HMIS Policies and Procedures Manual, Data Quality Plan, Privacy Plan, Security Plan, and Governance Charter

Cincinnati/Hamilton County CoC, Strategies to End Homelessness HMIS Lead

HMIS Policy and Procedures

Introduction

The Homeless Management Information System (HMIS) is a local information computerized system meant to collect information on persons who are experiencing homelessness to better serve their needs. It is designated by the Cincinnati/Hamilton County Continuum of Care (CoC) OH-500 to comply with the requirements of CoC Program interim rule 24 CFR 578. It is implemented to provide an unduplicated count of participants served as well as record and analyze participant, service, and housing data for individuals and families who are homeless or at risk of homelessness. Data entered into the HMIS is used to track and improve services for individuals and families, understand the needs of people experiencing homelessness in our community, identify gaps in service, and secure funding for local homeless and homeless prevention projects. Aggregate data is also used by HUD and other policymakers at the federal, state, and local levels to facilitate funding for persons experiencing homelessness.

This manual is developed by the Strategies to End Homelessness HMIS Department and authorized by the Cincinnati/Hamilton County Continuum of Care (CoC) Board, locally known as the Homeless Clearinghouse. The manual was made available to Agency HMIS Primary Point Persons, also known as Agency HMIS Leads, and various workgroups for review and comment during a revisions period. Their feedback was used to produce the final approved manual.

The purpose of this manual is to guide and clarify federal regulations related to HMIS for Cincinnati/Hamilton County Continuum of Care (CoC) OH-500 agencies in their daily operations. In no way should this document serve as a substitute for any federal regulations outlined and updated by HUD in its 2004 HMIS Data and Technical Standards. All Cincinnati/Hamilton County Continuum of Care (CoC) OH-500 agencies are responsible for maintaining their own compliance with federal, state, and local regulations as well as any outside applicable regulations such as the Health Insurance Portability and Accountability Act (HIPAA) standards if applicable.

The HMIS Software for the Cincinnati/Hamilton County Continuum of Care (CoC) OH-500 is Clarity Human Services by Bitfocus.

HMIS Lead Agency Contact Information

KManning@end-homelessness.org	STEH HMIS Director
HMISsupport@end-homelessness.com	HMIS Support Email monitored by support team to answer all HMIS related questions including, user maintenance, report and dashboard inquiries, and data quality concerns
513 – 263 - 2790	HMIS Support Line open Monday – Friday 9:00am-3:00pm (excluding STEH holidays
HMIS Knowledgebase - https://steh.freshdesk.com/support/solutions	HMIS Support Knowledgebase with step-by-step guides and information on most HMIS features and processes. These articles are written and updated by the STEH HMIS Support Team
STEH YouTube Channel - https://tinyurl.com/2p92tzey	Strategies to End Homelessness YouTube Channel with videos demonstrating many HMIS processes.
HMIS On-Demand Training - https://steh.talentlms.com/	HMIS Training Courses On Demand Course List : (freshdesk.com)
https://help.bitfocus.com	Help articles published by the HMIS vendor Bitfocus

Definitions

Cincinnati/Hamilton Continuum of Care (CoC) - A Continuum of Care (CoC) is a collaborative funding and planning approach that helps communities plan for and provide a full range of emergency, transitional and permanent housing, along with prevention and other services to address the various needs of persons experiencing homelessness. HUD also refers to the group of community stakeholders involved in the decision-making process as the "Continuum of Care."

Homeless Clearinghouse – The Cincinnati/Hamilton County CoC Board is known locally as the Homeless Clearinghouse. The CoC board is the collective of individuals designated to provide oversight and governance on behalf of the CoC. The CoC Board's responsibilities are defined by the CoC and are described in the CoC's governance charter. The CoC Board must be representative of the relevant organizations and projects serving homeless populations and subpopulations within the CoC's geographic area. The CoC Board must also include at least one person who is currently or has previously experienced homelessness.

CoC Lead/Unified Funding Agency (UFA)– Strategies to End Homelessness is designated by the OH-500 Governance Charter as the CoC Lead and applies annually for UFA Designation. The CoC Lead is selected by the CoC to fulfill the duties in the CoC Program Interim Rule. A Unified Funding Agency (UFA) is a Collaborative Applicant selected by the CoC (and approved by HUD) to apply for, receive, and distribute funding for all projects in a CoC. The UFA is the sole grant recipient for the CoC; HUD signs a grant agreement with the UFA and the UFA signs separate grant agreements with each subrecipient carrying out the CoC-funded projects.

Homeless Management Information System (HMIS) - The information system designated by the CoC to comply with the HMIS requirements prescribed by HUD.

HMIS Lead - Strategies to End Homelessness, the entity designated by the Clearinghouse to operate the CoC's HMIS on its behalf. Section VI of the OH-500 Governance Charter designates Strategies to End Homelessness as the HMIS Lead and HMIS Administrator for the CoC.

HMIS Support Team – Members of the HMIS Lead Agency who provide training, user support, and system administration responsibilities regarding the HMIS. Also referred to as STEH HMIS Department or HMIS Administrators/Staff.

Contributing HMIS Organization (CHO) - An organization that operates a project that contributes data to an HMIS.

CHO HMIS Primary Point Person (PPP)– Each CHO must designate a Primary Point Person (previously known as the Agency HMIS Lead) who will approve new users, approve customization requests, participate in regularly scheduled HMIS update meetings, be the point person for HMIS contacts with the CHO, and represent the CHO's interest through feedback to the HMIS Lead Agency.

CHO Security Officer – Each CHO must designate a staff member to perform an annual security review and ensure compliance with applicable security standards (this can be the same person as the Primary Point Person or a separate individual).

HMIS End User – An individual who uses or enters data in an HMIS or another administrative database from which data is periodically provided to an HMIS.

Program Participant/Participant– Persons whose data is entered into HMIS and receive services from CHOs.

Victim Services Provider – a private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking.

Personally Identifiable Information (PII) or Protected Personal Information (PPI) -Any information maintained by or for a HMIS about a person experiencing homelessness that:

- Can be used directly or indirectly to identify a specific individual.
- Can be linked with other available information to identify a specific individual.
- Can be reasonably manipulated to identify a specific individual.

For more key terms, definitions, and acronyms, HMIS, CoC, and other Acronyms : (freshdesk.com) or Homeless Management Information Systems - Implementation Guide - Glossary (hud.gov)

Grant Management Requirements and Process

Governance

Homeless Clearinghouse, Cincinnati/Hamilton County CoC Board

Policy: The Homeless Clearinghouse, provides a leadership role for the Cincinnati/Hamilton County Continuum of Care (CoC) HMIS including:

1) Designation and annual review of the HMIS Lead Agency.
2) Designation and annual review of the HMIS software application/vendor.
3) Review, revision, and approval of the HMIS Policy and Procedures Manual including:
    a. The HMIS Governance Charter
    b. The Data Quality, Data Privacy, and Data Security Plans
    c. The HMIS Agency Participation Agreement
    d. The HMIS User Agreement
    e. The HMIS Privacy Notice and Client Consent Form.
4) Ensures -consistent participation of HUD-funded recipients and subrecipients in the HMIS; and encourages and facilitates 100% HMIS participation regardless of partner funding source or HUD mandate.
5) Ensure STEH HMIS is administered in compliance with requirements prescribed by HUD.

Explanation: Consistent with the CoC Governance Charter, The Homeless Clearinghouse will conduct a certification process to recommend either renewal or new designation of the HMIS Lead and HMIS Vendor every five years. The Homeless Clearinghouse will also conduct an annual review process for satisfactory performance of the HMIS Lead Agency and HMIS Vendor.

The Homeless Clearinghouse, in conjunction with the HMIS Lead Agency, will conduct a periodic review of the HMIS system and will conduct a Request for Proposal (RFP) process for current HMIS systems available on the market at least every ten years.

