. **HMIS Advisory Committee**
   The CEO or designee will convene a committee to advise the project's operations, policies, and procedures and provide feedback on a regular basis. The CEO or designee will seek out particularly skilled individuals whose breadth and depth of expertise is well-suited to the project.

6. **HMIS End Users**
   In addition to an HMIS Agency Administrator, CHO's must designate other individuals to access the system on their behalf, and CHO's are encouraged to use ServicePoint as their primary tool for client and service tracking, case management, and operational reporting. The HMIS Administrator will work with CHO's to determine the appropriate User Access Level designation for each End User.

Toledo Homeless Management Information System (HMIS) Consolidated Policies and Procedures

There is no upper limit to the number of End Users each CHO may authorize, but Toledo HMIS may assess participation fees to recover the cost of ServicePoint licenses.

All End Users, including HMIS Agency Administrators and HMIS staff, must complete an End User agreement with the HMIS Administrator on an annual basis. End User accounts with expired End User Agreements may be locked or removed to maintain the security, confidentiality, and integrity of the system.

7. **Communication**

General communications from the HMIS Administrator will be directed toward Agency Administrators. Specific communications will be addressed to the person or people involved. The Toledo HMIS Administrator will be available via email, phone, and U.S. mail. The ServicePoint Newsflash feature may also be used to distribute HMIS information.

Participating CHO's are responsible for communicating needs, questions, and concerns regarding the Toledo HMIS directly to the HMIS Administrator.

8. **System Availability**

Wellsky (formerly Mediware and Bowman Systems) will provide a highly available database server and will inform Toledo HMIS staff in advance of any planned interruption in service. Whenever possible, if the database server is unavailable due to disaster or routine maintenance, Toledo HMIS staff will inform End Users of the cause and duration of the interruption in service. The HMIS Administrator will log all downtime for purposes of system evaluation.

9. **Client Grievances**

Clients will contact the CHO with which they have a grievance for resolution of HMIS problems. CHO's will provide a copy of the Toledo HMIS Policies and Procedures Manual upon request, and respond to client issues. CHO's will send written notice to the HMIS Administrator of any HMIS-related client grievance. The HMIS Administrator will record all grievances and will report these complaints to the HMIS Advisory Committee.

Toledo Homeless Management Information System (HMIS) Consolidated Policies and Procedures

II. Security and Privacy Plan

1. **Security Officer**
Each CHO must designate an HMIS Security Officer to be responsible for ensuring compliance with applicable security standards. The Security Officer need not be an End User. The Security Officer must be an employee of the CHO. For any CHO with no employees, the Security Officer must be the President, Chair, or other top-level representative responsible for the CHO.

2. **Workforce Security**
Each CHO must have a workforce security policy that includes conducting a criminal background check on its Security Officer and on any users with Agency Director level access or greater. Criminal background checks must be completed at least once every five years. On request, CHOs must certify to Toledo HMIS when the most recent criminal background check has been completed for each applicable staff member. The background check must include local and state records; CHOs are strongly encouraged to include federal records as well.

3. **Security and Privacy Awareness Training**
Toledo HMIS will conduct a security and privacy awareness training on an annual basis, which will be required for all End Users and Security Officers. This training will cover relevant statutory and regulatory requirements, local policies, and best practices for HMIS security and privacy.

4. **Disaster Recovery Plan**
In the event of a disaster involving substantial loss of data or system downtime, Toledo HMIS will contact CHO Security Officers by phone or email within one business day to inform them of the expected scale and duration of the loss or downtime. Toledo HMIS will continue to inform CHO Security Officers as new information becomes available about the scale and duration of lost data or system downtime. In the event that loss of data is expected to exceed three business days of activity or system downtime is expected to exceed 24 hours, Toledo HMIS will begin to disclose estimates of loss and downtime to the public as well.

