COALITION FOR HOMELESSNESS
INTERVENTION & PREVENTION

:

INDIANAPOLIS CONTINUUM OF CARE
HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS) POLICIES AND PROCEDURES
UPDATED 12/2/2022

Introduction

The purpose of the policies and procedures set forth in this manual are to establish standard operating procedures and guide the use and functions of the Homeless Management Information System (HMIS). Users and participating agencies in the HMIS agree to adhere to all policies and procedures included in this document, as acknowledged in the HMIS User Agreement and HMIS Partner Agency Agreement.

Use of the HMIS is required in order to respond to the needs of the community and the requirements set forth by the US Department of Housing and Urban Development (HUD), and the City of Indianapolis, acting as the primary fiscal agent.

The Indianapolis Continuum of Care (CoC) via the Blueprint Council designates the Coalition for Homelessness Intervention and Prevention (CHIP) as the HMIS Lead, as outlined in the CoC and HMIS Lead Entity Memorandum of Understanding. CHIP uses the web-based software known as ClientTrack as its HMIS. The HMIS Lead is responsible for providing logistical support to the CoC and is empowered to lead system change in coordination with a balanced governance and implementation infrastructure.

Purpose and Benefits

HMIS stores longitudinal, client-level data about persons who access the homeless service system in Indianapolis. The purpose of the HMIS is to network the informational resources of homeless service providers, streamline reporting, and increase the efficiency in providing services. To that end, the HMIS allows for service providers to check service history in an effort to minimize the duplication of services to clients, and the HMIS provides a single point of entry for intakes, assessments, services, case notes, and reporting requirements.

The HMIS provides standardized information in an aggregate format to funders, as well as a monitoring platform to ensure compliance with funding regulations and requirements. The HMIS also provides standardized aggregate-level data to inform the community and public policy makers of the current efforts, strengths, and needs of homelessness services.

Roles and Responsibilities

CHIP

GENERAL RESPONSIBILITIES OF CHIP

CHIP has been selected by the Indianapolis CoC to be the HMIS Lead. These responsibilities include operating and maintaining the HMIS and administering the CoC plans for privacy, security, review frequency, and data quality. Further information on responsibilities and expectations as the HMIS Lead can be found in the Indianapolis CoC Governance Charter and the HMIS Data Quality Plan.

GENERAL RESPONSIBILITIES OF CHIP'S HMIS STAFF

CHIP is responsible for providing staff to fulfill the following HMIS Lead responsibilities:

- **Manage a single HMIS for the entire CoC geography in compliance with HUD requirements.**
- **Annual review of HMIS policies and procedures.**
- **Annual review, revision, approval, and implementation of privacy, security, and data quality plans.**
- **Communication and outreach on changes in HMIS procedures and data collection to providers.**
- **Develop and conduct regular trainings and technical assistance support for providers including operating user support and ticketing systems.**
- **In collaboration with the Collaborative Applicant, ensure consistent participation of the CoC Program Grantee and sub-recipients in HMIS.**
- **Track and reinforce recipient and subrecipient participation in HMIS.**
- **Execute participation and user agreements with contributing HMIS organizations and users.**
- **Enhance the HMIS system and data capabilities by actively encouraging HMIS participation and overseeing data quality and completeness.**
- **Complete or provide information for all private, local, state, and federal reports, including but not limited to Point-in-Time count, Housing Inventory Count, Longitudinal System Analysis, and System Performance Measures.**
- **Work with the Blueprint council committees to support HMIS data use in project monitoring.**
- **Ensure HMIS policies and procedures are consistent with CoC goals.**

PARTNER AGENCIES

Partner Agencies in the HMIS are committed to improving the social welfare of those who are near-homeless or are already experiencing homelessness in the community (hereinafter referred to as "Client") by collecting, maintaining, and reporting computerized data in a manner that respects the privacy of the Client. Roles and responsibilities for Partner Agencies include the following:

