Heartland Continuum of Care

Homeless Management Information System

Community Services formerly Servicepoint

Policies and Procedures Manual

Revised October 2022

Table of Contents

Policy: Roles and Responsibilities

Heartland Continuum of Care is participating in the use and utilization of an HMIS system called Servicepoint/Community Services, an HMIS (Homeless Management Information System) software package. McKinney-Vento, HUD COC, DHS, ESG and many other state and federally funded grants require the use of an HMIS or comparable database (domestic violence victims service providers) to collect and report accurate data to funders. This data is beneficial in strategic planning throughout the continuum.

Systems Administrator Responsibilities

a. M.E.R.CY. Communities has elected to be the Lead Agency in coordinating and implementing the HMIS technology for the Heartland Continuum of Care (HCoC) agencies.

b. They provide system wide data quality and reporting.

c. They ensure compliance with software provider, security protocols, privacy and data quality.

d. They ensure compliance with all HUD, VA, SAMHSA, ESG, and all local, state and federal partner standards.

e. They ensure all agency info is accurate and up to date.

f. They ensure all agencies have received proper forms and signage.

g. They authorize end users and access levels.

h. They are responsible for all ongoing training and support for all licensed users.

Agency and End User Responsibilities

Agencies are responsible for maintaining HMIS security in their care. End Users will be responsible for entering client data.
These policies are outlined in the Master Service Agreement (Addendum A) and the HMIS End User Confidentiality Agreement (Addendum B)

Policy: Initial Implementation Requirements

To provide the structure of on-site support and compliance expectations, each agency must complete the following:

- Contact the HMIS System Administrator for proper forms
- Sign and return a Master Service Agreement with HCoC HMIS lead and pay the annual fee per license (this will be prorated based on date of request)
- Have appropriate Internet Access along with acceptable anti-virus software

- Determine what staff will be licensed users. The agency must only authorize users who need access to the system for technical administration, data entry, editing of client records, viewing of client records, report writing, and/or administration of other essential activity associated with carrying out HMIS responsibilities.
- All users will sign the End User Confidentiality Agreement.
- HMIS System Administrator will then setup at minimum a 2-hour training and conduct such training or give access to the Heartland Learning Management Software (LMS) and monitor user progress until completion. Completion of HMIS training will be required. There will also be modules available at the discretion of the CoC of which some or all would be required components for new case workers. These modules would be comprised of current and future training of how the entire systems of a CoC should work and not just the HMIS aspect.
- New user will then have full access to the system.
- Ongoing and new training opportunities would be available at the users pace in the LMS once that has been implemented.

Policy: Users and User Licenses

1. A User License will be required for all those given access to the database whether their function is to complete data entry or to generate reports. Licenses within a particular organization may be transferred as staff members leave and replacements are hired.
    a. The URL to the HMIS site should never be sent via email with the User ID and Temporary Password. Send the information in two emails to maintain security. The User will sign onto the site and change the password upon receiving his/her temporary password.
    b. Client information shall never be sent via email unless it is in client ID form only.
2. All those who are given user access to the database must have signed the User Agreement with Privacy Policy and completed User Training.
3. After the Provider Site and subsequent projects are completed, the System Administrator will add the users to the site according to their workflow plan.
4. User Profile Issues: The System Administrator (SA) will issue a License to Servicepoint and one for the Business Objects Reporting site (BO)'
5. Agencies MUST contact the SA within 48 hours of user's employment termination to deactivate their profile and license for security purposes.

Policy: Federal/State Confidentiality Regulations

- The agency will abide specifically by federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2, regarding disclosure of alcohol and/or drug abuse records. In general terms, the federal regulation prohibits the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by

42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The agency understands the federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.

- The agency will abide specifically, when applicable, with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and corresponding regulations passed by the Federal Department of Health and Human Services. In general, the regulations provide consumers with new rights to control the release of medical information, including the right: to give advance consent prior to disclosures of health information; to see a copy of health records; to request a correction to health records; to obtain documentation of disclosures of health information; to obtain an explanation of privacy rights and to be informed about how information may be used or disclosed. The current regulation provides protection for paper, oral and electronic information.
- The agency will abide by Illinois State Laws and Federal Laws related to confidentiality and security of medical, mental health and substance abuse information.
- The agency will provide a verbal explanation of the HMIS and arrange, when possible, for a qualified interpreter or translator for an individual not literate in English or having difficulty understanding the Privacy Notice or consent form(s).
- The agency will not solicit or input information from clients into the HMIS unless specific information proves essential to provide services, to develop reports and provide data, and/or to conduct evaluations and research. In all cases, the agency shall maintain compliance with all state and federal laws regarding research, evaluation, and confidentiality of individual client identities.
- The agency will not divulge any confidential information received from the HMIS to any organization or individual without proper written consent by the client (or guardian where appropriate) unless otherwise permitted by relevant regulations or laws.
- The agency will ensure that every person issued a User Identification and Password to the HMIS will comply with the following:
    - The HMIS Policy and Procedure Manual
    - The HMIS End User Confidentiality Agreement stating an understanding of, and agreement to, comply with HMIS confidentiality and ethical practices.
    - Create a unique User I.D. and password; and will not share or reveal that information to anyone by written or verbal means.
    - Will comply with the Master Service Agreement.
- The agency understands that all client information is encrypted on file servers physically located in a locked facility with controlled access, at the offices of Bowman Internet Systems, a Division of Wellsky, located at 11711 West 79th St, Lenexa, Kansas 66214
- Wellsky has provided Mercy Communities with copies of their Privacy policies and Security Policies and Protocols. This can be viewed in person by appointment at 1344 North 5th Street, Springfield, Illinois 62702.