5. **Annual Security Review**
All CHOs must undergo an annual security review, which includes, at a minimum, completion of the following security checklist:
   a. Proper display of "Purpose of Data Collection" notice
   b. Workstation security as described in Section 10
   c. Policies for tracking "HMIS Disclosure" forms
   d. Certification of most recent background check for applicable personnel as described in Section 2; and
   e. Mobile Security Policy

   Annual Security Review will be scored using a points system. CHOs that meet the required standards for security during the review will receive five (5) points. CHOs that do not meet the required standards initially but correct their findings in the mitigation time frame will receive five (5) points. CHOs that do not meet the security standards or fail to correct their findings in the mitigation timeframe will receive zero (0) points.

Toledo Homeless Management Information System (HMIS) Consolidated Policies and Procedures

6. **Contracts and Other Arrangements**
   Toledo HMIS must retain copies of all contracts and agreements executed as part of the administration and management of HMIS or required to comply with the requirements of these policies.

7. **Allowable Use and Disclosure of HMIS Data**
   Toledo HMIS will only collect client data relevant to the delivery of services to people experiencing homelessness, a housing crisis, or housing instability in Lucas County, Ohio.

   a. Service Delivery
   Client-level data may be stored and retrieved by CHOs when relevant to assessing program eligibility, providing services, and making corrections.

   b. Reporting to Program Funders
   Reports of client data in aggregate may be generated to satisfy the reporting requirements of certain program funders, including but not limited to:

   - U.S. Department of Housing and Urban Development Emergency Solutions Grant Program;
   - U.S. Department of Housing and Urban Development Continuum of Care Program
   - U.S. Department of Health and Human Services Substance Abuse and Mental Health Services Administration (SAMHSA) and Family and Youth Services Bureau (FSBY) Programs; and
   - State of Ohio Development Services Agency.

   c. Planning and Analysis
   Reports of client data in aggregate may be generated to improve planning and analysis of homelessness, housing crises, and related issues. These include local Continuum of Care planning efforts as well as national reports such as the Longitudinal System Analysis (LSA) Report to Congress, Point-in-Time Counts (PIT), Housing Inventory Chart (HIC), and the System Performance Measures (SysPM) including Data Quality Framework.

   d. Coordinated Assessment
   Reports of client data in aggregate, bed lists, or other availability may be generated to facilitate use of a Coordinated Assessment system.

   e. Documentation of Homelessness
   Client shelter stay records in HMIS may be used by CHOs as documentation of homelessness in accordance with guidance from HUD.

   f. Data Quality
   Reports of client data (individually or in aggregate) may be generated to assess and improve the quality of data being entered.

   g. Troubleshooting
   Toledo HMIS and Wellsky may from time to time access individual client-level data in order to manage system configuration, conduct special projects, troubleshoot system issues, and provide technical assistance.

   h.   Prohibition on CHO Transmission of Identifiable Client Data
Under no circumstances will CHOs transfer reports with readable or retrievable client-level identifying data. Any security breaches and consequences thereof due to violation of this prohibition will be the sole responsibly of the CHO.

   i.   Data Integration and Warehousing
Client-level data may be exported and transferred from the designated Toledo HMIS system for use in research within an interagency data warehouse. Client-level data exported in this fashion will be accompanied by an obfuscated hash value to be used as a key for integrating data from multiple sources.

   j.   Toledo HMIS Transmission of Identifiable Data
In order to further Continuum of Care (CoC) goals, Toledo HMIS may need, from time to time, to transmit unhashed, client-level personally identifiable information to tertiary entities. In these cases, data sharing agreements with non-disclosures will be implemented and any transmitted data will be encrypted to secure the data.

8. Openness of Data
Client-level data in HMIS will generally be Closed and not shared between CHOs unless specific consent is given by a client for data to be shared.

There are two routine exceptions to this general rule. First, any CHO who is performing Coordinated Assessment duties will always be able to search and find clients, regardless of which CHO first created the client record, in order to minimize duplication of client records. Second, any CHO to which Coordinated Assessment refers a client will be granted visibility of Client Identifiers and Coordinated Assessment information in order to transmit the referral, verify the identity of the referred client, and document eligibility for services.

