West Central Illinois Continuum of Care Consortium (WCICCC)
Homeless Management Information System (HMIS)
Policies and Procedures

Purpose of HMIS

The purpose of the WCICCC HMIS 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 WCICCC service area.

I. Roles and Responsibilities

1. **HMIS Lead** Ensures all HMIS activities are carried out in accordance with the Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act.

2. **Project Staffing** The Support Entity, contractually as the HMIS staff and has primary responsibility for coordination and administration of the HMIS and reports to the HMIS Lead and the WCI Homeless Assistance Council.

3. **Contributory HMIS Organizations** Any agency, group, or other entity that has completed an Agency Partner Agreement with the HMIS Lead or HMIS System 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. HMIS proposed policy and procedure changes must be submitted to HMIS Advisory workgroup for consideration. 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. **HMIS Advisory Workgroup** The Executive Director or designee will convene a committee to advise the project's operations, policies, and procedures and provide feedback on a regular basis. The Executive Director or designee will seek out particularly skilled individuals whose breadth and depth of expertise is well-suited to the project.

5. **HMIS End Users** CHO's designate individuals to access the system on their behalf, and use ServicePoint as their primary tool for client and service tracking, case management, and operational reporting.

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

   All End Users, including HMIS staff, must complete an End User agreement with the HMIS System 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.

6. **Communication** General Communications from the HMIS staff will be directed toward HMIS End Users. Specific communications will be addressed to the person or people involved. The HMIS staff will be available via email, phone, and U.S. mail. Participating CHO's are responsible for communicating needs, questions, and concerns regarding the HMIS directly to the HMIS staff.

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

8. **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 WCICCC HMIS Policies and Procedures Manual upon request, and respond to client issues. CHO's will send written notice to the HMIS System Administrator of any HMIS-related client grievance. The HMIS System Administrator will record all grievances and will report these complaints to the HMIS Advisory Workgroup.

II. Security and Privacy Plan

1. **Security and Privacy Awareness Training** WCICCC staff will conduct a security and privacy awareness training on an annual basis, which will be required for all End Users. This training will cover relevant statutory and regulatory requirements, local policies, and best practices for HMIS security and privacy. End-user will sign their User Policy, Responsibility Statement and Code of Ethics document at this annual training.

2. **Disaster Recovery Plan** In the event of a disaster involving substantial loss of data or system downtime, HMIS staff will contact CHO's Executive Director within one business day to inform them of the expected scale and duration of the loss or downtime. HMIS staff will continue to inform CHO Executive Director as new information becomes available about the scale and duration of lost data or system downtime.

3. **Annual Security and Monitoring Review** All CHOs must undergo an annual security and monitoring review, which includes, at a minimum, completion of the following security and monitoring checklist:
   - Security and Privacy Awareness Training as described in Section II.1;
   - Proper display of "Purpose of Data Collection" notice, see Section II.7;
   - Workstation security as described in Section II.8;
   - Spot checking of client paper files with HMIS data file, including checks of data completeness with program entry/exit dates, see Section III.4a.

4. **Contracts and Other Arrangements** HMIS Lead 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.

5. **Allowable Use and Disclosure of HMIS Data** WCICCC's HMIS will only collect client data

relevant to the delivery of services to people experiencing homelessness, a housing crisis, or housing instability in WCICCC's service region.

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 Continuum of Care Program;
   - Illinois Department Economic Opportunity, Emergency Solutions Grant Program;
   - Illinois Department Human Services, Homeless Prevention Program.

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 CoC planning efforts as well as national reports such as the Annual Homelessness Assessment Report to Congress, Point-in-Time Counts, and the Housing Inventory Chart.

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.

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

g. Troubleshooting HMIS staff and Bowman Systems 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 Use of Identifiable Client Data Under no circumstances will reports be generated or data transferred with readable or retrievable client-level identifying data.

6. **Openness of Data** Client-level data in HMIS will generally be Opened and shared between CHOs unless specific consent is given by a client for data not to be shared. The client receiving homeless services is informed that their personal information is entered into an online homeless database and will be shared with other services providers. Consent for such disclosure is obtained during the initial intake appointment.