HMIS Policies and Procedures will be reviewed annually for approval or required revisions. The CoC community of stakeholders, including CHOs, HMIS End Users, HMIS Lead, or UFA/CoC Lead may also request revisions to the HMIS Policies and Procedures. All revisions will be distributed to the CHO Primary Point Person and relevant CoC

workgroups for comment and discussion as is consistent with the CoC Policies and Procedures and presented to the Homeless Clearinghouse for review, revisions, and final approval. Cincinnati/Hamilton County CoC HMIS Policies and Procedures Manual will be implemented as current only after the final approval vote from the Homeless Clearinghouse.

Strategies to End Homelessness (STEH), UFA, and CoC Lead

Policy: STEH, in its role as UFA and CoC Lead Agency, ensures the HMIS is in compliance with HUD rules and regulations, provides a leadership role in conjunction with the Homeless Clearinghouse, and other duties as outlined in the HMIS Governance Charter Key Roles and Responsibilities (in Appendix D).

Explanation: STEH will monitor HMIS for compliance with HUD rules and regulations, negotiate and execute contract(s) with the HMIS vendor(s), execute HMIS Agency Participation Agreements, and develop HMIS policies and procedures that are consistent with HUD guidelines, the 2004 HMIS Data and Technical Standards, and HMIS best practices.

Contributing HMIS Organizations (CHO), HMIS Participating Agencies and Organizations

Policy: Each CHO will play a leadership role in the successful implementation of the HMIS within their agency and projects. Participating CHOs will be required to comply with all applicable operating procedures and must agree to execute and comply with the community approved HMIS Agency Participation Agreement.

Explanation: Any agency, organization, or group who has signed an HMIS Agency Participation Agreement will become a Contributing HMIS Organization (CHO) and given access to the Cincinnati/Hamilton County CoC HMIS database through trained HMIS End Users. CHO's will use HMIS reports to identify internal HMIS related training needs and to ensure HMIS data is accurate for use in system-wide reporting and analysis. CHO's will contact the HMIS Support team for assistance with user training, user support, data collection concerns, or data collection questions as needed.

Victim Services Providers

Policy: Victim Services Providers (VSPs) that are recipients or sub recipients under the CoC and ESG Programs are required to collect participant-level data consistent with HMIS data collection requirements. Aggregated or de-identified data will be provided for community or local reporting and processes. The Violence Against Women Act (VAWA) and the Family Violence Prevention and Services Act (FVPSA) contain strong, legally codified confidentiality provisions that limit VSPs from sharing, disclosing, or revealing victims' PII, including entering information into shared databases like HMIS. To protect participants, VSPs must enter required participant-level data into a comparable database that complies with all HMIS requirements.

Explanation: Victim Service Providers are required to not participate in the community HMIS, rather they are required to utilize a Comparable Database which is an alternative system used to collect participant-level data over time. The Comparable Database is required to comply with the requirements of the most current HUD HMIS Data Standards and generate unduplicated aggregate reports based on the data. Information entered in a Comparable Database must not be entered directly into or provided to a community HMIS. All CoC privacy, security, and data quality policies and procedures will apply to the comparable database at a minimum, although Victim Services Providers may opt to implement more stringent requirements.

Management of the HMIS

Strategies to End Homelessness (STEH), HMIS Lead Agency

Policy: Strategies to End Homelessness (STEH), as the HMIS Lead, is responsible for system administration and project management of the Cincinnati/Hamilton County CoC HMIS.

Explanation: STEH is the lead agency for the Cincinnati/Hamilton County CoC HMIS. STEH, through the HMIS Support Team, is responsible for helping agency users to gain access to the database system, as well as provide training and technical assistance to the HMIS participants.

Policy: As the HMIS Lead Agency, STEH will oversee the HMIS project for day-to-day operations, ensure compliance with HUD requirements and locally established policies and procedures, enforce data quality standards as set forth in the approved HMIS Data Quality Plan, act as liaison with HUD representatives and other communities, act as liaison to the HMIS vendor, and take primary responsibility for all HMIS activities. And other duties as outlined in the HMIS Governance Charter Key Roles and Responsibilities section.

Explanation: STEH has a designated HMIS department responsible for all HMIS project day-to-day activities including:

1) Ensuring the HMIS software provides data collection and reporting consistent with HUD regulations and requirements.
2) Managing HMIS users, including providing training, technical support, terminating users, and all other user management responsibilities.
3) Development of initial drafts of HMIS policies and procedures and ensuring those drafts have opportunities for review and revisions by HMIS stakeholders prior to final approval by the Homeless Clearinghouse, as is consistent with Cincinnati/Hamilton County CoC policies.
4) Maintain communication with HMIS end users and stakeholders about changes in HUD HMIS related regulations, standards, and/or guidance.
5) Monitor and manage the HMIS software system to ensure compliance with the most current HUD HMIS Technical Data Standards.
6) Monitor and manage data quality reports and user audit logs to improve system performance and ensure security of the system.

Policy: The HMIS Lead will work with all dedicated homeless projects operating in the geographic area to incorporate their data into the HMIS, including support in transferring data securely from other data systems.

Explanation: STEH HMIS Administrators will:

1) Monitor and/or manage all data transfer systems (including automated data transfer through the API and manual data transfer) to ensure the transfer is working correctly and accurately. HMIS Administrators will notify the HMIS vendor, source vendor, or CHO of any issues they are unable to resolve.
2) Work directly with CHOs to set-up new CHOs or programs for data collection in HMIS. CHOs can report new programs to the HMIS Director or the HMIS Support Team noted in the contact information.

Contributing HMIS Organizations (CHO)

Policy: Each participating CHO agrees to use the Cincinnati/Hamilton County HMIS software as part of the community's effort to provide accurate data on homelessness in accordance with the Department of Housing and Urban Development's (HUD) data collection, management, and reporting standards and data elements

required locally for coordinated entry processes and system-wide or project specific analysis or funder requirements. The HMIS is used to collect participant-level data and data on the provision of housing and services to individuals and families experiencing homelessness and those at risk of homelessness.

Explanation: CHOs' approved and trained HMIS users shall collect the program-specific and universal data elements as defined by HUD and other data elements as defined by the Homeless Clearinghouse or required/requested by local funders or processes for all applicable program participants served by projects participating in HMIS. CHOs will:

1) Agree to abide by the most current *HMIS Policy and Procedures Manual* (Policy) approved and adopted by the Homeless Clearinghouse.
2) Develop internal procedures for self-monitoring of privacy, security, and data quality. These procedures should include monitoring monthly data quality (DQ) reports, action steps to improve data quality issues discovered by DQ reports, and methods to protect HMIS access (e.g., no sharing of usernames or passwords).
3) Ensure that all employees and agents comply with the established policies and procedures.
4) Participate in monitoring and oversight procedures as conducted by the HMIS Lead on behalf of the Homeless Clearinghouse.
5) Maintain their own compliance with federal regulations as well as any outside applicable regulations.
6) Ensure staffing, training, and secure equipment necessary to implement and ensure HMIS participation.

CHO Primary Point Persons

Policy: Each CHO is required to identify a Primary Point Person(s) who will be the main communicator and liaison between the HMIS Lead and their respective CHO's administration and users.

Explanation: The CHO will appoint a Primary Point Person who will:

1) Participate in meetings with the HMIS Lead to remain current on available functionality, pending HMIS changes, HMIS issues/concerns, policy and procedural changes. These meetings also offer the CHO Primary Point Person the opportunity to represent their specific CHO or community needs regarding HMIS.
2) Ensure compliance with HMIS policies within their agency.
3) Troubleshoot HMIS issues within their agency.
4) Attend HMIS trainings and maintain full knowledge of the system.
5) Provide internal HMIS support within their agencies or request/approve additional support to be provided by the HMIS Support team.
6) Advise and recommend changes to HMIS Policies and Procedures on behalf of their agency and users.

CHO HMIS Security Officer

Policy: Each CHO must designate an HMIS Security Officer to be responsible for ensuring compliance with applicable security standards (this can be the same person as the Primary Point Person or a separate individual).