9. Informed Client Participation
CHOs will display a Purpose of Data Collection Notice at all locations where HMIS data are collected from clients, and educate clients as to the purpose and scope of data collected and entered into HMIS.

10. Workstation Security
At a minimum, the primary workstation used by each End User to log in to ServicePoint should be configured to meet the following best practices:
   a.   Password-protected log on for the workstation itself;
   b.   Password-protected (aka locked) screensaver after five minutes or more of inactivity;
   c.   Operating system updated with manufacturer's latest patches at least weekly;
   d.   Ports firewalled;
   e.   Using a currently supported browser and checking for updates regularly. The latest versions of Firefox, Chrome, Safari, and Edge qualify. Exceptions can be made when CHO non-HMIS activities needs a specific browser or version (e.g., Internet Explorer v9) but all other security measures must be maintained to mitigate increased security risks; and
   f.   Systems scanned at least weekly for viruses and malware.

Toledo HMIS may provide recommendations or advise in pursuing these best practices, but proper workstation configuration remains the responsibility of each CHO.

11. End User Accounts

The HMIS Administrator will provide an End User Account username and an initial password to each authorized End User. End User Accounts are assigned on a per-person basis, rather than to a particular position or role. End User Accounts are not to be exchanged, shared, or transferred between personnel at any time.

a. CHO Authority to Demand Usernames and Passwords
Under no circumstances shall a CHO demand that an End User hand over his or her username and password. CHOs shall inform the HMIS Administrator of any changes in personnel or other requests to revoke or transfer accounts.

b. End User Password Security
End User Account passwords must be changed every forty-five (45) days. Passwords should never be written on any item left in an office, desk, or other workspace, and passwords should never be in view of another person.

c. End User Inactivity
End Users who have not logged into the system in the previous 90 days will be flagged as inactive. Inactive End Users may have their ServicePoint accounts locked or removed to maintain the security, confidentiality, and integrity of the system.

12. Prohibition on Client-level Data from Victim Services Providers

Projects which are primarily for survivors of domestic violence, dating violence, sexual assault, and stalking are prohibited from contributing client-level data into the designated HMIS System. However, these programs must record client-level data within a comparable internal database and be able to generate aggregate data for inclusion in reports as described in Section 7.

13. Reporting Security and Privacy Incidents

Any End User or Security Officer suspecting violations of Security and Privacy policies or other should report incidents in writing. Reports should include, at a minimum, the date, time, location, and personnel involved in the incident, along with a description of the suspected violation.

a. Chain of Reporting
End Users should report issues first to their CHO's designated Security Officer within one business day. Security Officers, in turn, should report the issue jointly to the CHO director and Toledo HMIS Staff within one business day.

b. Public Disclosure of Security Incidents
If a CHO is found to have committed a major violation as described in Section 14, the incident will be disclosed to the public along with the sanctions instituted in response.

14. Sanctions for Violations

a. Minor Violations
Minor violations include but are not limited to:
- End User or Security Officer absence at a required quarterly End User meeting or annual Security and Privacy Training, unless prior arrangements have been made for receiving missed training.
- Workstations non-compliant with up to two Workstation Security items described in Section 10.

The sanctions for minor violations are dependent on the number of minor violations by the CHO within a 24 month period.

- First violation
  (a) A letter documenting violating event and involved personnel will be sent to CHO from Toledo HMIS and kept on-file with Toledo HMIS. CHO must submit to Toledo HMIS a written plan for corrective action, including any internal actions taken against employee who violated policy, within 10 business days and complete the corrective action within 30 days.