Policy: Confidentiality

1) **Compliance** Agency privacy practices will comply with all applicable laws governing HMIS client privacy/confidentiality. Applicable standards include but are not limited to the following.
    a) Federal Register Vol. 69, No. 146 (HMIS FR 4848-N-02) - Federal statute governing HMIS information.
    b) HIPAA - the Health Insurance Portability Act.
    c) 42 CFR Part 2. - Federal statute governing drug and alcohol treatment.

2) **Use of Information** PPI (protected personal information that is information which can be used to identify a specific client) can be used only for the following purposes:
   a) To provide or coordinate services to a client.
   b) For functions related to payment or reimbursement for services.
   c) To carry out administrative functions such as legal, audit, personnel, planning, oversight, and management functions.
   d) For creating de-personalized client identification for unduplicated counting.
   e) Where disclosure is required by law.
   f) To prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.
   g) To report abuse, neglect, or domestic violence as required or allowed by law.
   h) Contractual research where privacy conditions are met (including a written agreement).
   i) To report criminal activity on agency premises.
   j) For law enforcement purposes in response to a properly authorized request for information from a properly authorized source.
   -See Federal Register FR-4848-N-02, Section 4.1.3, Pages 45928-29 or contact System Administrator for guidance.

NOTE: if a client refuses to release PPI, and such information is needed/required in order to provide services, the client's refusal may necessitate denial of service. Agencies may choose to make provisions for such denial of services in their policy.

3) **Collection and Notification** Information will be collected only by fair and lawful means with the knowledge or consent of the client.
   a) PPI will be collected only for the purposes listed above.
   b) Clients will be made aware that personal information is being collected and recorded.
   c) A written sign will be posted in locations where PPI is collected. (see Addendum E) This written notice will read:

"We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve our services for homeless persons, and to better understand the needs of homeless persons. We collect only information that we consider to be appropriate. **If you feel that there has been a breach of PPI, please contact HMIS administrator located at Mercy Communities 217-753-1358 or info@mercycommunities.org."**

4) **Data Quality**
   a) PPI data will be accurate, complete, timely, and relevant.
   b) All PPI collected will be relevant to the purposes for which it is to be used.
   c) Data will be entered in a consistent manner only by authorized users.
   d) Data will be entered in as close to real-time data entry as possible.
   e) Measures will be developed to monitor data for accuracy and completeness and for the correction of errors.

- The Lead Agency (M.E.R.C.Y.) runs reports and queries monthly to help identify incomplete or inaccurate information.
- The Lead Agency (M.E.R.C.Y.) monitors the correction of incomplete or inaccurate information.

f) Data quality is subject to routine audit by the System Administrator who has administrative responsibilities for the database. There is currently a Data Quality Management Plan in the works and will be added as Addendum J once completed.

5) **Record Access and Correction** Provisions will be maintained for the access to and corrections of PPI records.
   a) Clients will be allowed to review their HMIS record within 5 working days of a request to do so.
   b) During a client review of their record, an agency staff person must be available to explain any entries the client does not understand.
   c) The client may request to have their record corrected so that information is up-to-date and accurate to ensure fairness in its use.
   d) When a correction is requested by a client, the request will be documented, and the staff makes a corrective entry if the request is valid.
   e) A client may be denied access to their personal information for the following reasons:
      - Information is compiled in reasonable anticipation of litigation or comparable proceedings,
      - Information about another individual other than the agency staff would be disclosed,
      - Information was obtained under a promise of confidentiality other than a promise from this provider and disclosure would reveal the source of the information
      - Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.
   f) A client may be denied access to their personal information in the case of repeated or harassing requests for access or correction. However, if denied, documentation will be provided regarding the request and reason for denial to the individual and be made a part of the client's record.
   g) A grievance process may be initiated if a client feels that their confidentiality rights have been violated, if access has been denied to their personal records, or if they have been put at personal risk, or harmed.
   h) Any client grievances relative to HMIS will be processed/resolved according to agency grievance policy.

6) **Accountability** Processes will be maintained to ensure that the privacy and confidentiality of client information is protected, and staff is properly prepared and accountable to carry out agency policies and procedure that govern the use of PPI data.
   a) Grievances may be initiated through the agency grievance process for considering questions or complaints regarding privacy and security policies and practices. All users of the HMIS must sign a User's Agreement that specifies each staff person's obligations with regard to protecting the privacy of PPI and indicates that they have received a copy of the agency's Privacy Notice and that they will comply with its guidelines.
   b) All users of the HMIS must complete formal training administered by the System Administrator only, in person or via LMS.
   c) A process is maintained to document and verify completion of training requirements. These worksheets are kept in the HMIS under the user's credentials.

7) **Sharing of Information**

a) Clients have the option to share or not share the data collected with other agencies. If they opt to share, the only data seen by outside agencies is listed below.

