Indianapolis Continuum of Care

HMIS Policies and Procedures

11.4.15

Introduction

The purpose of the policies and procedures set forth in this manual are to establish standard operating procedures and to 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.

Responding to the desires of the community and the requirements set forth by the US Department of Housing and Urban Development (HUD), the City of Indianapolis, acting as the primary fiscal agent, requires the use of the HMIS at all sub-grantee agencies when applicable. The City of Indianapolis contracts with the Coalition for Homelessness Intervention and Prevention (CHIP) to manage the HMIS. The Indianapolis Continuum of Care has designated CHIP as the HMIS Lead. The HMIS uses the web-based software known as ClientTrack, and is administered locally by a consultant, @ Work Solutions. With HMIS under the management of CHIP, the CHIP Board of Directors and staff provide the direct oversight of HMIS.

The administration of the HMIS as provided by CHIP strives to achieve effective community solutions that address the identified needs of the community. The oversight decisions and practices reflect the desire to maximize the effectiveness and efficiency of HMIS among service providers while respecting and adhering to client's confidentiality. Additionally, the oversight decisions and practices seek to inform public policy and reflect best practices in order to comply with federal regulations.

Purpose and Benefits

The HMIS is an electronic data collection system that 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 service provision. To network informational resources, 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 and as well as a monitoring platform to ensure compliance with all funding regulations and requirements. The HMIS also provides standardized aggregate level data to inform the community and public policy of the current efforts, strengths, and needs of homelessness services.

Roles and Responsibilities

General Responsibilities of CHIP

CHIP has been selected by the Continuum of Care to be the HMIS Lead. These responsibilities include operating and maintaining the HMIS and administering the CoC plans for privacy, security, and data quality.

General Responsibilities of the HMIS Staff

- Ensuring participating agencies are entering the HUD minimum data elements as required and provide ongoing training opportunities for participating agencies.

- Ensure the compliance with current HMIS requirements.
- The first point of contact for users and agencies dealing with HMIS and HMIS related issues.
- Provide customized HMIS programming to collect and report locally identified client and community level outcome indicators.
- Provide data quality monitoring and feedback to ensure that accurate and reliable information is entered in the HMIS.
- Facilitate regular meetings of individual HMIS users.

Partner Agencies

Partner Agencies in HMIS are committed to improving the social welfare of those who may become homeless or are already experiencing homelessness in the community 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:

- Create and maintain internal procedures to collect, secure, and share client data, including compliance with the HMIS Privacy Notice.
- Comply with current HMIS data collection requirements.
- Ensure that services are not denied to a client who refuses to consent to share personal data on HMIS.
- Consent to authorize the City of Indianapolis and/or CHIP to utilize aggregate data for planning, reporting, and grant writing.
- Consent to authorize CHIP to reconcile and release de-identified aggregate data to the Continuum of Care 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 handbook.
- Maintain onsite equipment.
- Designate a Security Officer (typically the site administrator) and comply with correlating requirements.

Site Administrators

Each Partner Agency is required to designate a 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's users which includes login and password protocols, logging off all unattended computers, privacy notice, federal and local regulations, and HMIS Policies and Procedures.
- Respond to feedback from CHIP about data quality and compliance with data collection.
- Provide support for generating agency reports.
- Monitor compliance with standards of client confidentiality and ethical data collection, entry and retrieval.

- Serve as the Agency's Security Officer if no other staff is identified.
- Participate in meetings for individual HMIS users.

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 handbook.
- Respect and abide by the policies set forth in the Privacy Policy, Individual User Agreement, and Security Policy.
- Using the HMIS in a manner that reflects the confidentiality of clients and training provided.

Participation Expectations and Acceptable Use Practices

Minimum Program Participation Requirements for Partner Agencies

- Ability to maintain adequate internet connectivity in order to begin to participate and continue to participate in the HMIS system
- Meet with the HMIS Administrator to assess and address data security issues
- Meet the minimum technical specifications set forth by CHIP in the HMIS Systems Requirements
- Secure Partner Agency and Individual User Agreements for all staff who will have access to the HMIS
- Clients may see their record in ClientTrack (just as with hardcopy files). A client may request to have their information in ClientTrack changed.