- Second violation
  (a) A letter as described in "First violation" above.
  (b) Toledo HMIS will conduct a mandatory training session on security and privacy policies for the CHO in question. This training must be attended by all end users, the CHO's Security Officer, and the Security Officer supervisor or CHO CEO. In organizations where the Security Officer is the CEO, the training must be attended by the chair or president of the CHO's board of directors.

b. Major Violations
   Major violations include but are not limited to:
   - Three or more minor violations within a 24 month period
   - Failure to submit a written plan for corrective action for minor violations within 10 days
   - Failure to complete corrective action for minor violations within 30 days
   - Failure to conduct a criminal background check as described in Section 2
   - Failure to participate in an Annual Security Review as described in Section 5
   - Workstations non-compliant with three or more Workstation Security items as described in Section 10
   - Failure to report security and privacy incidents as described in Section 13
   - Transmitting Client Identifiers in plain text via unsecured or unencrypted e-mail

   The sanction for a major violation is:
   - A letter as described in "First violation" for minor violations above;
   - A mandatory training as described in "Second violation" for minor violations above; and
   - The End User violating the policy or procedure will be prohibited from accessing ServicePoint or participating in HMIS data collection for 90 days. The CHO remains responsible for meeting data quality and other obligations during this 90 day period.

c. Severe Violations
   Severe violations include but are not limited to:
   - Two or more major violations within a 24 month time period
   - Sharing ServicePoint End User accounts
   - End users leaving ServicePoint account credentials in plain view or unattended
   - Improper access of client data beyond the scope outlined in Section 7

   The sanction for a severe violation is:
   - A letter as described in "First Violation" for minor violations above
   - A mandatory training as described in "Second Violation" for minor violations above

- The End User violating the policy or procedure will be prohibited from accessing ServicePoint or participating in HMIS data collection for one year
- Toledo HMIS will levy a fine of one percent (1%) of the CHO's annual budget for activities reported on the Housing Inventory Chart, to a maximum of five hundred dollars ($500). If a CHO has no activity on the Housing Inventory Chart, the fine will be calculated from their overall agency budget.

d. Findings
The TLCHB HMIS Administrator will document any suspected finding of violation(s) and provide them to the TLCHB CEO. The CEO will issue notices to the CHO in question describing the finding of violation(s) and the associated sanction(s).
.

e. Appeals
Findings of violations may be appealed, in writing, by the CHO in question. All appeals must be submitted in writing and should include any available supporting documentation. Appeals must be submitted within five (5) business days of the date the CHO received notice of the finding.

- Appeals for Minor Violations will be received and reviewed by the CEO. The CEO will issue a response within five (5) business days of receiving the appeal, including any amendments to the sanction(s).
- Appeals for Major or Severe Violations will be received and reviewed by the Quality & Performance Committee, which will issue a response within thirty (30) calendar days of receiving the appeal, including any amendments to the sanction(s).

III. Data Quality Plan

1. Data Definitions
With the exception of custom fields used for Coordinated Assessment activity or other local data requests, Data Elements used by Toledo HMIS match those prescribed by HUD in their current Data Standards Manual and Data Dictionary which can be found at https://www.hudexchange.info/programs/hmis/. Data collected for Coordinated Entry and other local data requests can be found at http://endinghomelessnesstoledo.org/thmis/cho-resources.

2. Required Data
CHO's will collect a required set of data elements for each client. The set of required data elements varies by project type or funding sources and individual data elements may not be required for all populations, as established in Section 1. For more information about the required data for each project type, please review the current Data Standards Manual and Data Dictionary which can be found at https://www.hudexchange.info/programs/hmis/. Local requirements for data collection by project type can be found at http://endinghomelessnesstoledo.org/thmis/cho-resources.

3. Data Completeness
a. Program Entry Date and Program Exit Date
CHOs are responsible for completing 100% of their Program Entry Dates and Program Exit Dates for all clients served.

    b. <u>All Other Data</u>
CHOs are responsible for completing ninety-five percent (95%) or more of all other client-level data at entry, interim, exit, and aftercare/follow-up, where applicable.

4. Data Validity/Congruence
CHO's are responsible for providing data that is valid and congruent, meaning that the data should not contain contradictions or impossibilities. No more than one half of one percent (0.5%) of clients should exhibit any given incongruence case, which includes but is not limited to:

    a. Date of birth indicating negative age;
    b. Date of birth indicating age greater than one hundred years old;
    c. Date of birth same as date client was created in HMIS;
    d. Age inconsistent with household relationship (nine-year-old grandmother, etc.);
    e. Veteran status is yes but age is less than eighteen;
    f. Gender conflicts with household relationship (male grandmother);
    g. Listed as head of household but relationship to head of household is not "self";
    h. Not listed as head of household but relationship to head of household is "self";
    i. Household membership but no household relationship; and
    j. Client listed as pregnant but not a female between twelve and fifty-five years old.