- Full name, date of birth, race, ethnicity, veteran's status and social security number. This same information is shared for all family members listed in their household, unless otherwise specified.
- Identifying and/or historical information regarding and services received.
- Housing information which may include type of housing prior, current housing situation, homelessness dates, and chronic determination.
- Income information which may include income source and amounts, employment information including TANF, WIC, SNAP, SSI, SSDI, and other benefits.
- Legal history/information
- Medical history and health insurance information
- Needs, Services and Referrals for specific needs, along with the outcomes of such.
- Coordinated Entry information including Place Value Housing scores, needs assessments and placement.

b) No confidential/restricted information received from the HMIS will be shared with any organization or individual without proper written consent by the client, unless otherwise permitted by release of information forms and applicable regulations or laws.

c) Restricted information, including progress notes and psychotherapy notes, about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence concerns shall not be shared with other participating Agencies without the client's written, informed consent as documented on an Agency-modified Authorization for Release of Confidential Form.

d) If a client has previously given permission to share information with multiple agencies, beyond identifying information listed under a) and non-restricted service transactions, and then chooses to revoke that permission with regard to one or more of these agencies, the effected agency/ agencies will be contacted accordingly, and those portions of the record, impacted by the revocation, to will be locked from further sharing.

e) All HCoC ROI forms will include an expiration date, and once a Client ROI expires, any new information entered will be closed to sharing until a new ROI can be submitted. This ROI is valid for 24 months or 2 years from date of signature.

8) **System Security**

a) Password Access:

- Only individuals who have completed Privacy and System Training may be given access to the HMIS through User IDs and Passwords.
- Temporary/default passwords will be changed on first use.
- Access to PPI requires a user name and password at least 8 characters long and using at least one number and one letter and 1 symbol.

- Passwords will not use or include the users name or the vendor name and will not consist entirely of any word found in the common dictionary or any of the above words spelled backwards.
- Username and password may not be stored or displayed in any publicly accessible location
- Passwords must be changed every 45 days.
- Users must not be able to log onto more than one workstation or location at a time.
- Individuals with User IDs and Passwords will not give, or share assigned User ID and Passwords to access the HMIS with any other organization, governmental entity, business, or individual or supervisor in their organization.

b) Virus Protection and Firewalls:

- Commercial virus protection software will be maintained to protect HMIS system from virus attack.
- Virus protection will include automated scanning of files as they are access by users.
- Virus Definitions will be updated regularly.
- All workstations will be protected by a firewall either through a workstation firewall or a server firewall.
- Data downloaded for purposes of statistical analysis will exclude PPI whenever possible.
- HMIS data downloaded onto a data storage medium must be disposed of by reformatting as opposed to erasing or deleting.
- A data storage medium will be reformatted a second time before the medium is reused or disposed of.

c) System Monitoring

- User access to the HMIS Live Web Site will be monitored using the specialized reports located in the HMIS software.

d) Hard Copy Security*:*

- Any paper or other hard copy containing PPI that is either generated by or for HMIS, including, but not limited to report, data entry forms and signed consent forms will be secured.
- Agency staff will supervise at all-time hard copy with identifying information generated by or for the HMIS when the hard copy is in a public area. If the staff leaves the area, the hard copy must be secured in areas not accessible by the public.
- All written information pertaining to the username and password must not be stored or displayed in any publicly accessible location.

Policy: Information Security Protocols

User Access Privileges to HMIS Database

- The System Administrator will determine user access levels. User accounts will be created and deleted by the System Administrator under authorization of the agency's Executive Director.
- The System Administrator will manage the proper designation of user accounts and will monitor account usage.

- The System Administrator will generate username and temporary passwords within the Administrative function of the HMIS. The URL address will be sent separately from the temporary username/password for security purposes.
    - The System Administrator will create all usernames using the First Initial of First Name and Last Name. Example John Doe's username would be jdoe. If there are two people with the same first initial and last name, a sequential number should be placed at the end of the above format. Ex. jdoe2, jdoe3.
        - Passwords are automatically generated from the system when a user is created. System Administrators will communicate the system-generated password to the user.
        - The user will be required to change the password the first time they log onto the system. The password must be between 8 and 16 characters and be alphanumeric along with symbols. Passwords should not be able to be easily guessed or found in a dictionary.
        - Any passwords written down should be securely stored and inaccessible to other persons. Users should not store passwords on a personal computer for easier log on.
        - Passwords expire every 45 days. Users may not use the same password consecutively.
        - The System Administrator will terminate the rights of a user immediately upon termination from their current position. The agency is responsible for contacting the System Administrator should this occur. If a staff person is to go on leave for a period of longer than 45 days, their password should be inactivated within 5 business days of the start of their leave. The System Administrator is responsible for removing users from the system.
        - If a user unsuccessfully attempts to logon 3 times, the user id will be "locked out", access permission revoked and unable to gain access until their password is reset by clicking on the "Forgot password" link where they will receive an email resetting their password.
        - **Passwords** are the individual's responsibility, and users cannot share passwords.
- Agency staff will not engage in electronic transmission of user IDs and passwords, except for first-time, temporary passwords or encryption keys.
- The Agency Executive Directors will inform Systems Administrator of any changes in personnel to ensure training of new personnel.
- Access to the software system will only be allowed from computers specifically identified by the Executive Director and Agency Administrator.
- Users will only be able to view the data entered by users of their own agency. Agencies are restricted from viewing each other's information unless specific sharing agreements have been negotiated. Items that can be viewed by all agencies include client's name and demographics, Household data, and entry/exit dates and what programs they were enrolled in from other agencies.
    - Effective July 2017. A Hybrid system has now been implemented allowing for data sharing. The data that will now be shared includes the above data along with the answers to all questions on the entry or exit into Servicepoint. This data will flow from one exit into another entry at another agency. This will allow for better communication on implementation of Coordinated Entry Policy.