General HMIS participant expectations for data security and confidentiality

- Locate computer systems in secured and semi-private areas on the agency's premises so that information on the screen cannot be seen by others.
- Abide by the established guidelines set forth in the Partner Agency and Individual User Agreements.
- Immediately report to CHIP 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
- Only use the HMIS in a manner that is pertinent and necessary for the organization.
- The data maintained in the HMIS will be treated as an agency would treat hard copy files of client information.

Requirements for participating agencies to continue to be in HMIS

- Only allow staff who have been trained to access and use the HMIS
- Ensure timely and accurate input and maintenance of client data
- Continued compliance with the most current HMIS data collection standards

Description of data sharing between users, agencies, funders, and CoC

Data sharing between stakeholders is pursuant to preventing duplication of services, coordination of referrals, reporting requirements, community planning, gaps analysis, and informing public policy. Data sharing for the purposes of reporting requirements, community planning, gaps analysis, and informing public policy will be de-identified, aggregate data at the agency, collection of agencies, or community level. Some examples would include (but not limited to) the annual Point-in-Time Count (PIT), annual Housing Inventory Chart (HIC), and the Annual Homelessness Assessment Report (AHAR).

Requirements for agency/CHIP termination of HMIS

- Agency may terminate HMIS participation upon sixty (60) days written notice to CHIP
- CHIP may terminate Agency or User access without cause or prior notice. Upon termination, CHIP may provide one copy of the data entered by the agency into HMIS as of the date of termination in an export format agreed up by both CHIP and Agency or in the most recent HUD defined export standard.
- Reasons for Agency or User access termination by CHIP include, but not limited to, violation of Agency or Individual User Agreements, failure to properly secure client level data, or failure to abide by the policies and procedures set forth in this handbook

Data

Universal Data Elements

Universal data elements as defined by the 2015 update to the 2014 HMIS Data Standards must be collected by all Participating Agencies for enrollments.

Program-Specific Data Elements

Program Data Elements such as income at entry and exit are collected by programs to comply with federal partner reporting and community goals. The Program-Specific Data Elements are required for all lodging programs from Contributing HMIS Organizations (CHOs) and other programs as required by federal partners per the 2015 update to the 2014 HMIS Data Standards. These elements include accurate program entry and exit dates.

Project Descriptor Data Elements

Project Descriptor Data Elements are data points that identify an organization, program, grant, and coding information. These data elements are collected for every CHO.

Data Elements to be excluded from data sharing

Data elements that are organization specific and cannot be accessed by HMIS partner agencies include information about the diagnosis or treatment of a mental illness, drug or alcohol addiction, HIV/AIDS, history of sexual abuse or domestic violence history. All records from agencies that exclusively provide those services (i.e. a CoC TBRA program from a community mental health center) are restricted from sharing. Clients may provide written consent to Agencies to share this information.

Security

All HMIS computers (any computer that accesses the HMIS) should be situated in secure locations (i.e. locked offices). If HMIS computers are in publicly accessible areas (i.e. laptop in meeting room or front desk area) they should be staffed at all times and screens should not be viewable by other individuals. All workstations should be password protected. This is not the same password as your HMIS login, rather a password to prevent access to the computer itself. A password protected screensaver should also be used. All workstations should have auto-updating virus protection and should be secured by either an individual or network firewall. The data maintained in the HMIS should be treated as an agency would treat hard copy files of client information.

HMIS usernames and passwords should not be shared with other users. Users should not keep username/password information in a public location (i.e. sticky notes on monitors). HMIS security policies require the use of Strict Passwords that must have at least one number, must be at least eight characters, must have at least one non-letter, non-numeric character, must contain at least one capital letter, and cannot be any of the previous six passwords you have used. Users should contact the HMIS Specialist to reset their login/password.

Log Monitoring

The HMIS Lead will review logs on a regular basis through automation and manual review.

Reporting Security Incidents

If you witness or experience a security breach you must notify your Agency's Security Officer 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 Security Officer and HMIS Lead have been notified, the HMIS Lead will inform the Security Officers 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 ClientTrack
- User name and/or password is lost or stolen
- When ClientTrack is accessed on an unsecured network.
- Unauthorized use or access of ClientTrack

While this list is not exhaustive, it is required that these incidents are reported.

Disaster Recovery Plan

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

In the event of large scale data loss or corruption, the HMIS Specialist will be the primary contact to CHOs and the CoC. The HMIS Specialist 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 ClientTrack 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.