5. HUD's Data Quality Framework Report (0640)
CHOs are responsible for providing data that is consistent with the completeness and timeliness standards in the HUD's Data Quality Framework Report. The Consistency Percentage should not drop below 85%.

No data element (listed below) should exceed 5% of error rate or calculability rate or in the case of timeliness, 90% of the data should be entered within six (6) days. Points will be awarded for each section of data according to the following principles:
    a. Section Q2. Personally Identifiable Information (PII): One (1) Point will be awarded for each of the six (6) data elements reported in the table where the error rate is less than 5%. The data elements are: Name, Social Security Number, Date of Birth, Race, Ethnicity, & Gender. The Overall Score is not used for this section.
    b. Section Q3. Universal Data Elements: One (1) point will be awarded for each of the five (5) data elements reported in the table where the error rate is less than 5%. The data elements are: Veteran Status, Project Entry Date, Relationship to Head of Household, Client Location, & Disabling Condition.
    c. Section Q4. Income and Housing Data Quality: One (1) point will be awarded for each of the four (4) data elements reported in the table where the error rate is less than 5%. The data elements are: Destination, Income and Sources at Entry, Income and Sources at Annual Assessment, & Income and Sources at Exit.
    d. Section Q5. Chronic Homelessness: One (1) point will be awarded for the Total Score if the % of Records Unable to Calculate does not exceed 5%.
    e. Section Q6. Timeliness: This section will not be scored at this time. However, HUD's commitment to timely data entry is recognized and important to Toledo HMIS.

The Consistency Percentage will be calculated by dividing the total points awarded by the total possible points (17 points). This percentage must exceed or equal 85%.

6. **Monitoring and Evaluation**

Toledo HMIS will periodically monitor and evaluate the Data Completeness and Validity of data along with consistency with HUD's Data Quality Framework. Data Completeness will be evaluated after each month, while Data Validity and HUD Consistency will be evaluated after each quarter.

a. <u>Reporting Schedule</u>
   - All data for a reporting period should be completed within six (6) days of the collection point but no later than the fifth day of the following month;
   - Toledo HMIS will provide preliminary reports of Data Completeness and Validity and the HUD Data Quality Framework (quarterly only) on the sixth day of the following month;
   - Toledo HMIS will provide support to CHOs as needed for corrections of the previous reporting period's data and CHOs are expected to make any corrections by the tenth day of the following month;
   - Toledo HMIS will provide a second, final report to each CHO on the eleventh day with updated figures; and
   - Preliminary and Final reporting deadlines may be changed at the discretion of the HMIS Administrator with notification to the CHOs and End Users.

b. <u>Performance Evaluation</u>
   CHO performance on Data Completeness., Data Validity and Data Quality Framework will be scored using a points system. CHOs who meet the required standard for Data Completeness will be awarded 1.50 points per month. CHOs who meet the required standard for Data Validity will be awarded 1.75 points per quarter. CHOs who meet the required standards for the Data Quality Framework will receive 1.0 points per quarter. The maximum number of points for Data Quality per calendar year is 29.00.

   The annual security visit point total will be added to the Data Quality point total to arrive at the final point total with a maximum of 34.00. The final performance percentage will be calculated by dividing the total accrued points by the total possible points. All points will be reported on the CHO Tracker that is available on the TLCHB website at http://endinghomelessnesstoledo.org/thmis/reports.

c. <u>Sanctions for Poor Performance</u>
   CHOs which consistently contribute low quality data may be required to receive additional training from Toledo HMIS, develop a written Data Quality Improvement Plan, and/or have End User Accounts suspended until appropriate action is taken to improve Data Quality. Ongoing poor performance will be documented and reported to Funding Programs and entities for review.