Policy: Security Incidents

- The HMIS Lead must implement a policy and chain of communication for reporting and responding to security incidents. Stated below.
- The participating agency and HMIS Lead will post the Privacy Notice anywhere HMIS data is collected or accessed that articulates the reporting mechanism for suspected breaches of client confidentiality. The notice will include contact information for the agency's HMIS Security Officer. The notice will include additional instructions for reporting anonymously.
- The participating agency and HMIS Lead will maintain records of all security incidents, responses, and outcomes.
    - Policies and Procedures are intended to prevent—to the greatest degree possible—any security incidents. However, should a security incident occur, the following procedures should be followed in reporting:
        - ➢ Any HMIS end user who becomes aware of or suspects a compromise of HMIS system security and/or client privacy must immediately report that possible incident to their agency executive director. The participating agency executive director shall inform the HMIS administrator.
        - ➢ 2.In the event of a suspected security compromise participating agency executive director should complete an internal investigation. If the suspected compromise resulted from an end user's suspected or demonstrated noncompliance with the HMIS End User Agreement, the Agency executive director should submit a request to the HMIS Lead to deactivate the end user's user ID until the internal investigation has been completed.
        - ➢ Following the internal investigation, the participating agency executive director shall notify the HMIS administrator of any substantiated incidents that may have resulted in a breach of HMIS system security and/or client privacy whether or not a breach is definitively known to have occurred. If the breach resulted from demonstrated noncompliance by an end user with the HMIS End User Agreement, the HMIS administrator and Lead agency reserves the right to permanently deactivate the User ID for the end user in question.
        - ➢ Within 1 business day after the HMIS administrator receives notice of the breach, the HMIS administrator and participating agency executive director will jointly establish an action plan to analyze the source of the breach and actively prevent future breaches. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed 30-days.
        - ➢ If the Agency is not able to meet the terms of the action plan within the time allotted, the HMIS System Administrator & HCoC may elect to terminate the Agency's access to HMIS. The Agency may appeal to the HMIS Board of Directors for reinstatement to HMIS following completion of the requirements of the action plan.
        - ➢ In the event of a substantiated breach of client privacy through a release of Personal Health Information (PHI) in noncompliance with the provisions of these Security Standards, the HMIS Policies and Procedures, or the Partner Agency Privacy Statement, the agency executive director will attempt to notify any impacted individual(s).
        - ➢ The HMIS Lead Agency will notify the Board of Directors of the Heartland Continuum of Care of any substantiated release of PHI/PPI in noncompliance with the provisions of these Security Standards, HMIS Policies and Procedures, or the Agency Privacy Statement.

- ➢ The HMIS Lead Agency will maintain a record of all substantiated releases of PHI/PPI in noncompliance with the provisions of these Security Standards, HMIS Policies and Procedures, or the Partner Agency Privacy Statement for 7 years.
- ➢ The Heartland Continuum of Care reserves the right to permanently revoke an Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, HMIS Policies and Procedures, or the Agency Privacy Statement that resulted in a release of PHI/PPI.

Policy: Training

- HMIS: All users must complete the trainings incorporating the following: Certificates will be awarded.

1. Introduction to the HMIS Project.
2. Review of applicable policies and procedures.
3. Connecting to the Internet.
4. Logging on to the HMIS System.
5. Entering client information including Intake, Assessment, Discharge and Follow-up data.
6. Ensuring good quality data.
7. Entry and Exit data integrity.
8. Overview of the HMIS Project.
9. Review of agency technical infrastructure including roles and responsibilities.
10. Review of security policies and procedures.
11. Overview of System Administrative functions.
12. Informing System Admin of updated information pertaining to the participating agency.
13. Oversight of data quality.
14. Using existing reports.
15. Using reports to monitor data quality and make corrections as needed.

- CoC Training: This list is a sampling of trainings that will be offered via Learning Management Software. These will be added to as modules are ready for use.

16. What is a Continuum of Care?
17. What is Outreach?
18. What is Emergency Shelter?
19. What is Transitional Housing?
20. What is Homeless Prevention?

21. What is Diversion?
22. What is Rapid Re-Housing?
23. What is Permanent Supportive Housing?
24. What is Other Permanent Housing?
25. What is Trauma Informed Care?
26. CPR and life saving techniques

Policy: Physical Access Control

Each agency must control physical access to the system data processing areas, equipment and media. Access must be controlled for the transportation of data processing media and other computing resources. The level of control is contingent on the level of risk and exposure to loss. Personal computers, software, documentation, disks and removable drives shall be secured proportionate with the threat and exposure to loss. Available precautions include equipment enclosures, lockable power switches, equipment identification and fasteners to secure the equipment.

Equipment Procedure

The agency must ensure that access to areas containing equipment, data, and software will be secured. All client identifying information will be strictly safeguarded in accordance with the latest technology available. All data will be securely protected to the maximum extent possible. Ongoing security assessments should be conducted on a regular basis.

- Computer hardware physical security (Locked office)
- Server software security (Location Access Controls and Username accounts)
- Network software security (Firewall protection)
- Wire security (SSL Encryption)
- Client data security
- Protected personal information is encrypted using the highest current standards and stored on the server in binary format.
- Agency Administrator will determine the physical access controls appropriate for their organizational setting based on security policies, standards and guidelines.