Annual Security Review

Every year the HMIS Lead must conduct a security review which includes reviewing the physical locations where clients are interviewed; the physical locations where client data is entered, asking about select personnel files, the machines used to process client data, and internal methods for monitoring data security. The review will consist of ensuring the security methods and procedures are appropriate according to the following checklist:

- User names and passwords are not stored or posted in a public area
- User names and passwords are not being shared
- Computers automatically lock after a period of inactivity
- Screen savers require a password to log back in
- Computers are logged off ClientTrack when left unattended
- Computers have commercially available, auto-updating anti-virus software
- The Agency's network has an active firewall
- Personal computers used to access ClientTrack have commercially available, auto-updating anti-virus software and an active firewall
- Client data storage devices are properly disposed of according to the HMIS Security Plan
- Privacy Notices are posted in plain sight in areas where clients are interviewed and client information is processed
- Physical ClientTrack files are securely stored
- All corrective actions have been completed or are on track to be completed according to a corrective action plan
- All users have completed and signed Individual User Agreements

Agencies required to have stricter levels of compliance for hardware and confidentiality (such as an agency covered by HIPAA) will need to submit documentation of HIPAA compliance from the last review.

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 HMIS. This includes but is not limited to inter-agency MOUs for sharing client data, inter-agency MOUs for program monitoring that includes access to client files, agreements for physical security for equipment, and agreements for technical security for equipment.

Transmission of Information

All CHOs will not transmit protected personal information (i.e. name, DOB, or SSN) via email. End users will not save documents generated from HMIS with protected personal information onto the hard drive of their local machine or their network without adequate protection.

Technical Support

All technical issues related to the HMIS should be addressed to the HMIS Specialist at CHIP.

Trainings

Before an individual can gain access to the HMIS, he/she must go through the Data Entry (formerly called New User) Training. This training is held every month and covers the Privacy and Security Policies, the basic data entry functions, and basic data management functions. Agencies can request specific trainings in addition to the Data Entry Training by contacting the HMIS Specialist.

Additional and more advanced trainings include Data Editing and Reports Training. All of these are held on the same day, once a month. The purpose of the trainings is to increase the system's value through increased functionality at an agency level and to increase data quality through better practices.

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 HMIS should be adequately shredded before disposal.

Attachments
Partner Agency Agreement
Site Administrator Designation and Agreement
Individual User Agreement
Privacy Notice (Posting)
Privacy Notice (Full)

Partner Agency Agreement
Indianapolis Homeless Management Information System

This Agreement, hereinafter referred to as the "Agreement", is entered into this _____day of _____, , by and between _____ an Indiana nonprofit corporation whose principal place of business is located at _____, Indianapolis IN _____, hereinafter referred to as "Agency" and the Coalition for Homelessness Intervention and Prevention, Inc., an Indiana nonprofit corporation whose principal place of business is located at Suite 350, 1100 W 42nd Street, Indianapolis IN 46208, hereinafter referred to as "CHIP", collectively referred to as the "Parties".

Background

1. The Parties recognize the benefit of collaborating on efforts to collect, maintain and report computerized data to and from the Homeless Management Information System pertaining to service providers and their near-homeless and homeless clients. The Homeless Management Information System hereinafter shall be referred to as "HMIS";
2. The Parties agree that the ultimate goal of collecting, maintaining and reporting such computerized data is to improve the social welfare of those who are near becoming or are already homeless members of the community and avoid compromising the privacy of these individuals;

Based on the foregoing, this Agreement shall govern the relationship between the Parties and their rights and obligations as they pertain to the HMIS.

Section 1. Term

This Agreement shall become effective on the signing hereof by both Parties and shall continue in effect for a period of two (2) years, unless renewed or sooner terminated in accordance with the provisions hereof.

Section 2. Appointment of Agent

Agency appoints CHIP as its exclusive agent for the management of the computerized data services and CHIP accepts the appointment, subject to the terms and conditions set forth in this Agreement.