Procedure: The CHO HMIS Security Officer will utilize the HMIS Self-Monitoring Checklist, or other documentation provided prior to or during HMIS monitoring visits, to ensure the CHO is in compliance throughout the year as well as to document completion of required security tasks, processes, requirements, and results.

HMIS End Users

Policy: All HMIS End Users are required to:

1) Be aware of the sensitivity of participant-level data and take reasonable and appropriate measures to prevent its unauthorized disclosure.
2) Protect institutional information to which they have access and report security violations.
3) Comply with all policies and standards described within this manual.
4) Be accountable for their actions and for any actions undertaken with their username and password.
5) Abide by the HMIS User Agreement (strategiestoendhomelessness.org) and acknowledge understanding and receipt of the HMIS Privacy Notice and Client Consent Form (strategiestoendhomelessness.org) before receiving access to project specific data within the HMIS. These agreements must be renewed annually or user access to the system will be revoked.
6) Operate the system under any requirements currently in place at the time of use.
7) Collect the program-specific and universal data elements as defined by HUD and other data elements as defined by the Homeless Clearinghouse or required/requested by local funders for all applicable participants served by projects participating in HMIS in accordance with the HMIS Data Quality Standards.

Procedure: Each HMIS End User will:

1) Participate in HMIS training that includes HMIS End User related policies and procedures.
2) Sign, confirm they have read, and agree to abide by the HMIS User Agreement annually.
3) Never share their HMIS username and password and will take responsibility for any interaction with the HMIS applied under their username and password.
4) Enter applicable data for all participants as correctly and accurately as possible and in accordance with the HMIS privacy, security and data quality policies.

User Access

Contributing HMIS Organizations (CHO)

Policy: Each CHO must ensure that only authorized HMIS users view or update participant data. CHO and the HMIS Lead shall authorize use of the HMIS only to users who need access to the system for data entry, editing of participant records, viewing of participant records, report writing, administration or other essential activity associated with carrying out participating agency responsibilities. Only actively engaged staff, in their status as paid employees, contractors, volunteers, affiliates or associates may be users.

Explanation: The HMIS offers different types of user access roles. CHOs should include specific access requirements for each new user reported to the HMIS Support Team (e.g., referral access, read only, reports only, etc.). The HMIS Support Team will work with CHO staff to determine the most appropriate access role or define the requirements for a new user access role if needed/possible. Some access, such as access to Coordinated Entry projects, require additional approvals. The HMIS Support Team will confirm the required approval and notify the CHO of the outcome.

Procedure: CHOs will notify the HMIS System Administrators of individual requests for HMIS Users and details of their access requirements. The CHO Primary Point Person(s) (PPP) and/or Executive Director (ED) will approve each Individual request. The HMIS Support Team will consider requests by the CHO ED or PPP as approved or will request approval from the CHO PPP prior to setting up the new user in HMIS.

The CHO will notify HMIS Administrators within one business day when an individual user's access must be

terminated.

HMIS Administrators

Policy: Only authorized users will have access to the Cincinnati/Hamilton County Coc HMIS via a username and password. Additional approval and/or training may be required for additional access.

Procedure: System Administrators will provide usernames and initial passwords to each user upon approval by the CHO PPP or ED. Access to HMIS will be provided once the user has reset their password, set-up 2 factor authentication, and signed an HMIS User agreement. Access to project specific data will be provided once the user has completed HMIS training provided by the HMIS Lead. The HMIS Lead will initiate any required additional approval or training for the user based on the CHO's access request for that user. The user will be provided additional access upon completion of required training and approval.

A User who has not accessed HMIS within 90-days will be set to inactive status. Such accounts will be re-activated at the specific request of the user. When a user account is inactive for more than a year, they may be required to participate in additional training in order to have their access restored. This will be determined by the HMIS Lead and is dependent on length of and reason for inactivity. The HMIS Lead retains the right to seek approval for the user and/or require additional training prior to re-activating their account.

HMIS End User

Policy: Each End User is required to understand and adhere to the responsibilities outlined in the HMIS User Agreement before being granted access to the Ohio Cincinnati/Hamilton County CoC HMIS. End Users will be required to complete assigned training prior to being provided access to program level data. The End User will be required to adhere to all data privacy, security, and data quality policies and procedures. End Users will keep their access information (e.g., username, password, two-factor authentication) confidential.

Procedure: End users will sign an HMIS User Agreement before their initial access to the HMIS system. Signature of the agreement will be confirmation the End User understands and agrees to abide by the terms and responsibilities outlined in the agreement. End users will be required to sign a new HMIS User Agreement and participate in additional data security training annually after being provided access to the HMIS. Failure to comply may result in the user losing access to the HMIS.

Each end user will complete the required HMIS training and demonstrate understanding of the training prior to being provided with access to program specific data. Failure to complete this training may result in the user losing access to the HMIS.

End users may request to repeat any HMIS training or request personalized assistance at any time.

HMIS PERFORMANCE MEASUREMENT

HMIS Lead

Policy: The HMIS Lead will work with the HMIS vendor to ensure the HMIS can generate project-level reports required by HUD and other federal funding partners, including HMIS CSV Exports for upload to (HUD) Sage Repository, (VA) SSVF Repository, and (HHS) RHYMIS Repository. Required progress reports and companion reports include: CoC APR, ESG CAPER, PATH Annual Report, and HOPWA APR.

The HMIS Lead will also work with the HMIS vendor to ensure the HMIS can generate required system-level reports, including Longitudinal System Analysis (LSA), the Coordinated Entry APR, HUD System Performance Measures, the Point-in-Time (PIT) count, and Housing Inventory Count (HIC) Reports.

Explanation: The HMIS Support Team will maintain understanding of the current HUD Data Standards and reporting requirements and work with the HMIS Vendor to ensure HUD requirements are met by the HMIS.

The HMIS Lead will work with CHOs to ensure timely submission of required reports. HMIS System Administrators will make every reasonable effort to confirm that HUD required reporting is functional and correct. Any reporting issues will be reported to the HMIS vendor for corrective measures.

QUESTIONS AND GRIEVANCE PROCEDURE

Participant Questions and Grievance

Contributing HMIS Organizations (CHO)

Policy: CHOs will develop a written procedure for accepting and considering questions and complaints. The procedure must include, at a minimum, how questions and complaints may be submitted (e.g., orally, in writing, if there's a specific form), to whom they should be submitted, who is involved in considering, how a response is communicated to the participant and by whom, and a timeline for giving response. CHOs will report all participant grievances to the HMIS Lead.

Explanation: Program participants bring HMIS complaints directly to the CHO with which they have a grievance. CHOs must respond to the issue as determined by the CHO's own written procedure and may also provide a copy of the HMIS Policies and Procedures Manual upon request.

CHOs will notify HMIS Support of all participant grievances by emailing HMISsupport@end-homelessness.org. The notification should include details of the grievance and any steps taken by the CHO to address the grievance. The notification may also include requests for support from the HMIS Support Team to resolve the grievance.

HMIS Lead

Policy: Participant grievances will be evaluated and recorded by the HMIS Lead. The HMIS Lead will respond to the CHO who reported the grievance confirming receipt and with any required next steps as needed.

Explanation: All participant grievances will be retained in HMIS Support's ticketing system. Each grievance will be reviewed by the HMIS Director who will determine if additional action is required. Additional action may include further investigation of the incident, review of clarification of policies, disruption of access to HMIS for the CHO or the CHO's user(s) if the CHO or user(s) is found to violate the standards set forth in the HMIS Policies and Procedures Manual or HMIS Agreements (HMIS User Agreement, HMIS Privacy Notice and Client Consent Form, HMIS Agency Participation Agreement).

User Grievance

Policy: Users will report HMIS grievances to the CHO's PPP. CHOs will report all HMIS-related user grievances to the HMIS Administrators. HMIS Administrators will provide an initial response to the grievance within three working days. A final resolution or plan for a resolution will be provided to the CHO PPP within three weeks of the grievance submission. If the user is not satisfied with the results of the grievance with the HMIS Administrators, the user may contact the STEH leadership as the CoC Lead and UFA for further assistance.