- All those granted access to an area or to data are responsible for their actions. Additionally, those granting another person access to an area are responsible for that person's activities

Media and hardcopy protection and transportation

- Printed versions of confidential data should not be copied or left unattended and open to unauthorized access.
- Media containing client-identified data will not be shared with any agency other than the owner of the data for any reason. Authorized employees using methods deemed appropriate by the participating agency may transport HMIS data that meet the above standard. Reasonable care should be used, and media should be secured when left unattended.
- HMIS information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

Policy: Disaster and Emergency Planning

Wellsky has procedures in place in the event of disasters to protect all data entered into HMIS. To see these policies contact HMIS System Administrator

Emergency planning will be at the request of Heartland Continuum of Care Board of Directors.

Policy: HMIS Quality Assurance Reports

HMIS will maintain an on-going process of Quality improvement. A data quality management plan is in the works and will be added as Addendum J once complete.

1) HMIS Procedures for ensuring quality:
   a) Monthly, Lead HMIS Agency (M.E.R.C.Y.) will review reports for completeness, accuracy and consistency.
   b) They will send out to participating Agencies: (unless that agency has received training on proper report functions and has agreed to run them monthly)
      i) Data Completeness Report
      ii) Clear protocols for correcting data.
      iii) DHS Tally Reports-Quarterly
      iv) Program Census Report for Shelters
      v) Annual Assessment reports for clients stays longer than 12 months.
   c) Software has error checking functions (out of range, missing values, incongruous data).

2) A sample of measures to monitor quality include the following queries:
      i) Null DOB and gender fields.
      ii) Rate of infants under the age of 1.
      iii) Gender by family relationship.

iv) HUD Assessment by entries & exits.
v) Age by family relationship.
vi) Number of users, and records on the live site.
vii) Null exit dates related to short term services.
viii) Ambiguous data in reports
ix) Any missing information that is pertinent to HUD reporting.
x) Excessive use of exit destinations of "data not collected" or "No exit interview completed"

Policy: Coordinated Entry System and Scheduled Meetings

See "Coordinated Entry System Policy and Procedures" Manual

GLOSSARY ADDENDUM

- Community Services (formerly known as Servicepoint)-An internet based HMIS developed for the purpose of client tracking & case management for HUD and non-HUD funded services provided by non-profit agencies.
- HCoC-Heartland Continuum of Care
- HMIS-Homeless Management Information System
- SA-System Administrator
- HUD-Housing and Urban Development
- APR-Annual Performance Review
- ROI-Release of Information
- DHS-Department of Human Services
- UDE-Universal Data Elements
- PSDE-Program Specific Data Elements
- NOFO-Notice of Funding Opportunity

- EULA-End User License Agreement
- PIT-Point in Time
- HIC-Housing Inventory Count
- ESG-Emergency Solutions Grant
- WIA-Workforce Investments Act
- SSI-Supplemental Security Income
- SSDI-Social Security Disability Income
- WIC-Women, Infants and children
- CANTS-Child Abuse & Neglect Tracking System
- SSVF-Supportive Services for Veterans Families
- GPD-Grant and Per Diem
- GIW-Grant Inventory worksheet
- SAGE-HUD website to upload CSV APRs for funded projects
- PATH- Projects for Assistance in Transition from Homelessness
- StellaP & StellaM-Located in HUDHDX2.0 a data tool that communities utilize
- LSA-Longitudinal Systems Analysis report
- HUDHDX/HUDHDX2.0-HUD reporting means for Continuums (HIC, PIT, LSA, SYSPM reports)
- SYSPM-System Performance reports
- LIHEAP-Home energy assistance program
- CV-19 OR COVID-19-Pandemic related funding
- CFLL-Community Foundation Land of Lincoln

AGENCY IDENTIFIERS

- AFM-Abundant Faith Ministries
- CM-Contact Ministries
- CC-Catholic Charities
- FSR-Fifth Street Renaissance
- HH-Helping Hands of Springfield
- ICM-Inner City Mission
- MBH-Memorial Behavioral Health
- MC-Mercy Communities

- PC-Phoenix Center
- SA-Salvation Army Springfield
- SHA-Springfield Housing Association
- SIU-Southern Illinois University School of Medicine
- SSVR-Spring Street Veterans Renaissance
- SUL-Springfield Urban League
- UW-United Way
- WSM-Washington Street Mission
- YSB-Youth Service Bureau

ADDENDUM A: MASTER SERVICE AGREEMENT

MOU - AGENCY MASTER AGREEMENT **FY 2020-2021**
Heartland Continuum of Care (HCoC)
Homeless Management Information System (HMIS)

The Heartland Continuum of Care (HCoC), in accordance with the US Department of Housing and Urban Development data collection mandates, participates in an HMIS system to serve its data collection and reporting requirements. Please review each section. Then, initial each point to indicate your understanding of, and agreement to, the terms and conditions of your participation in the HMIS system. Sign last page please.