Section 3. Professional Management Standards and HMIS System Responsibilities

Section 3.1. Rights and Responsibilities of CHIP

a) CHIP agrees to exert its best efforts and to exercise the highest degree of professional skill and competence in operating and managing the HMIS in order that the HMIS satisfies the needs of Agency.

b) CHIP shall have the sole authority to establish policies, procedures and forms for use of the HMIS by Agency and shall provide Agency with a written copy of such policies and

procedures. CHIP will provide opportunities for Agency to comment on policies, procedures, and forms.

c) CHIP will provide to Agency regular opportunities to comment on the development and the performance of the HMIS through regularly scheduled user meetings and community progress updates.

d) CHIP will not release identifying client information to any organization other than the originating Agency or as identified in this Agreement or the Privacy Notice.

Section 3.2. Rights and Responsibilities of Agency

a) Agency will display the HMIS Privacy Notice Posting at the agency's intake area.

b) Agency will adopt the HMIS Privacy Notice and provide copies of the full Privacy Notice to clients upon request. Agency will provide reasonable accommodations for persons with disabilities to ensure that they understand the Privacy Notice.

c) Agency agrees to use the HMIS Privacy Notice provided by CHIP, to obtain client consent, hereinafter referred to as "Consent," of each client before any of his/her personal information is shared through the HMIS. If a client refuses to provide Consent, his/her personal data may be entered into the HMIS only for access by and use of Agency, and Agency is prohibited from sharing such data with any other person or entity through the HMIS. **Agency agrees that it will not refuse to serve any client because that client denies Consent to Agency to share his/her personal data through the HMIS.**

d) Agencies will retain all originals or copies of documents referenced in the document library for a minimum of seven (7) years. Agency agrees to facilitate one (1) annual audit of such documents by CHIP or its designee at a time to be determined by CHIP. Agency will establish mechanisms to protect hard copy data that is either generated by or for HMIS, including reports, data entry forms, signed consent forms, etc.

e) Agency agrees to comply with the current HUD Data and Technical Standards and Indianapolis Continuum of Care HMIS data collection requirements. Agency shall make every effort to ensure that all client data entered or shared in the HMIS shall be truthful, accurate, complete and timely.

f) Agency agrees to abide by HMIS policies and procedures, including but not limited to, those pertaining to Consent, client confidentiality, collecting and entering minimum data elements, the HMIS Security Plan, and maintaining the integrity of the data. Policies and procedures are available by contacting CHIP and at www.chipindy.org

g) Agency agrees to comply with all state and federal laws regulating the collection, storage, and use of data. Agency agrees to comply with additional Continuum of Care privacy policies on notification and/or consent.

h) Agency agrees to ensure that prior to any access to the HMIS, employees, volunteers and agents, hereinafter referred to as "User" or "Users", receive appropriate instruction on the use of the HMIS, confidentiality, policies and procedures, and use of the system, and will access the HMIS only for purposes authorized by Agency. Agency must allocate paid staff time for training. The Agency is responsible for the actions of its Users and for their training and supervision.

i) Agency will ensure that all Users understand and comply with the Privacy Notice.

j) At Agency's discretion, it may designate and terminate any User's access to the HMIS. Each User will have a unique user name and password that may not be shared with any other person and which governs the security level for that User. Users will be required to sign a User Agreement. Prior to access to the HMIS by any User, Agency agrees that no User will access the HMIS until CHIP receives one (1) copy of such User's executed User Agreement. Agency further agrees to notify CHIP promptly when Agency designates or terminates any User's authorization to access the HMIS.

k) Agency will adopt a written grievance policy related to all client data entered in the HMIS and will provide all clients with a copy of such policy upon client request.

l) Upon receipt of a written request from a client, Agency agrees to provide any client with an opportunity to review his/her personal information in the HMIS, to request corrections in the data, and to pursue a grievance regarding the data changes or corrections in the data.

m) Agency agrees to immediately report to CHIP in writing 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.

n) In the event of collaborative agreements among agencies, each agency shall be responsible for providing CHIP with authorization in order that CHIP may establish protocols necessary for exchanging or sharing client data. The collaborating Agencies must provide a copy of the agreements that define and authorize the sharing of data to CHIP.

o) Agency must designate an Agency Site Administrator who will serve as the Agency's primary contact related to HMIS issues, including training, data collection, and attendance at User Group Meetings.