Procedure: Users will submit HMIS grievances to the CHO PPP. The CHO will report the grievance to HMISsupport@end-homelessness.org. Receipt of the email will create a ticket in the HMIS Support ticketing system so the grievance and subsequent communications will be recorded. HMIS Leadership will review and evaluate the grievance.

The HMIS Support Team will provide an initial response to the grievance within three business days. Additional communications will be recorded within the HMIS Support ticketing system. A final resolution or plan for resolution will be provided to the CHO within three months of the initial grievance. The CHO or User may contact STEH Leadership if they are not satisfied with the response from HMIS support.

Consequences for Violation of the HMIS Policies and Procedures

Access Termination

Policy: All HMIS CHOs, End Users, and Administrative Users are subject to the security, privacy, and confidentiality terms outlined in this document as well as the federal regulations in the HUD Data and Technical Standards. At any point if a breach of rules and/or policies occurs, the CHO, End User, or Administrative User may be penalized by loss of access to the HMIS or, should the CHO, End User, or Administrative User decide not to comply for any reason, they may voluntarily terminate their continued involvement with the Cincinnati/Hamilton County CoC HMIS. If the relationship between the Cincinnati/Hamilton County HMIS and a CHO is terminated, the CHO will no longer have access to the HMIS.

Explanation: The HMIS Lead or COC monitoring team will work with CHOs, End Users, and HMIS Administrators to understand and correct violations of the HMIS Policies and Procedures. In some cases, a corrective action plan may be required. Egregious violations (e.g., Compromising HMIS privacy and security) or failure to implement corrective action may result in termination of access. Although an egregious violation may result in a CHO's immediate termination of access to the HMIS, the violation will be reviewed with the Homeless Clearinghouse for recommendations and potential corrective action plan. The HMIS Lead will follow the guidance of the Homeless Clearinghouse when possible, however, as the liable party, must reserve the right to the final decision.

HMIS Administrators will remove access to the HMIS for any End User that is terminated, or all End Users associated with a terminated CHO. The HMIS Lead shall make reasonable accommodations to assist a CHO to export its data in a format that is usable in its alternative database upon request. To the extent possible, a separation plan will be developed between the HMIS Lead and the CHO with a timeline and cost proposal for voluntary terminations. Any costs associated with exporting the data will be the sole responsibility of the CHO.

After termination, the CoC retains the right to use historical data entered into the HMIS for continued analysis.

APPENDIX A: HMIS Data Quality Plan

Introduction

This document describes the Homeless Management Information System (HMIS) data quality plan for the Cincinnati/Hamilton County Continuum of Care (CoC). The data quality plan includes protocols for ongoing data quality monitoring that meets requirements set forth by the Department of Housing and Urban Development (HUD). It is developed by Strategies to End Homelessness (HMIS Lead) in coordination with HMIS Contributing Organizations and approved by the Homeless Clearinghouse (the CoC Board). This HMIS Data Quality Plan is considered to be part of the HMIS Policies and Procedures and is to be reviewed, revised, and approved annually in accordance with S 578.7(b) of the CoC Program Interim Rule, and considering the latest HMIS data standards and locally developed performance plans. The data quality standards ensure the completeness, timeliness, accuracy, and consistency of the data in the HMIS.

What is Data Quality

Data quality is a measurement of the reliability and validity of participant-level data gathered and entered into the HMIS. Several factors influence good data quality: timeliness and consistency of data entry and the completeness and accuracy of the data. Adhering to a strong data quality plan will ensure better outcome reporting, easier submissions of grant performance reports such as the HUD Annual Performance Report (APR) and supports the submission of the Longitudinal System Analysis (LSA) and System Performance Measures Report (SPMs).

Benefits of Good Data Quality

Data quality is critical to the work of ending Homelessness. Maintaining good data quality from the start provides the following benefits:

- Reduces efforts needed to correct data for program participants and case managers.
- Allows case managers to have information necessary to help program participants.
- Improves CHO and CoC reports on performance outcomes.
- Maintains compliance with federally funded requirements and competitiveness in federal funding initiatives.
- Provides a way to view system performance, identify gaps of service, and develop a comprehensive plan to end homelessness in our community.

Data Quality Benchmarks

The CoC's goal is to collect 100% of all data elements in real time. However, the CoC recognizes this may not be possible in all cases. Therefore, the CoC has established an acceptable range of timeliness and missing/null, client doesn't know, client prefers not to answer, and data not collected responses, depending on the data element and the type of program entering data. Data quality will be reviewed during Annual Monitoring by STEH Compliance. Results will be communicated in the monitoring report.

Data Quality Policies, Procedures, Benchmarks

HMIS Data Quality Benchmark Development

CoC, Homeless Clearinghouse, CHOs, HMIS Lead, UFA/CoC Lead

Policy: Cincinnati/Hamilton County HMIS Data Quality Benchmarks are developed through a collaborative process which includes input from CHOs, the HMIS Lead, UFA/CoC Lead, and other stakeholders (e.g. CoC

Workgroups, Persons with Lived Experience) as defined by the Continuum of Care Policy Development policy. HMIS Timeliness Benchmarks will be in effect once approved by the Homeless Clearinghouse.

Procedure: HMIS Data Quality Benchmarks will be developed through a collaborative process consistent with Continuum of Care Policy Development policy. Drafted Benchmarks will be reviewed by the STEH CoC Manager and brought to the STEH Compliance Department to ensure compliance with HUD regulations/requirements. After being approved for circulation by the STEH Compliance Department, Benchmarks will be circulated to the CHO PPPs, and other workgroups or committees as required. This comment period will allow CHOs, workgroup members, and stakeholders to receive responses to requests for clarification and suggest changes. Once a final draft has been established it will be submitted to the Homeless Clearinghouse for approval. Approved Benchmarks are incorporated into the HMIS Data Quality Plan.

Data quality and timeliness will be monitored using the HMIS Data Quality Report built to HUD specifications. Only engaged outreach and night-by-night clients will be considered for the purposes of data quality.

Incentives and Consequences: Timeliness and quality of data entry may be reviewed during Annual Monitoring by STEH Compliance. Results will be communicated in the monitoring report in accordance with a framework developed in collaboration with the Monitoring Subcommittee of the Homeless Clearinghouse. Timeliness and quality of data entry may also be considered in the Cincinnati/Hamilton County scoring process. Projects that meet data quality benchmarks may be awarded more points while projects which fail to meet data quality benchmarks may lose scoring points. This scoring point system is used to determine competitiveness for funding renewal projects. Scoring criteria are determined annually in accordance with the Cincinnati/Hamilton County Scoring Subcommittee.

Timeliness

Timeliness Benchmarks

Benchmarks for intake and exit records entered beyond the 3-day standard by program type				
	Intake records for all programs (PSH, RRH, TH, HP/Diversion, ES, ES NBN, SO/SSO, SH)	Exit records for all programs (PSH, RRH, TH, HP/Diversion, ES, ES NBN, SO/SSO, SH) except Winter Shelter exit	Exit Records for Winter Shelter	Exit Records for non-HUD SO
4-6 days	5%	5%	N/A	N/A
7-10 days	3%	3%	N/A	N/A
11+ days	0%	0%	N/A	N/A

Contributing HMIS Organizations (CHO) and End User

Policy: Real time data entry is considered best practice, however, the timeliness requirements outlined in the Timeliness Benchmark is considered acceptable in circumstances where real-time data entry cannot be achieved for intake (aka project start or project enrollment) and project exit.