Section I: Software Selection and Governance

- ☐ The HMIS system is Servicepoint (soon to be changed to Community Services), an Internet-based management information system developed by Bowman Internet Systems (BIS), a Wellsky company based in Shreveport, Louisiana & Lenexa, Kansas, for the purpose of client tracking and case management for HUD and Non-HUD funded services provided through the agency.
- ☐ To govern Servicepoint, the HCoC has chosen to implement the "HMIS Lead Organization" Governance Structure. Where the HCoC provides oversight, it shall be so indicated.
- ☐ M.E.R.C.Y. Communities (MERCY) serves as the lead Agency for the HCoC, and holds the umbrella contract with Wellsky Companies, as well as secures individual licenses for participating Agencies.
- ☐ MERCY is responsible for ensuring that the terms of the agreement with Wellsky continue to be satisfied so that all agency data remains secure. Wellsky handles the provision of disaster recovery services, daily backup of data, system maintenance and regularly scheduled product upgrades. MERCY trains and administers policies and procedures designed to protect database level security via login/password maintenance.

Section II: Password Protection-User Responsibility and Ethics Statements

- ☐ Your unique User ID and Password give you access to the HCoC HMIS.
- ☐ HCoC HMIS Users will treat clients and partner agencies with respect, fairness and in good faith, and maintain high standards of professional conduct in their capacity as an HCoC HMIS User. Failure to uphold the standards of the HCoC HMIS is grounds for immediate termination from the HCoC HMIS and may result in personnel action.
- ☐ I have been trained on how to access and use the HCoC HMIS system and will abide by the security protocols as provided to me during said training.
- ☐ **My User ID and Password are for my use only and must not be shared with anyone including my Agency Administrator and Executives.**
- ☐ I will take reasonable means to keep my password physically secure.
- ☐ A computer that has the HCoC HMIS open and running should never be left unattended. Failure to log off the HCoC HMIS appropriately may result in a breach in client confidentiality and/or system security. Therefore, I will log off of the HCoC HMIS each time I use it.
- ☐ Hard copies of client information printed from the HCoC HMIS must be kept in a secure file. When hard copies are no longer needed, they must be properly destroyed to maintain confidentiality.

- ☐ Electronic files exported from the HCoC HMIS must be password protected to maintain confidentiality.

Section III: Operations and Compliance

- ☐ MERCY provides set-up, training and ongoing support to HCoC participating agencies.
- ☐ Further technical support as needed is provided by Wellsky's secured support network called Wellsky Portal. As the lead agency, MERCY works directly with Wellsky on behalf of the HCoC participating agencies through this system for all issue tracking, and participating agencies are **not** authorized to contact Wellsky directly. Additions, enhancement requests and changes must be channeled through MERCY as the lead agency.
- ☐ Participating agencies will operate in accordance with HUD's published HMIS Data and Technical Standards, as published and regularly updated at this link.
  https://www.hudexchange.info/resources/documents/HMIS-Data-Dictionary.pdf
- ☐ Participating agencies will comply with all HCoC HMIS operating procedures, as provided in the training and accessible online within the Wellsky software. And, further agrees to monitor its users for adherence to security and privacy policies.
- ☐ The HCoC has the right to terminate this agreement at any time if the standard operating procedures are not followed.
- ☐ A feedback mechanism regarding Lead Agency performance is in place through monthly meetings of the HCoC and direct contact to the HCoC Chair and Administrator.

Section IV: Data Quality, Data Sharing and Data Release

- ☐ Data Quality Standards are set at the highest level that may be achieved. These comply with the HUD specifications, which are monitored on a monthly basis. MERCY, as the lead Agency, shall run the following reports for ensuring compliance with Data Quality Standards, and distribute to each participant Agency:
  - Duplicate Clients Report (Done internally)
  - Data Incongruity Locator Reports
  - Data Completeness Report Card **AND/OR**
  - HUD CoC APR Data Quality/Completeness
- ☐ If any information contained in these HMIS generated reports is inaccurate, the participating Agency agrees to correct the information immediately, as the data integrity of each Agency is critical to the overall data reporting for the HCoC.
- ☐ Data Sharing – Per agreement of the HCoC participating Agencies, the following data sharing occurs: Client Name, Social Security Number, DOB, Gender, Race, Ethnicity, Type of Household, Entry/Exit data, Identifying or historical information, Housing information, Income Information, Legal history/information, Medical information, health insurance and services needed/provided and the outcomes of such of all members of the client's household. Also included in sharing will be any assessments agreed upon for use in compliance with Coordinated Assessment such as VI-SPDAT, VI-TAY-SPDAT, VI-FSPDAT but not limited to these.
- ☐ This information can only be accessed by the HCoC Participating authorized HMIS users. This ensures that the HCoC is not duplicating individuals and also provides a better understanding of the service usage within the HCoC. This was by the agreement of the HCoC participating agencies and subsequently programmed as such by Wellsky

☐ Data Release – Requests of Data shall only be honored from authorized individuals in participating Agencies. MERCY shall never provide your data or reports to any outside entity. MERCY shall take the position that each Agency has the authority to release their own information consistent with their privacy policies. Generally, an Agency's aggregate data and reports would be for purposes of obtaining or reporting on grants. Individual client data should only be released with specific client consent to provide information to a named recipient.

Section V: Policy Development and Oversight

☐ Client Confidentiality and Privacy Training is provided upon initial set-up with a new user. User ensures that client confidentiality and data privacy is maintained at their Agency. If a suspected breach has occurred, Agency agrees to contact the lead Agency immediately.

☐ Community Planning Goals and Objectives are provided through the Strategic Plan of the HCoC, which the HMIS supports.

☐ Business and Best Practices are provided at the initial training and set-up. As new information or upgrades occur, the Lead Agency shall distribute to all participants.

☐ Program Funding and Orientation is provided by the HCoC via several funding partners.