Section 3.3. Agency Participation without direct User input into HMIS

a) Agencies may decline to use the HMIS interface if they have another appropriate data system collecting demographic and service data. These Agencies are still responsible for providing accurate and timely client, demographic and services data for Continuum-wide reporting.

b) Agencies that do data transfer instead of using the HMIS interface must a) provide quality, accurate timely data in a digital format, and b) provide a regularly scheduled automated data transfer of data files in the appropriate format, no less than once annually.

c) Agencies that do not use the HMIS interface must still abide by policies concerning consent, confidentiality and timely accurate data entry, and will still be subject to the Agency participation fees as outlined in Section 6.

Section 4. HMIS Data

a) Agency acknowledges that all data is highly confidential and agrees that it will not use or disclose data other than as permitted or required by this Agreement or as permitted or required by law. Agencies will use appropriate standards to prevent use or disclosure of

the information other than as permitted by this Agreement, the HMIS Policies and Procedures, or the Privacy Notice.

b) Agency agrees that it has appropriate data confidentiality protections in place, including agency policies and procedures and training, to ensure that sensitive or protected client information is properly collected, recorded, and/or shared, including but not limited to HIV/AIDS, mental health, addictions, and disability.

c) Agency shall be able to view, enter and edit data pertaining to all of Agency's clients and services. Agency shall be able to produce data reports by exporting data from the HMIS or by any other appropriate method available from the HMIS.

d) Approximately two (2) times per calendar year, CHIP will provide to Agency a report that includes community-wide, aggregate HMIS data. These reports will contain raw, point-in-time data that will not disclose any confidential information pertaining to clients. Agency may utilize the information in these reports for any purpose. CHIP shall not publicly report Agency's proprietary information, including but not limited to client services, client procedures, or client demographics, unless CHIP receives written authorization from Agency.

e) Agency further agrees to authorize CHIP to utilize data for planning, reporting and grant writing. Agency also agrees to authorize CHIP to reconcile and release de-identified aggregate data to the Continuum of Care facilitator or any other governmental or other entity for purposes that include, without limitation, the development of Consolidated Plans, Gaps Analysis, HUD reporting, Emergency Shelter Grants, Continuum of Care funding applications, etc.

f) CHIP may contract with external organizations to perform system administration, technical support, auditing, research and compliance with legal and regulatory requirements, data quality assurance, data analysis, and data reporting. The Agency grants CHIP's contractors permission to access and utilize client data for the purposes identified above. CHIP and its contractors will not disclose information except as permitted or required in this agreement, in the Privacy Notice, or required by law. Agency may request a list of all CHIP contractors at any time in writing to the CHIP System Administrator.

Section 5. HMIS Hardware, Software and Connectivity

a) Agency shall provide and maintain computer systems, operating software, networks and Internet access that meet at least the minimum technical specifications set forth by CHIP in "*HMIS System Requirements*".

b) Agency agrees to locate its computer systems in secured and semi-private areas on the Agency's premises.

c) Agency acknowledges that the sublicense to use the HMIS or any software provided to Agency by CHIP confers no ownership or other rights to the software, other than the specific right to use the software according to the terms and conditions of this Agreement. Agency, its employees, volunteers and agents are prohibited from and have no right to sell, distribute or transfer an original or any copy of the software or software manual, if any. Agency, its employees, volunteers and agents are also prohibited from allowing any non-licensed party to access or use the software.

d) ClientTrack, Inc. (the software developer) will maintain the server and software, perform regular data backups and comply with industry standards for security of the server and the data on it. The data and the software will be available for access 24 hours a day. However, the server may be occasionally taken down for maintenance and service, but ClientTrack, Inc. and @ Work Solutions will make every effort to avoid disruption during daily operating hours.

e) Agency will be able to access a demonstration version of the software with pretend client data for demonstration and training. Real client data should never be used for this purpose.

Section 6. Compensation for HMIS

a) To maintain the HMIS and to obtain a sublicense(s) to use HMIS, Agency agrees to pay a fee in the amount of $20 per user per month. @ Work Solutions will invoice the license fees quarterly to the Agency in advance. User licenses may be temporarily deactivated if payment of invoices by Agency is not received by @ Work Solutions within 45 days of invoice date..

b) Data pertaining to homeless and near homeless clients may be entered in the HMIS by Agency; however, Agency may incur other fees related to additional HMIS services for clients served by programs that are not targeted towards homeless and/or homeless prevention. These additional fees will be determined on a case by case basis.

c) CHIP and @ Work Solutions will provide limited technical assistance for troubleshooting, report generation, imports and exports, one-on-one and classroom training for users. Extensive customizations to the software and for new report generation are available to Agency for an additional fee, to be determined on a case by case basis.