- **Comply with the HMIS Privacy Notice by creating and maintaining internal procedures to collect, secure, and share Client data.**
- **Comply with current HMIS data collection requirements as outlined in the Partner Agency Agreement and HMIS Policies and Procedures.**
- **Ensure that services are not denied to a Client who refuses to consent to share personal data in the HMIS.**
- **Consent to authorize the City of Indianapolis, CHIP, and other HMIS Partner Agencies to utilize aggregate data for evaluation, research, planning, reporting, and grant writing.**
- **Consent to authorize CHIP to reconcile and release de-identified aggregate data to the CoC facilitator or any other governmental or other entity for purposes that include, without limitation, the development of Consolidated Plans, Gaps Analysis, HUD reporting, Emergency Solutions Grants, etc.**
- **Abide by the stipulations and requirements set forth in the Partner Agency agreement.**

- **Abide by HMIS Policies and Procedures set forth in this document.**
- **Maintain onsite equipment in accordance with the security section of this document.**
- **Maintain adequate internet connectivity in order to begin to participate and continue to participate in the HMIS.**
- **Meet with the HMIS Administrator to assess and address data security issues as they arise and on an annual basis.**
- **Meet the minimum technical specifications set forth by CHIP in the Basic Security Requirements.**
- **Secure Partner Agency and Individual User Agreements for all staff who will have access to the HMIS.**
- **Clients may see their record in HMIS (just as with hardcopy files). A Client may request to have their information in HMIS changed by working with designated Partner Agency staff.**
- **Ensure timely and accurate input and maintenance of Client data in accordance with the Data Quality Plan.**
- **Continued compliance with the most current HMIS data collection standards.**
- **Participate in an annual security review.**
- **Immediately report to CHIP HMIS staff, via email or phone call, any actual or suspected violations of HMIS Policies and Procedures, including but not limited to, violations related to breaches of Client confidentiality or consent, data integrity, or any misuse of the HMIS.**

BASELINE SECURITY REQUIREMENTS

- **Apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, an agency's networks, desktops, laptops, mini-computers, mainframes and servers.**
- **Secure HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. Users must update their password every 90 days and will be prompted to do so by the system.**
- **Protect HMIS systems from viruses by using commercially available virus protection software**
- **Protect HMIS systems from malicious intrusion behind a secure firewall.**
- **Locate computer systems in secured areas on the agency's premises so that information on the screen cannot be seen by others. 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. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. Password protected screen savers are a standard feature with most operating systems and the amount of time can be regulated by an agency. If staff from an agency will be gone for an extended period of time, staff should log off the data entry system and shut down the computer.**
- **The data maintained in the HMIS will be treated as an agency would treat hard copy files of Client information.**
- **Secure any paper or other hard copy containing personal protected information that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms. An agency must supervise at all times any paper or other hard copy generated by or for HMIS that contains PPI when the hard copy is in a public area. When agency staff are not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to**

user access (e.g., username and password) must not be stored or displayed in any publicly accessible location.

- HMIS usernames and passwords cannot be shared with other users. Users should not keep username/password information in a public location (i.e., sticky notes on monitors).

SITE ADMINISTRATORS

Each Partner Agency is required to designate at least one Site Administrator. The roles and responsibilities of the Site Administrator are as follows:

- Provide a formal point of contact between agency users and CHIP.
- Ensure stability of the agency's connection to the Internet and HMIS, either directly or through communications with other technology professionals.
- Coordinate training for agency users that includes login and password protocols, logging off all unattended computers, privacy notice, federal and local regulations, and HMIS Policies and Procedures.
- Maintain data quality and compliance with data collection as defined in the HMIS Data Quality Plan.
- Ensure the on-time submission of required local and federal reporting.
- Provide support for generating agency reports.
- Monitor compliance with standards of Client confidentiality and ethical data collection, entry and retrieval.
- Participate in HMIS User Group meetings. Site Administrators are invited to join the HMIS Advisory Workgroup to inform policy but are not required.
- Communicate to HMIS Lead when users need to be removed or updated in the HMIS.
- Communicate project and funding updates and changes to the HMIS Lead including changes to bed unit inventory.