☐ MERCY Communities maintains the documents of agreements at its' main headquarters in Springfield, IL.

☐ Participation Rates are overseen by the HCoC, who also oversees the ongoing community engagement activity and barrier resolution occurring with non-participants.

☐ MERCY ensures that Wellsky maintains the existence of HMIS Policy and Use documentation. MERCY is also available during normal business hours to answer questions, provide interpretation or support, and to travel to participating Agencies as needed to maintain the highest level of HMIS support possible to all participants

☐ Each participating Agency must have Client Consent protocol to guide its data collection efforts. By initialing, you assert that you have such consent forms in place at your Agency and can provide upon notice.

The signing of this Master Service Letter of Agreement certifies understanding and concurrence with the terms and conditions of the Heartland Continuum of Care's HMIS System.

AGENCY: _____

Signature of Executive Director: _____ **Date:** _____

HCoC - HMIS Lead Agency: M.E.R.C.Y. Communities, Inc.

Amy Voils, Executive Director

Signature: Amy Voils **Date:** June 12, 2020

Tracie Cunningham, HMIS Administrator

Signature: Tracie Cunningham **Date:** June 12, 2020

RETURN SIGNED AGREEMENT TO:
M.E.R.C.Y. Communities
1344 N. 5th Street
Springfield, IL 62702
(217) 753-1358

ADDENDUM B: END USER CONFIDENTIALITY AGREEMENT

Heartland Continuum of Care

HMIS/Servicepoint End User-Confidentiality Agreement

This agency recognizes the privacy of client needs in the design and management of the Homeless Management Information System (HMIS) called Community Services formerly known as Servicepoint. These needs include both the need to continually improve the quality of homeless and housing services with the goal of eliminating homelessness in our community, and the need to vigilantly maintain client confidentiality, treating the personal data of our upmost vulnerable populations with respect and care. As the guardians entrusted with this personal data, HMIS users have a moral and a legal obligation to ensure that the data they collect is being collected, accessed and used appropriately. It is also the responsibility of each user to ensure that client data is only used to the ends to which it was collected, ends that have been made explicit to clients and are consistent in assisting families and individuals in our community to resolve their housing crisis. Proper user training, adherence to the HMIS Policies and Procedures and a clear understanding of client confidentiality are vital to achieving these goals.

By executing the agreement, you agree to abide by the following client confidentiality provisions:

1. A Heartland Continuum of Care Release of Information form must be completed by each Head of Household or unaccompanied youth and include all members of their family experiencing this hardship or seeking services. **This form is not an "option".** Whether they Share or do not share is irrelevant, it is an acknowledgement of being informed of their rights.

2. Personal User Identification and Passwords must be kept secure and are not to be shared.

3. Client consent may be revoked by that client at any time through a written notice from client or advocate of.

4. No client may be denied services for "not sharing" their data in the HMIS.

5. Only general, non-confidential information is to be entered in the "Client Notes" section of the Client Profile in Community Services. Confidential information, including TB diagnosis, domestic violence and mental and/or physical health information, is not permitted to be entered in this section.

6. Clients have the right to inspect, copy, and request changes in their HMIS records based on validity of request.

7. HMIS users may not share client data with individuals or agencies that have not entered into an HMIS Master Service Agreement and/or have a valid release of information from client.

8. Discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, or sexual orientation are not permitted in the HMIS. Profanity and offensive language are not permitted in the HMIS. These items are only permitted in case notes where documenting is necessary.

9. HMIS users will maintain data in such a way as to protect against revealing the identity of clients to unauthorized agencies, individuals, other clients or entities.

10. Any HMIS user found to be in violation of the HMIS Policies and Procedures, or the points of client confidentiality in this agreement, may be denied access to the HMIS and/or proper discipline from their agency and/or Heartland Continuum of Care.

I affirm the following:

1. I have received training in proper use of the HMIS/Community Services formerly known as Servicepoint.

2. I have received and will abide by all policies and procedures in the HMIS Policies and Procedures Manual.

3. I will maintain the confidentiality of client data in the HMIS/Community Services as outlined above.

4. I will only collect, enter and extract data in the HMIS/Community Services relevant to the delivery of services to people experiencing a housing crisis or needing services in our community and that is necessary to perform my job.

5. If I notice or suspect a security breach, I must notify my supervisor and the HMIS Administrator immediately.

Your signature below indicates your agreement to comply with this statement of confidentiality. There is no expiration date of this agreement.

User's Signature	Title/Agency Name M.E.R.C.Y. Communities	Date
HMIS System Administrator	Agency	Date

ADDENDUM C: PROJECT DATA DESCRIPTORS AND BED/UNIT INVENTORY

ADDENDUM D: FEDERAL PARTNER FUNDING SHEET

Data Standards- HUD Required		Bed and unit

Program & Agency Name_____

Printed name_____ **Signature**_____

Executive Director Signature verifying all of the funding sources are accurate for 20XX Housing Inventory Count

FederFeal Federal Partner Funding Sources **Is funding directly from Federal partner?**

If not, from who? Grant Number (Identifier) **Grant**

start date **Grant**

end date

McKinney-Vento Funding
- HUD: CoC-Permanent Supportive Housing
- HUD: CoC-Rapid Re-Housing
- HUD: CoC-Transitional Housing
- HUD: CoC-TH-RRH
- HUD: CoC- Single Room Occupancy (SRO)
- HUD:ESG-Emergency Shelter
- HUD:ESG-Rapid Re-Housing
- HUD:ESG-Youth Homeless Demonstration Program (YHDP)
- Shelter Plus Care Program (S+C)
- Supportive Housing Program (SHP)
- Section 8 Moderate Rehabilitation Single room occupancy (SRO), including grants formerly funder under McKinney-Vento but renewed under Section 8