Explanation: In accordance with HUD requirements, any residential project (including Emergency Shelter, Safe Haven, Transitional Housing, PH RRH, and PSH) must complete a project enrollment at the time of project start and project exit at the time a participant exits the program. Data entered must, at a minimum, include the required data elements as outlined by the current HUD HMIS Data Standards. Status Update assessments will be completed if a participant's situation changes. For example, changes in income, non-cash benefits, health insurance, etc. Residential projects must also complete an annual assessment for any individual or family participating in the program for 1 year or longer, regardless if the participant's situation has changed in that year. The annual assessment must be completed within the window of 30 days prior to the head of household's program anniversary date – 30 days after the head of household's program anniversary date.

Data import considerations: Date entered is an element that is imported from the source database into the HMIS database, therefore, timeliness factors should not be affected by importing data into HMIS.

Accuracy and Completeness

Data collected by HMIS is used to improve service provision, and obtain an accurate picture of the extent, characteristics, and patterns of service use for local persons experiencing homelessness. Complete and accurate data is essential. Complete and accurate Personally Identifiable Information (PII) is critical for the HMIS to produce an unduplicated count of persons access services covered by HMIS. Data unavailable or inaccurate at the time of data entry may be added or corrected later.

Accuracy and Completeness Benchmarks

Personally Identifiable Information (PII)

Benchmarks for unknown (don't know/refused) and missing/data issues responses for all program types (PSH, RRH, TH, HP/Diversion, ES, ES NBN, SSO/SO, SH)		
Data Element	Client Doesn't Know/Client Refused	Information Missing/Data Issues
3.1 Name	0%	0%
3.2 Social Security Number	1%	1%
3.3 Date of Birth	0%	0%
3.4 Race	0%	0%
3.5 Ethnicity	0%	0%
3.6 Gender	0%	0%

Universal Data Elements

Benchmarks for all program types (PSH, RRH, TH, HP/Diversion, ES, ES NBN, SSO/SO, SH)	
Data Element	% Error rate
3.7 Veteran Status	0%
3.10 Project Start Date	0%

3.15 Relationship to Head of Household	0%
3.16 Client Location	0%
3.8 Disabling Condition	1%

Program Specific Data Elements

Benchmarks for error rates by program type							
Data Element	PSH, HP	RRH, TH	ES, SO/SSO	ES NBN	SH	Non-HUD Housing Programs	Non-HUD ES, SO/SSO
	% Error rate	% Error rate	% Error rate	% Error rate	% Error rate	% Error rate	% Error rate
3.12 Destination	0%	0%	3%	N/A	0%	0%	3%
4.2 Income and Sources at Start	0%	0%	0%	0%	0%	N/A	N/A
4.2 Income and Sources at Annual Assessment	5%	10%	0%	0%	0%	N/A	N/A
4.2 Income and Sources at Exit	0%	0%	0%	N/A	0%	N/A	N/A
4.3 Non-Cash Benefits at Start	0%	0%	0%	0%	0%	N/A	N/A
4.3 Non-Cash Benefits at Annual Assessment	5%	10%	0%	0%	0%	N/A	N/A
4.3 Non-Cash Benefits at Exit	0%	0%	0%	N/A	0%	N/A	N/A

Chronic Homeless Data Elements

Benchmarks for Records Missing Information Needed to Calculate Chronic Homelessness	
Data Element	PSH, RRH, TH, ES, ES NBN, SO
% of records unable to calculate	0%

Inactive Records

Benchmarks for Inactive Records	
	SO, ES NBN

Data Element	% of Inactive Records
Contact (Adults and Heads of Household in Street Outreach or ES-NbN	0%
Bed Night (all clients in ES-NbN)	0%

Accuracy (No benchmarks proposed at this time)

Benchmarks for Income Records in HMIS Inconsistent with Income Documentation in Participant Record	
Data Element	PSH, RRH, TH, HP/Diversion, ES, ES NBN, SO/SSO, SH
	# Error Count
Income entries inconsistent with documentation in client file	

Client Release of Information - Additional Data Quality Element Considerations (No benchmarks proposed at this time)

Benchmarks for Participant Records Missing Releases of Information		
Data Element	PSH, RRH, TH, HP/Diversion, ES, ES NBN, SO/SSO, SH	
	Error Count	% Error Rate
Active client records missing ROIs at the time of monitoring		
Client records missing ROIs in the 12 months preceding the monitoring		

CHOs and End Users

Policy: The Cincinnati/Hamilton County CoC expects all participants receiving housing and/or services through the homeless assistance system will have their service delivery documented in HMIS. Complete and accurate data is key to producing accurate bed utilization data which is used to determine need and attain funding for CHOs and our community. Complete data entry is considered best practice, however, the attainment of complete data is not always possible, therefore, CHOs are expected, at a minimum, to maintain data completeness consistent with the current approved HMIS Data Quality Benchmarks.

Explanation: End users will make every effort to enter complete and accurate data. In some cases where the data is not available at time of intake (aka project start or enrollment) the end user will make every effort to enter corrected data within two business days or as soon as the data becomes available. CHOs will monitor their data collection and implement processes to improve data accuracy and completeness as needed.

Consistency

HMIS Lead and HMIS Administrators

Policy: The HMIS Lead will provide training, user support, and data quality monitoring both reactively and proactively to ensure all HMIS End Users understand required data elements and processes.

Explanation: The HMIS Lead, through its administrators will proactively provide user training and user support documentation to assist users in consistent data entry. The HMIS Lead will respond to CHO and user requests, making resources available to support improvements in consistent data entry, quality, timeliness, and completeness.

CHOs and End Users

Policy: CHOs and End User will take responsibility for consistency in data entry.

Explanation: CHOs and End Users will fully participate in training opportunities and fully utilize supporting documentation provided by the HMIS Lead. CHOs and End Users will contact HMIS Administrators with any questions or support needs and engage HMIS Administrators to assist with data quality improvements as needed.

Monitoring

CHOs

Policy: CHOs are expected to monitor their own data quality at least monthly in order to quickly identify and resolve data entry issues.

Procedure: CHOs will download and save a timestamped PDF file of the HUD HMIS Data Quality Report at least monthly for each HMIS project. CHOs will notify staff of data correction needed and may opt to download a new version of the HUD HMIS Data Quality Report which reflects the corrected data. CHOs will develop a data quality improvement plan for individual staff or programs to address persistent data quality issues as needed. CHOs and users may contact HMIS Support with any questions or assistance resolving issues.

HMIS Lead

Policy: The HMIS Lead will monitor HMIS Data at least annually in order to, at a minimum, ensure system wide HUD reporting is accurate.

Procedure: The HMIS department will monitor HMIS data using HUD provided and/or custom designed tools and resources. The HMIS department will notify the CHO PPP and/or HMIS User of required data corrections. Failure to correct data will be communicated to the STEH Compliance Department at the time of the CHO's annual compliance evaluation. Results will be communicated in the monitoring report in accordance with a framework developed in collaboration with the Monitoring Subcommittee of the Homeless Clearinghouse.

UFA/CoC Lead

Policy: Annual monitoring by STEH Compliance includes monitoring of HMIS requirements, including data quality standards.

Explanation: STEH incorporates HMIS monitoring into its annual monitoring visit. If HMIS data quality issues are found by STEH's monitoring team, STEH will collaborate with the CHO to resolve the issue as well as provide counseling on potential problems that may arise and identify systemic improvements. The extent to which the issue results in a monitoring "finding," "concern," or "additional note" may depend on the severity and/or exigency systemic nature of the problem.

Non-compliance with STEH counseling or significant and/or egregious data quality problems that continue unresolved and/or which impact the wider CoC community may result in referral to the CoC monitoring subcommittee for consideration of next steps, which could include a recommendation of sanctions to be voted upon by the Homeless Clearinghouse.

Additional Data Quality Concerns

Some HMIS or CoC processes may require additional data entry requirements beyond the HUD required data elements. These data points and processes are critical to Coordinated Entry documentations, required by non-HUD funders, or critical for other requirements within the HMIS.

HMIS Lead and HMIS Administrators

Policy: The HMIS Lead will document and train users on required data entry.

Explanation: HMIS Administrators will include additional data entry requirements in HMIS trainings and support documentation. HMIS Administrators may notify users and CHOs of data entry issues which need to be resolved.