   The only exception is case notes which is Closed. Case notes is only Opened to individuals that work at the same CHO.

7. **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.

8. **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 either Internet Explorer 8, Firefox 3, Chrome 8, or Safari 3, or later versions of these browsers; and
    f. Systems scanned at least weekly for viruses and malware.

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

9. **End User Accounts** The HMIS staff will provide an End User Account username and 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 staff 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. End Users may keep passwords written down and stored in a purse, wallet, or other container kept on their person at all times. 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.

10. **Prohibition on Client-level Data from Victim Services Providers** Programs 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. 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 II.5.

11. **Reporting Security and Privacy Incidents** Any End User suspecting violations of Security

and Privacy policies or other should report incidents in writing, via email, to HMIS Lead and Support Entity. HMIS Lead is responsible to report incidents to HMIS Advisory Workgroup. If the HMIS Lead organization is in violation, then the Support Entity will report incidents to the HMIS Advisory Workgroup. 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 within one business day to the HMIS Lead and Support Entity;

b. Public Disclosure of Security Incidents If a CHO is found to have committed a major violation as described in Section II.12, the HMIS Advisory Workgroup will decide the method to handle disclosure. If the incident is severe, then the public will be informed along with the sanctions instituted in response.

12. **Sanctions for Violations**

a. Minor Violations Minor violations include but are not limited to:

- End User absence at a required End User meeting or annual Security and Privacy Awareness Training, unless prior arrangements have been made for receiving missed training;
- Workstations non-compliant with up to two Workstation Security items described in Section II.8.

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

i. First violation

1. A letter documenting violating event and involved personnel will be sent to CHO from WCICCC HMIS System Administrator and kept on-file with WCICCC HMIS System Administrator. CHO must submit to WCICCC HMIS System Administrator 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.

ii. Second violation

1. A letter as described in "First violation" above.

2. WCICCC 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 and the CHO executive director. In organizations where the end user is the executive director, 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 participate in an Annual Security Review as described in Section II.3;
- Workstations non-compliant with three or more Workstation Security items as described in Section II.8;
- Failure to report security and privacy incidents as described in Section II.11;
- Transmitting Client Identifiers in plain text via unsecured or unencrypted e-mail;
- 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 II.5.

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 CHO will lose their eligibility to apply for funding from the Continuum for a period of 12 months from the date of the infraction(s) being “founded”.

c. Findings The HMIS System Administrator will document any suspected finding of violation(s) and provide them to the WCI Homeless Assistance Council and/or HMIS Lead. The WCI Homeless Assistance Council and/or HMIS Lead will issue notices to the CHO in question describing the finding of violation(s) and the associated sanction(s).

d. 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.

i. Appeals for Minor Violations will be received and reviewed by the HMIS Lead. The HMIS Lead will issue a response within five (5) business days of receiving the appeal, including any amendments to the sanction(s).

ii. Appeals for Major will be received and reviewed by the WCI Homeless Assistance Council, 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 a few custom fields used for specialized activities, Data Elements used by WCICCC's HMIS match those prescribed by the U.S. Department of Housing and Urban Development in their March 2010 HMIS Data Standards Revised Notice.

2. **Categories of Data Elements**

a. Client Identifiers

- Name
- Date of Birth
- Social Security Number
- Gender

b. Universal Data Elements

- All Client Identifiers
- Race
- Ethnicity
- Veteran Status
- Disabling Condition
- Residence Prior to Program Entry
- Last Permanent ZIP Code
- Housing Status
- Household Membership
- Program Entry Date
- Program Exit Date (if applicable)

c. Program-Specific Data Elements

- Extent of Homelessness
- Chronic Homelessness Status
- Income Amounts & Sources
- Non-Cash Benefit Amounts & Sources
- Physical Disability
- Developmental Disability
- Chronic Health Condition
- HIV/AIDS Diagnosis
- Mental Health Condition