INDIVIDUAL END USERS

The Individual End Users of the HMIS consist of any staff that input, utilize, or have access to data in the HMIS. The roles and responsibilities of the Individual End User include the following:

- Abide by the protocols set forth in this document.
- Respect and abide by the policies set forth in the Privacy Policy, Individual User Agreement, and Security Policy.
- Use the HMIS in a manner that reflects the confidentiality of Clients and training provided.
- Participate in the HMIS User Group Meetings

HMIS Data Use and Disclosure

The HMIS Lead Agency requires that partner agencies notify individuals seeking their assistance that data collection, use, and disclosure will occur and be consistent with the Partner Agency Agreement. By entering data into the HMIS, the partner agency verifies that individuals have provided the partner agency with consent to use and disclose their data.

The HMIS Lead Agency and partner agencies may only collect, use, and disclose personally identifiable information (PII) and aggregate data for the specific purposes described in the HMIS Privacy Notice.

Data

UNIVERSAL DATA ELEMENTS

Universal data elements as defined by HUD's current HMIS Data Standards must be collected by all Participating Agencies for enrollments.

PROGRAM SPECIFIC DATA ELEMENTS

To meet the statutory and regulatory requirements of federally funded programs using HMIS, additional elements are required for different funding sources. Program Specific Data Elements such as income at entry and exit are elements that are required by at least one of the HMIS Federal Partner Programs. The Indianapolis CoC may elect to require all projects participating in HMIS to collect a subset of the Program Specific Data Elements, independent of funding source, to obtain consistent information across a range of projects that can be used to plan service delivery, monitor the provision of services, and identify Client outcomes.

FEDERAL PARTNER PARTICIPATION

Additional HMIS requirements may be defined by participating federal partners. HMIS specifications and instructions can be found in the respective HMIS manuals for each program type.

PROJECT DESCRIPTOR DATA ELEMENTS

Project Descriptor Data Elements are data that identify an organization, program, grant, and coding information per HUD's current HMIS Data Standards. These data elements are collected for every HMIS Participating Organization and Project.

DATA ELEMENTS TO BE EXCLUDED FROM DATA SHARING

Data elements that are organization specific and cannot be accessed by HMIS partner agencies are included in the table below; case notes are also excluded from data sharing. Clients may provide written consent to Agencies to share this information.

Data Elements Excluded:

Element Number	Description	Location in HMIS Software
4.05	Physical Disability	Barriers Assessment
4.06	Developmental Disability	Barriers Assessment
4.07	Chronic Health Condition	Barriers Assessment
4.08	HIV/AIDS	Barriers Assessment
4.09	Mental Health Disorder	Barriers Assessment
4.10	Substance Use Disorder	Barriers Assessment

DEDUPLICATION OF CLIENT RECORDS

CHIP will regularly review duplicate client records, and work to deduplicate multiple records with distinct Personal Identifier metadata elements that represent the same individual based on identifying information (such as name, date of birth, and Social Security Number).

REPORTING SECURITY INCIDENTS

If you witness or experience a security breach, you must notify your Agency's Site Administrator and the HMIS Lead. A security breach consists of an incident where client data and/or system access information has been lost, stolen, or missing. After the Agency Site Administrator and HMIS Lead have been notified, the HMIS Lead will inform the Site Administrator and any other necessary administrators and/or users of any corrective action.

The following is a list of security breaches that require mandatory reporting:

- **Lost or stolen computer that was used to access HMIS**
- **Username and/or password is lost or stolen**
- **When HMIS is accessed on an unsecured network**
- **Unauthorized use or access of HMIS**

While this list is not exhaustive, it is required that these incidents are reported. The HMIS lead should be notified by contacting a CHIP HMIS team member via phone and email.