CHOs and HMIS Users

Policy: CHOs and HMIS Users will be responsible for accurate data entry for data elements and processes that are required beyond the HUD HMIS data requirements.

Explanation: HMIS Users will fully participate in all training opportunities for additional data collection requirements. HMIS Users will correct data quality issues within a minimum of 1 week of being notified of the issues. CHOs will monitor HMIS data collection to ensure all required data is collected completely and accurately. CHOs and HMIS Users will notify the HMIS of any concerns preventing them from entering additional required data.

APPENDIX B: HMIS Privacy Plan

The HMIS Lead and CHOs have specific responsibilities to uphold and comply with the baseline privacy requirements with respect to data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability. A CHO may adopt additional substantive and procedural privacy protections that exceed the baseline requirements for each of these areas.

The core tenet of this privacy plan is the HMIS Privacy Notice & Client Consent Form approved and adopted by the Homeless Clearinghouse. The HMIS Privacy Notice & Client Consent Form, as required by HUD proposed rules, describes how participant information may be used and disclosed and how participants can get access to their information and ensures all Cincinnati/Hamilton County CHOs are governed by the same minimum standards of participant privacy protection. It is each CHOs' responsibility to ensure that its own policies and practices are in line with the full extent of HUDs proposed rule and adhere to any additional local, state, or federal requirements. All CHO policies regarding privacy requirements must at a minimum include the criteria in this document. Additional requirements may be added at the discretion of each CHO.

Participant Rights and Consent

Contributing HMIS Organizations (CHO) and End User

Policy: Participant confidentiality and shared data is a cornerstone of a healthy, informed HMIS system. Sharing data within HMIS is critical for the health of the HMIS database and de-duplication of participants' records. Each CHO must explain system privacy measures, participant rights, and how their information may be used or disclosed for each participant. The HMIS Privacy Notice and Client Consent Form was developed to serve this purpose. Participants who wish their data to not be shared in the HMIS should still be entered into HMIS and the record set to private status. Information shared previously in the HMIS will remain shared and cannot be set to private. No CHO shall refuse or change their service delivery based on whether a participant agrees to have their data entered into HMIS.

Procedure: Each CHO must post the HMIS Privacy Notice and Client Consent Form in intake areas or a comparable location and on their public-facing website.

Each user must review and understand the HMIS Privacy Notice and Client Consent Form. The HMIS Privacy Notice and Client Consent Form must be reviewed for new adult participants seen by each CHO (vs. each project) and again every seven years the participant remains engaged with the CHO.

Participants may read and sign the HMIS Privacy and Client Consent Form either on paper or digitally during face-to-face intakes. The HMIS Privacy and Client Consent Form may be read to the participant and verbal consent offered for intakes completed virtually or over the phone. It is preferred that each adult sign their own HMIS Privacy and Client Consent Form; however, the head of household may provide consent to share household members' information within HMIS if the household members are under the age of 18 or the adult household member is not available at the time of intake. Child only participants may not consent to share information within the HMIS and child only participants' records must be set to private in the HMIS. The participant's consent to share information within the HMIS or refusal to share information must be documented within the HMIS.

End Users must enter all required data elements into HMIS. Set the participant's HMIS record to private if the participant refuses to share data within HMIS or is in a child only household. Existing shared records in HMIS

cannot be unshared. Create a new participant record and set that record to private cases where a current shared record exists.

Each CHO and HMIS User must perform duties consistently with the HMIS Privacy Notice and Client Consent Form.

HMIS Uses and Disclosures

Allowable Uses and Disclosures of Protected Personal Information (PPI) /Personally Identifiable Information (PII)

Policy: Participants' data must be made available to them when requested. Additionally, as is described in the HMIS Privacy Notice & Client Consent, any organization (including its employees, volunteers, affiliates, contractors, or associates) that records, uses, or processes PII for or from an HMIS may use or disclose PII from the HMIS for the following purposes:

- To provide or coordinate services.
- For administrative purposes, including but not limited to legal, audit, personnel, oversight and management functions.
- To research and better understand homelessness.
- To provide government required count(s) of people receiving services.
- Meet requirements of funders such as the U.S. Department of Housing and Urban Development (HUD) or functions related to funding for services.
- Develop and improve programs to work towards ending homelessness in our community.
- When required by law through a court order or in the event of a public health emergency.

Uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with CoC policies, or grant requirements). However, nothing in this standard modifies an obligation under applicable law to use or disclose personal information.

PII or PPI must never be published publicly.

Explanation: HMIS data can only be disclosed for the purposes listed above unless the additional uses are described in a separate agreement signed by the participant.

Provision or Coordination of Services

Participant PII may be shared to coordinate or provide services consistent with the program's goals or to achieve housing stability. If participant PII is shared outside of the provider agency the participant must agree. CHO's may choose to implement additional sharing agreements with participant to reflect this agreement. Data shared should be limited to the data required to coordinate or provide services and should be shared in a secure manner.

Functions Related to Funding for Services

De-identified data should be reported to funders when possible. In some cases, participant PPI may be required to prepare demographic, service provision, or outcome details for specific funders. There may also be situations where more specific data is required by funders (e.g. age, DoB, zip code, etc.) which may reasonably be used to identify specific individuals in some cases. In these cases, data should only be shared through secure means, limited to requested/required data elements, and only shared with persons/organizations required to access the data for the purposes of securing funding for services.

Administrative Processes

When possible, a CHO should limit access to HMIS data to the CHO's paid or unpaid staff, volunteers, contractors, or agents. There may be occasion where external contractors or agents may need access to HMIS data (e.g. external audits). In these situations, the CHO should ensure any external contractor, agent, or stakeholder is bound by signed confidentiality agreements consistent with the guidelines provided for within this document.

Research Purposes

When possible de-identified data should be used for research purposes, however, there may be circumstances where PPI is critical for the intended research or specific details shared may reasonably be used to identify specific individuals. In these situations, the individual or institution receiving the data must have a formal relationship with the organization disclosing the PPI. The research project must be conducted under a written research agreement approved in writing by an agency administrator unless the research is being completed by an employee/paid contractor of the organization providing the PII.

A written research agreement must: (1) Establish rules and limitations for the processing and security of PPI in the course of the research; (2) provide for the return or proper disposal of all PPI at the conclusion of the research; (3) restrict additional use or disclosure of PPI, except where required by law; and (4) require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

Government Required Count(s)

Counts or aggregate data by their nature do not disclose PII. However, PPI may be required to prepare required counts or there may also be situations where more specific data used in counts (e.g. age, family size, zip code, etc.) may reasonably be used to identify specific individuals in some cases. In these cases, data should only be shared through secure means, limited to requested/required data elements, and only shared with persons/organizations required.

Develop and Improve Services

HMIS data is intended to be used to develop strategies to end homelessness, identify gaps in service, and improve existing services. De-identified data should be used whenever possible, however, in some instances PII or specific details shared may reasonably be used to identify specific individuals. PPI should only be shared if through secure means, only for the expressed purpose, and only to individuals or organizations bound by a signed confidentiality agreement or written research agreement.

Required by Law or in the Event of a Public Health Emergency

Disclose PII if: (1) The organization disclosing, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

Where the disclosure is required by law, it must be limited to the requirements of the law and must be authorized by statute or regulation, or lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial officer, or a grand jury subpoena.

Limits on Data Collection

CHOs and End Users

Policy: PII collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes. HMIS End Users will only collect or access participant data relevant to the delivery of

services to people experiencing a housing crisis or for the specific purpose the data was collected. A CHO may collect PII for individuals or families receiving services from the CHO. A CHO must collect PII by lawful and fair means and, where appropriate, with the knowledge or consent of the individual. Data allowable includes all HUD mandated data as well as any other data deemed necessary and approved by the CHO which complies with federal regulations and the policies and procedures of this document.