Additional Federal Funding
- HUD:HOPWA – Hotel/Motel Vouchers
- HUD:HOPWA – Permanent Housing (facility based or TBRA)
- HUD:HOPWA – Short-Term Supportive Facility
- HUD:HOPWA – Transitional Housing (facility based or TBRA)
- HHS:PATH – Street Outreach & Supportive Services Only
- HHS:RHY –Basic Center Program (prevention and shelter)
- HHS:RHY –Maternity Group Home-Pregnant & Parenting Youth
- HHS:RHY –Transitional Living Program
- HHS:RHY –Demonstration Project
- HUD:VA Supportive Housing (HUD-VASH)
- VA: Supportive Services for Veteran Families
- VA: Healthcare for Homeless Veterans
  - VA:CRS Contract Residential Services
  - VA: Community Contract Safe Haven Program (HCHV/SH)
- VA: Grant and Per Diem Program

VA:GPD Bridge Housing
VA:GPD Low Demand
VA:GPD Hospital to Housing
VA:GPD Clinical Treatment
VA:GPD Service Intensive Transitional Housing
VA:GPD Transitional in Place

ADDENDUM E: AGENCY SIGNAGE

"WE COLLECT PERSONAL INFORMATION DIRECTLY FROM YOU FOR REASONS THAT ARE DISCUSSED IN OUR PRIVACY STATEMENT. WE MAY BE REQUIRED TO COLLECT SOME PERSONAL INFORMATION BY LAW OR BY ORGANIZATIONS THAT GIVE US MONEY TO OPERATE THIS PROGRAM.
OTHER PERSONAL INFORMATION THAT WE COLLECT IS IMPORTANT TO RUN OUR PROGRAMS, TO IMPROVE SERVICES FOR HOMELESS PERSONS, AND TO BETTER UNDERSTAND THE NEEDS OF HOMELESS PERSONS. WE COLLECT ONLY INFORMATION THAT WE CONSIDER TO BE APPROPRIATE."

If you feel that there has been a breach of PPI, please contact HMIS administrator located at Mercy Communities 217-753-1358 or info@mercycommunities.org.

ADDENDUM F: RELEASE OF INFORMATION/CLIENT DATA SHARING

Heartland Continuum of Care
Client Consent-Release of Information

The Homeless Management Information System (HMIS) serves the Heartland Continuum of Care, a group of partner agencies working together to provide services to the homeless and low-income individuals and families in the community. Heartland Continuum of Care is also partnered with other Continuums of Care that provide services in the urban areas of the state. The agencies in the Statewide Continuum of Care include shelter, housing, food, state, private, and non-profit social service agencies, and faith-based organizations.

The information that is collected in the HMIS database is protected by limiting access to the database and by limiting with who the information may be shared, in compliance with the standards set forth in the Health Insurance Portability and Accountability Act (HIPAA). Every person and agency that is authorized to read or enter information into the database has signed an agreement to maintain the security and confidentiality of the information. Any person or agency that is found to violate their agreement may have their access rights terminated and may be subject to further penalties.

If you choose to share your information:
I authorize the partner agencies and their representatives to share the following information regarding my family and me. I understand that this information is for the purpose of assessing our needs for housing, utility assistance, food, counseling, and/or other services.

This information may consist of the following:

- **My name, date of birth, race, ethnicity, Social Security number and the same information from any other family members of my family who are being served with me at this time.**
- **Identifying and/or historical information regarding myself and members of my household.**
- **Housing information (may include type of housing prior, reason for homelessness)**
- **Income Information (sources and amount of household income, employment information)**
- **Legal History/information**
- **Medical and Health Insurance information**
- **Services needed and provided; outcome of services provided**

I understand that:

- **Details of your physical or mental health issues will NEVER be shared with other partner agencies.**
- **The partner agencies have signed agreements to treat my information in a professional and confidential manner. I have the right to view the client confidentiality policies used by the HMIS.**
- **Staff members of the partner agencies who will see my information have signed agreements to maintain confidentiality regarding my information.**
- **The partner agencies may share non-identifying information about the people they serve with other parties working to end homelessness.**
- **The release of my information does not guarantee that I will receive assistance, and my refusal to authorize the use of my information does not disqualify me from receiving assistance.**
- **This authorization will remain in effect for 24 months (2 Years) unless I revoke it in writing, and I may revoke authorization at any time by signing written statement available at my partner agency.**
- **If I revoke my authorization, all information about me already in the database will remain, but it will become invisible to all of the partner agencies.**
- **If I refuse this authorization, my information will still be entered into the HMIS however it will be invisible to all of the partner agencies.**
- **I have the right to request information about who has accessed my information.**
- **A listing of the partner agencies within the Heartland Continuum of Care may be viewed prior to signing this agreement**

PLEASE CHECK ONE BOX: ❑OK TO SHARE ❑DO NOT SHARE

Client Name (Please Print)	Client Signature	Date

Agency Name	Agency Personnel Signature	Date

ADDENDUM H: DATA QUALITY MANAGEMENT PLAN
(Under construction)