Section 7. Eligibility and Termination

Section 7.1 Eligibility

CHIP will have the sole authority for determining eligibility for participation by Agency in the HMIS. Participation in the HMIS by one or more of Agency's programs does not guarantee that all of Agency's programs are eligible to participate in the HMIS.

Section 7.2 Termination

a) Agency may terminate this agreement, without cause, upon sixty (60) days written notice to CHIP.

b) CHIP may terminate Agency's participation in the HMIS without cause and without prior notice to Agency. In the event of termination by CHIP, Agency will receive one (1) export copy of all data entered by Agency into the HMIS as of the date of termination. Agency data in the system on the date of termination will remain in the HMIS indefinitely and may be utilized for any lawful purpose whatsoever. In the event of termination, Agency agrees that all fees are non-refundable.

c) CHIP may terminate an individual User's access to the HMIS without cause and without prior notice to Agency. CHIP will immediately contact Agency if an individuals User's

access to the HMIS is terminated. Termination of an individual User's access to the HMIS may have no effect on Agency's participation in the HMIS.

d) On termination of this Agreement, it is agreed by both Parties:

i) All records in the possession of CHIP and data in the HMIS, together with all supplies or other items of property owned by CHIP and in Agency's possession, shall be forthwith delivered to CHIP;

ii) CHIP's right to compensation shall immediately cease, but CHIP shall be entitled to be compensated for services rendered hereunder prior to the date of termination; and

Section 8. Renewals

Unless written notice of expiration from either party is received thirty (30) days before the expiration date of this Agreement, the Agreement shall be automatically renewed, under the same terms and conditions contained herein, for another one (1) -year term, and the same notice and renewal terms shall apply to each subsequent renewal period.

Section 9. Mailing and Notice Requirements

(a) All notices and periodic statements required under this Agreement shall be in writing, and shall be delivered in person or by regular United States mail. Notices and periodic statements shall be deemed communicated as of deposit in the United States mail, delivery to an express company, or on personal delivery.

(b) Notices and periodic statements shall be addressed as follows:

CHIP: HMIS System Administrator
1100 W 42nd Street, Suite 350
Indianapolis IN 46208

AGENCY:

_____

_____

_____

_____

Section 10. Assignment

At all times this Agreement will inure to the benefit and constitute a binding obligation on the Parties and their respective successors and assigns. This Agreement may not be assigned by the either Party without the prior written consent of the other Party hereto.

Section 11. Entire Agreement

a) This Agreement constitutes the entire agreement between the Parties, and no change will be valid unless made by supplemental written agreement, executed and approved by both of the Parties hereto.

b) If this Agreement is executed in several counterparts, each shall constitute a complete original Agreement which may be introduced in evidence or used for any other purpose without production of any of the other counterparts.

IN WITNESS WHEREOF, CHIP and Agency have executed this Agreement in Indianapolis, Indiana on the dates subscribed below.

Coalition for Homelessness Intervention and Prevention of Greater Indianapolis, Inc.

By: _____

Title: _____

Date: _____

Agency:

By: _____

Printed: _____

Title: _____

Date: _____

Site Administrator Designation
Indianapolis Homeless Management Information System

The HMIS Site Administrator is the primary HMIS contact at the Agency. This person will be responsible for:

- Providing a single point of contact between the end users at the Agency and the Coalition for Homelessness Intervention and Prevention.
- Ensuring the stability of the Agency's connection to the Internet and the HMIS, either directly or through communications with other technology professionals.
- Training and coordinating Agency end users: This training includes the login and password protocols, logging off all unattended computers, privacy notice, federal and local regulations, and HMIS Policies and Procedures.
- Responding to feedback from CHIP about data quality and compliance with minimum data elements collection.
- Providing support for the generation of agency reports.
- Monitoring compliance with current standards of client confidentiality, ethical data collection, data entry and retrieval, and information security.
- Participating in the HMIS User Group Meetings.