DISASTER RECOVERY PLAN

The information in the Indianapolis HMIS environment is routinely backed up on HMIS off site servers every night and at several times during the day. Once every three months, CHIP receives a copy of the entire database.

In the event of large-scale data loss or corruption, the HMIS Administrator will be the primary contact to CHOs and the CoC. The HMIS Administrator will inform the CHOs and the CoC on the data loss/corruption, the extent of the loss/corruption, and corrective actions as they become available.

In the event that HMIS is unavailable for an extended period of time, CHIP will work with organizations to adequately record client information and transactions to be entered into the system at a later time.

DATA DISPOSAL

If an agency stores information electronically on a computer, external hard drive, etc., the agency must reformat the electronic medium twice (or erase with at least two passes) before the piece of equipment can be disposed. Any paper copies of data entered into the HMIS should be adequately shredded before disposal.

CONTRACTS AND OTHER ARRANGEMENTS SUCH AS PHYSICAL AND TECHNICAL SAFEGUARDS.

CHIP will retain copies of all contracts and agreements executed as part of the administration and management of the HMIS. This includes but is not limited to inter-agency MOUs for sharing client data, security for equipment, and agreements for technical security for equipment.

Trainings

Before an individual can gain access to HMIS, they must complete the HMIS New User Training through the Learning Management System (LMS). These trainings are self-paced, available online, and cover the Privacy and Security Policies, basic data entry functions, and basic data management functions. The new user's supervisor or site administrator should submit an HMIS Training Request Form on behalf of the new user to request access to the training site. These requests are housed in AirTable, which is also used to track trainee progression through the modules and record who has completed the training in its entirety. Once that training has been completed, each new user signs the HMIS User Agreement, which is then saved and stored by CHIP in a shared drive. Both AirTable and the shared drive are used to record new and pre-existing HMIS users.

Agencies can request specific trainings or ad hoc advanced trainings in addition to the Data Entry Training by contacting the HMIS Administrator.

USER PERMISSIONS

The following permissions are available for all HMIS users following the completion of training.

- **Delete and Recycle Function**
- **Data Explorer**
- **Data Entry**
- **Data Export (security training needed)**
- **Print Forms/Reports**
- **By Name List Access**

Technical Support

HMIS TECHNICAL SUPPORT AND ASSISTANCE

CHIP has two dedicated roles to address HMIS technical support and assistance- the HMIS Administrator and the HMIS Technical Assistance Coordinator. The HMS Administrator oversees the HMIS user experience, and the HMIS Technical Assistance Coordinator focuses on agency level data improvement and support. Below is an overview of available agency

support provided by each role. Support available may include but is not necessarily limited to the following items.

HMIS ADMINISTRATOR:

- **Addresses technical issues related to the HMIS software**
- **Works with HMIS software vendor for to address issues and optimize system**
- **HMIS Helpdesk (tickets submitted in the HMIS)**
- **HMIS program, grant, and project setup**
- **Annual Reporting**
- **New User Onboarding and Training (Learning Management System)**
- **Ongoing user training**
- **Creates and manages Help Center content**
- **Disseminates updates to the system and the workflows therein**
- **Security and Compliance**
- **HMIS User Agreements**
- **Agency Agreements**

THE HMIS TECHNICAL ASSISTANCE COORDINATOR

- **Conducts agency site visits annually or as needed/requested**
- **Provides open trainings and office hours as relevant**
- **Leads HMIS User Group and HMIS Planning Committee Meetings**
- **Administers annual organizational needs assessments,**
- **Data entry coaching (e.g. exit destinations, enrollments, assessments)**
- **Provides targeted training on request (1:1 or group)**
- **Implements the Community Data Quality Plan**
- **Data quality review and support (training or plan creation)**
- **System performance measures support (training or plan creation)**
- **Data collection workflow problem solving**

To request technical support or assistance, HMIS users can email the Administrator or Coordinator in accordance with the roles outlined above, submit a Technical Assistance Request Form through Airtable, or submit a ticket through the HMIS Helpdesk for specific software issues.