- Substance Abuse
- Domestic Violence
- Reason for Leaving (if applicable)
- Destination (if applicable)

d. Local Data Elements
   - Employment
   - Education
   - General Health
   - Pregnancy
   - Veteran Details
   - Children's Education
   - Primary Reason for Homelessness/Threat to Housing Stability

e. Service and Shelter Records
   - Alliance of Information and Referral Systems (AIRS) Taxonomy Code
   - Start and End Dates
   - Bed Assignment (if applicable)
   - Amount or Units of Assistance (if applicable)
   - Funding Source (if applicable)
   - Current or Arrears Designation (if applicable)

f. Extended Data
   - Includes Case Notes
   - Goals
   - Action Steps
   - Follow-Up Plans
   - Needs
   - Referrals
   - Self-Sufficiency Matrix measurements
   - Case Manager(s)

3. **Required Data** CHO's will collect a required set of data elements for each client. The set of required data elements varies by program type and individual data elements may not be required for all populations, as established in Section I.

   a. Emergency Shelters Includes any programs designated as an Emergency Shelter on the Continuum of Care's Housing Inventory Chart. The following data are required:
      - Universal Data Elements: All

- Program-Specific Data Elements: None
- Local Data Elements: None
- Service and Shelter Records: All
- Extended Data: None

b. Continuum of Care Programs Includes Continuum of Care Funded Programs. The following data are required:
   - Universal Data Elements: All
   - Program-Specific Data Elements: All
   - Local Data Elements: All
   - Service and Shelter Records: All
   - Extended Data: None

c. Emergency Solutions Grant Includes Emergency Solutions Grant Funded Programs. Emergency Shelters and Transitional Shelters need to complete the steps for Emergency Shelters. Rapid Rehousing and Homeless Prevention following data are required:
   - Universal Data Elements: All
   - Program-Specific Data Elements: None
   - Local Data Elements: None
   - Service and Shelter Records: All
   - Extended Data: None

d. Transitional Housing and Permanent Supportive Housing Includes any programs designated as Transitional Housing or Permanent Supportive Housing on the Housing Inventory Chart that does not get funds that come from HUD. The following data are required:
   - Universal Data Elements: All
   - Program-Specific Data Elements: All
   - Local Data Elements: All
   - Service and Shelter Records: All
   - Extended Data: None

e. Other Direct Financial Assistance Programs Includes rent, deposit, and/or utility assistance programs not funded through programs described in (3)(c) and (3)(d), above. The following data are required:
   - Universal Data Elements: All
   - Program-Specific Data Elements: Reason for Leaving and Destination at Exit only
   - Local Data Elements: Primary Reason for Homelessness/Threat to Housing Stability only

- Service and Shelter Records: All
- Extended Data: None

f. Other Non-Residential Services Only Includes any participating programs which are not listed on the Housing Inventory Chart and which do not provide direct financial assistance or subsidies in support of client housing costs.

  - Universal Data Elements: All
  - Program-Specific Data Elements: None
  - Local Data Elements: Primary Reason for Homelessness/Threat to Housing Stability only
  - Service and Shelter Records: All
  - Extended Data: None

4. **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. Entry and Exit Dates must match client files. Spot checking of data done at the CHO's Annual Security and Monitoring Review.

b. All Other Data CHOs are responsible for completing ninety-five percent (95%) or more of all other client-level data at both entry and exit.

5. **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.

6. **Monitoring and Evaluation** WCICCC HMIS will periodically monitor and evaluate the Completeness and Validity of data. Data Completeness will be evaluated after each month, and Data Validity will be evaluated after each quarter.

a. Reporting Schedule

  - All data for a reporting period should be completed by the fifth day of the following month;

- WCICCC HMIS System Administrator will provide draft reports of Data Completeness and Validity (quarterly only) on the sixth day of the following month;
- WCICCC HMIS System Administrator 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; and
- WCICCC HMIS System Administrator will provide a second, final report to each CHO on the eleventh day with updated figures.

b. Performance Evaluation
CHO performance on Completeness and Validity of data will be scored using a points system. CHOs who meet the required standard for Completeness will be awarded 1.50 points per month. CHOs who meet the required standard for Validity will be awarded 1.75 points per quarter. The maximum number of points for Data Quality per calendar year is 25.00.

c. Sanctions for Poor Performance
CHOs which consistently contribute low quality data may be required to receive additional training from WCICC HMIS Staff, develop a written Data Quality Improvement Plan, and/or have End User Accounts suspended until appropriate action is taken to improve Data Quality.