Explanation: CHOs and HMIS End Users will limit data collection to individuals or families receiving services from the CHO. HMIS Users should only enter or access data for the express purpose of providing services or for the specific purposes for which the data was collected. It is the CHO's responsibility to ensure any requested data elements, beyond those required by HUD or approved by the CoC, comply with local, state, and federal regulations.

Access and Correction

CHO and HMIS Users

Policy: A CHO must allow an individual to inspect information in the HMIS, ask for changes, or ask for a printed copy upon request.

Procedure: CHOs and HMIS Users will allow individuals to review, provide corrections, or provide a printed copy of their HMIS data upon request. CHOs and HMIS User may request assistance from HMIS Administrators if needed.

APPENDIX C: Security Plan

What is Security?

Security is the degree of resistance to, or protection from, harm or access by persons not authorized by a CHO or HMIS Lead to HMIS data. The security of the data held in and outside the HMIS database is a high priority in the community. Those in contact with HMIS data must take the confidentiality, integrity, and availability of all HMIS information seriously. This plan aims to protect against any reasonably foreseeable threats or hazards to security and ensure that HMIS users are in compliance with the standards set forth in this plan.

Application Security

HMIS Lead

Policy: The HMIS Lead will ensure that HMIS processes and software application meets security provisions required by HUD during data entry, storage and review or any other processing function, including:

- A user authentication system consisting, at a minimum, of a username and a password. And those passwords are required to meet the reasonable industry standard requirements.
- HMIS data is encrypted during transmittal and at rest.
- The HMIS system contains user audit logs pertaining to participant data.
- The HMIS vendor institutes security process including physical server infrastructure and security audits.
- HMIS system data is limited to trained, authorized users.

Explanation: The HMIS Lead and Administrators work with the HMIS vendor to ensure HUD security requirements are met or exceeded by the HMIS application. Additionally, HMIS Administrators use applications and processes that include data encryption when working with HMIS data outside of the system. For example, when sharing data or data sets that contain PII they are shared using Microsoft OneDrive, an encrypted, secure method of sharing data.

Hard Copy Security

Contributing HMIS Organizations (CHO), HMIS Participating Agencies and Organizations and End Users

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

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

Remote work considerations: Staff working remotely are required to supervise paper or hard copy PII generated by or for the HMIS when in use and secure hard copy PII in a locked location (a locked drawer, room, or briefcase). Hard copy PII no longer in use should be shredded or burned.

Physical Access

Contributing HMIS Organizations (CHO), HMIS Participating Agencies and Organizations and End Users

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

Explanation: A CHO must take steps to secure each computer by:

1) When possible, ensure workstations are located where they are not easily viewed by the public (located in areas where there is low public traffic or in such a way that screens cannot be viewed from high public traffic areas).
2) Computers in public areas should be locked with a password protected screen or turned off when not in use, staff are not present, or if viewable by unauthorized persons.
3) Enable an automatic password protected screen saver or automatically log users off if the system has remained dormant for a maximum 15 minutes and the computer is in a publicly highly trafficked area or a maximum of 30 minutes for workstations placed in low publicly trafficked areas. only accessible by agency staff.
4) Power off a workstation when not in use for an extended period of time. Consider enabling an automatic computer shut down of a system if it has remained dormant for 2 hours.
5) Consider locking computers that are located in public areas so they cannot be physically removed.

Note: A high publicly trafficked would include areas where non-employees frequent. A low publicly trafficked area would include areas where non-employees are supervised or areas where employees without HMIS access can access. Although requirements are less stringent for low publicly traffic areas, it is still important that users are aware of their surroundings and reduce the potential for inadvertently sharing sensitive information.

Remote work considerations: Staff working remotely are required to be diligent to avoid inadvertently sharing HMIS data.

- Orient computer screens so that the content is not easily viewed by others.
- Identify strategies to quickly conceal HMIS data so it cannot be viewed by other people (e.g., quickly lock your computer using keyboard shortcuts, or use “lid” configuration settings to lock when laptop lid is closed).

CHO Hardware, Software, and Connectivity

Contributing HMIS Organizations (CHO)

Policy: A CHO must apply system security provisions to all the systems where personally identifying information generated either by or for the HMIS is stored, including, but not limited to, a CHO’s networks, desktops, laptops, and servers.

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

- Each workstation used to access HMIS or store data for or from the HMIS must include up to date virus protection and firewall protection.
- Any server or network used to access the HMIS or store data for or from HMIS must include up to date virus protection and firewall protection.
- Any workstation, server, or network used to access the HMIS or store data for or from HMIS must include at a minimum password protection.

Remote work considerations:

- Only use secure networks or hot spots, never work within the HMIS or with HMIS data on a public network.
- Save HMIS data to a secure server; never to your personal or work-computer.
- When working from home, reboot the home router or modem to improve performance and ensure your internet provider maintains the most current network security.
- Use a personal VPN for an extra layer of protection.

Policy: A CHO must maintain the minimum workstation specifications for all HMIS Users. These requirements apply to all workstations, including laptops and other mobile devices used on or off- site.

Explanation: Each CHO will ensure each workstation/device accessing the HMIS has the most up-to-date version of a supported web browser to ensure the latest security features are in place. Supported Web Browsers for Accessing Clarity Human Services (bitfocus.com)

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Apple Safari

Policy: A CHO must delete all HMIS data from a data storage medium and must reformat the storage medium more than once before reusing or disposing of the medium.

Explanation: A CHO must reformat any computer, server, CD, thumb drive, or other medium which contains participant level HMIS data more than once before disposal or reuse.

Disaster Protection and Recovery

HMIS Lead

Policy: The HMIS Lead must confirm the following baseline disaster and recovery requirements are met for the HMIS.

- System redundancy allows HMIS data to be recovered in case of a disaster.
- The system and data held within the system are stored in a secure location with the appropriate temperature controls, fire suppression systems, and surge protections.
- Data disposal protocols.
- Protocols for communication with staff, the CoC, and CHOs in case of a disaster.
- Annual security review.

Procedure: The HMIS Lead will confirm at least annually that the disaster protection and recovery protocols provided by the HMIS vendor are at a minimum consistent with the HUD requirements. Disaster communications will include UFA/CoC Lead and CHO Primary Point Persons and HMIS. Notifications will be sent as soon as reasonably possible in the event of a disaster and will describe the impact of the disaster on HMIS and remedial actions. Additional update notifications will be sent as soon as practicable and after additional information is available.

Security Breaches

A data breach occurs when any person in contact with HMIS data allows said data to fall into the hands of a party not authorized by the Contributing HMIS Organization This can involve data in any form, including that which is printed, transmitted verbally, electronically stored, etc.

HMIS Lead, CHOs, HMIS Users

Policy: To protect the data in the HMIS and the integrity of the community level database, procedures have been put in place to ensure consistent responses to incidents (such as security or privacy breaches and/or inappropriate User, project, or agency actions). This policy, while subject to revision, is intended to address how the HMIS Lead will respond to any incident, including: assessing the incident, minimizing damage, ensuring rapid response, and documenting and preserving evidence.

Procedure: The CHO or HMIS End User shall inform the System Administrator in a timely manner of any breach of the privacy and security policies outlined in this document or the HUD Data and Technical Standards. HMIS Administrators will investigate the issue and determine a proper course of action for correction. If a permanent resolution is unforeseen or the System Administrator deems it necessary, a CHO and/or user termination may occur:

- The CHO will be notified in writing of the intention to terminate their participation in the HMIS.
- The HMIS System Administrator will revoke access of the HMIS End User or CHO staff.
- The HMIS System Administrator will keep all termination records on file.

APPENDIX D: HMIS Governance Charter

Introduction

Through the annual CoC Governance Charter, the Cincinnati/Hamilton County CoC Board, locally known as and named the Homeless Clearinghouse, along with the full membership of the CoC has selected Strategies to End Homelessness (STEH) as the CoC lead agency/Unified Funding Agency (UFA) and HMIS Lead Agency for the geographic area known as OH-500. The coverage area for both the CoC and the HMIS includes all municipalities in Hamilton County. STEH has primary responsibility to manage all HMIS activities on behalf of the CoC and the Homeless Clearinghouse.

The HMIS Governance Charter is effective in coordination with the CoC Governance Charter. In consultation with the UFA, HMIS Lead, CoC Board, and full CoC membership (as defined by the CoC Governance Charter) the CoC governance charter, the HMIS Governance Charter, and all applicable policies and procedures will be reviewed/updated and approved at least annually.

Purpose

The HMIS Governance Charter serves to delineate the roles and responsibilities related to key aspects of the governance and operations of the Cincinnati/Hamilton County HMIS and includes the most recent HMIS Policies and Procedures Manual developed and adopted by the CoC Data Committee and the Homeless Clearinghouse, which is incorporated into this charter by reference.

Beginning with the 2003 Continuum of Care (CoC) grants and continuing with the Emergency Solutions Grants (ESG), the United States Department of Housing and Urban Development (HUD) requires all grantees and sub-grantees to participate in their local Homeless Management Information System. This policy is consistent with the Congressional Direction for communities to provide data to HUD on the extent and nature of homelessness and the effectiveness of its service delivery system in preventing and ending homelessness.

The HMIS and its operating policies and procedures are structured to comply with the most recently released HUD Data and Technical Standards for HMIS. Recognizing that the Health Insurance Portability and Accountability Act (HIPAA) and other Federal, State and local laws may further regulate agencies, the Continuum may negotiate its procedures and/or execute appropriate business agreements with Partner Agencies so they are in compliance with applicable laws.

THE HMIS LEAD uses all submitted data for analytic and administrative purposes, including the preparation of reports to funders and the Continuum's participation in the Longitudinal Data Analysis (LSA), the national report on the state of homelessness as defined by HUD. Aggregate data taken from the HMIS is used to inform strategic planning activities, including the Consolidated Plans in the applicable jurisdictions of Hamilton County and the City of Cincinnati County as required.

Key Roles and Responsibilities

The roles and responsibilities of each group identified below are not meant to be all inclusive and a successful HMIS implementation requires all named groups and HMIS agencies to work together. Some roles and responsibilities may overlap between groups.

The Homeless Clearinghouse (Continuum of Care Board)

1) Designates an eligible applicant to manage the CoC's HMIS, which will be known as the HMIS Lead.

2) Designates a single Homeless Management Information System (HMIS) for the geographic area.
3) Reviews, revises, and approves the HMIS Governance Charter, HMIS Policies and Procedures Manual, HMIS Data Quality Plan, HMIS Data Privacy Plan, HMIS Data Security plan, HMIS User Agreement, and the HMIS Privacy Notice and Client Consent Form
4) Ensures minimum required participation of HUD-funded recipients and subrecipients in the HMIS; and encourages and facilitates 100% HMIS participation regardless of partner funding source or HUD mandate.
5) Ensures the HMIS is administered in compliance with requirements prescribed by HUD.

Strategies to End Homelessness (STEH), UFA, CoC Lead, and HMIS Lead for the Cincinnati/Hamilton County CoC

As UFA:

1) Ensures HMIS compliance with all HUD rules and regulations;
2) Encourages and facilitates participation in the HMIS from homeless agencies;
3) Makes public all applicable CoC and HMIS meetings, inviting participation from the HMIS community at large;
4) Consults with the full CoC to develop HMIS policies and procedures in compliance with HUD regulations and facilitates at least an annual review and approval from the Homeless Clearinghouse; (intro?)
5) In consultation with and subject to oversight of the Homeless Clearinghouse, negotiates, approves and executes annual contract(s) with HMIS vendor(s).

As HMIS Lead

1) Oversees the HMIS project and has primary responsibility for all HMIS activities;
2) Authorizes/makes decisions regarding day-to-day operations of the HMIS;
3) Ensures compliance with HUD requirements and locally established policies and procedures;
4) Monitors and enforces data quality in accordance with the benchmarks as set forth in the HMIS Policies and Procedures Manual and Data Quality Plan;
5) Acts as liaison between the CoC and regional or national HMIS related organizations;
6) Participates in applicable regional or national HMIS related activities;
7) Supervises contract(s) with HMIS vendor(s);
8) Provides initial and on-going training and support to CHO HMIS users;
9) Facilitates data sharing agreements between partner agencies;
10) Facilitates HMIS continuing quality improvement in coordination with the Homeless Clearinghouse and the STEH Planning and Evaluation Department.
11) The HMIS Lead must designate one staff member as the HMIS security officer.
12) Generate system-level and project-level reports for submission to local, state, and federal partners.
13) HMIS System Administration
    a. User support and training
    b. HMIS Help Desk and support ticketing system
    c. Communications with CHOs and HMIS Users
    d. User account management
    e. HMIS program and reporting customizations
    f. Confirm that HUD required reporting is functional and correct

Covered Homelessness Organizations (CHOs)

1) Play a leadership role in the successful implementation of the HMIS;

2) Execute an HMIS Agency Partner Agreement and, if applicable, an agency partnership data sharing agreement; pg. 7
3) Agree to abide by the most current HMIS Policy and Procedures Manual (Policy) approved and adopted by the Homeless Clearinghouse;
4) Ensure that all employees and agents comply with the established policies and procedures;
5) Participate in monitoring and oversight procedures as conducted by the HMIS Lead on behalf of the Homeless Clearinghouse;
6) Maintain their own compliance with federal regulations as well as any outside applicable regulations;
7) Ensure staffing, training, and secure equipment necessary to implement and ensure HMIS participation.
8) Each CHO is asked to identify a Primary Point Person(s) who will be the main communicator and liaison between the HMIS Lead and their respective agency's users. Pg 7
9) Each CHO must designate an HMIS security officer to be responsible for ensuring compliance with applicable security standards (this can be the same person as the Primary Point Person or a separate individual).
10) Notify the HMIS Lead/HMIS Administrators of new or terminating users.

CHO Primary Point Person (aka Agency HMIS Lead)

1) Participate in meetings and/or communicate regularly with the HMIS Lead;
2) Ensure compliance with HMIS policies within their agency;
3) Troubleshoot HMIS issues within their agency;
4) Attend HMIS trainings and maintain full knowledge of the system;
5) Provide internal HMIS support within their agencies;
6) Advise and recommend changes to HMIS Policies and Procedures on behalf of their agency and users.

CHO HMIS Security Officer

1) Must be familiar with the HMIS Self-Monitoring Checklist to ensure compliance with security standards
2) Complete required security tasks/process noted within the HMIS Self-Monitoring Checklist and document and results.

HMIS Users

1) Be aware of the sensitivity of participant-level data and must take reasonable and appropriate measures to prevent its unauthorized disclosure.
2) Protecting institutional information to which they have access and for reporting security violations.
3) Comply with all policies and standards described within this manual, including privacy, security, and data quality.
4) Be held accountable for their actions and for any actions undertaken with their username and password.
5) Sign a HMIS User Agreement (hmis-user-agreement-2019-final.pdf (strategiestoendhomelessness.org) before receiving a username and password. These agreements must be renewed annually or user access to the system will be revoked.
6) Never share their HMIS username and password under any circumstances.
7) Operate the system under requirements currently in place at the time of use.
8) Participate in HMIS training.
9) Collect the program-specific and universal data elements as defined by HUD and other data elements as defined by the Homeless Clearinghouse or required/requested by local funders for all applicable

participants served by projects participating in HMIS in accordance with the Data Quality Standards.

10) Participate in annual HMIS security training.

Victim Services Provider

Victim Service Providers are required to *not* participate in the community HMIS, rather they are required to utilize a Comparable which is an alternative system used to collect participant-level data over time and to generate unduplicated aggregate reports based on the data, and that complies with the requirements of the most current HUD HMIS Data Standards. Participant specific information entered into a comparable database must not be entered directly into or provided to a community HMIS. All CoC privacy, security, and data quality policies and procedures will apply to the comparable database at a minimum, although Victim Services Providers may opt to implement more stringent requirements.