The following individual is designated the HMIS Site Administrator for the Agency named below:

Agency Name:	
Name of Site Administrator (Print):	
Title:	
Phone Number:	
Email Address:	

_____ _____

Signature of Site Administrator Date

Individual User Agreement

Indianapolis Homeless Management Information System

Name (Please Type or Print) _____

Agency/Program Name (Please Type or Print) _____

Email Address (Please Type or Print) _____

Phone Number with Extension _____

Indianapolis providers recognize the privacy of client needs in the design and management of the Indianapolis Homeless Management Information System. These needs include the desire to improve community efforts that will lead to the elimination of homelessness in Indianapolis, the need to maintain client confidentiality, and the need to treat personal data of individuals with the utmost respect and care.

As the guardians entrusted with this personal data, Indianapolis HMIS users have a moral and a legal obligation to ensure that the data being collected is accessed and used appropriately. It is also the responsibility of each user to ensure that client data is only used to the ends to which it was collected - ends that have been made known to clients and are consistent with the mission of the Indianapolis HMIS. Proper user training, adherence to the Indianapolis HMIS Policies and Procedures Manual, and a clear understanding of client confidentiality are vital to achieving these goals.

Relevant points regarding client confidentiality include:

- Partner Agencies shall at all times have rights to the data pertaining to their clients that was created or entered by them in the Indianapolis HMIS. Partner Agencies shall be bound by all restrictions imposed by clients pertaining to the use of personal data that they do not formally release.
- All Partner Agencies must have a signed HMIS Agency Agreement with the Coalition for Homelessness Intervention and Prevention in order to participate in the HMIS.
- Client data may be entered into the HMIS with implied client consent.
- Client authorization to share data in the Indianapolis HMIS may be revoked by that client at any time through a written notice.
- No client may be denied services for failure to provide authorization for sharing data within the HMIS.
- Clients have a right to inspect, copy and request corrections in their HMIS records.
- Indianapolis HMIS Users will maintain HMIS data in such a way as to protect against revealing the identity of clients to unauthorized agencies, individuals or entities.

- Any Indianapolis HMIS User found to be in violation of the Indianapolis HMIS Policies and Procedures, the points of client confidentiality in this User Agreement, or the points of user responsibility in this User Agreement, may be denied access to the Indianapolis HMIS.

I affirm the following points of User Responsibility:

- I have received a copy of the HMIS Privacy Notice. I understand and agree to comply with the Privacy Notice.
- I will only collect, enter, view, disclose and extract data in the Indianapolis HMIS that is necessary to perform my job.
- I will keep my username and password secure and will not share my username and password with other individuals inside or outside my organization.
- I will maintain the confidentiality of client data in the Indianapolis HMIS as outlined above and in the Indianapolis HMIS Policies and Procedures Manual, the Privacy Notice, and the Privacy Policy (to be approved by the CoC Planning Body).
- I will provide reasonable accommodation to persons with disabilities and persons that do not speak English to ensure that they understand the Privacy Notice.
- I will comply with state and federal law governing the collection, storage, and use of client information, and I will comply with the Continuum of Care procedure for providing notice and/or consent to clients.
- I must take all reasonable means to keep my password physically secure.
- If I am logged into the Indianapolis HMIS and must leave the work area where the computer is located, I **must log off** of the Indianapolis HMIS before leaving the work area.
- A computer that has the Indianapolis HMIS "open and running" shall never be left unattended.
- Hard copies of Indianapolis HMIS information must be kept in a secure file.
- When hard copies of Indianapolis HMIS information are no longer needed, they must be properly destroyed to maintain confidentiality.
- If I notice or suspect a security breach, I must immediately notify my Agency Site Administrator for the Indianapolis HMIS or the HMIS System Administrator at the Coalition for Homelessness Intervention and Prevention.
- I will comply with all aspects of the HMIS Security Plan (to be approved by the CoC Planning Body).

I understand and agree to comply with all the statements listed above.

_____ _____

Signature, Indianapolis HMIS User Date

_____ _____

Signature, Partner Agency Site Administrator Date

POSTING: Privacy Notice

Indianapolis Homeless Management Information System

Effective 10/1/2009
Version 1.2

When you request services from this agency, we enter information about you and members of your family into a computer system called Indianapolis Homeless Management Information System (HMIS). The HMIS is used by many social service agencies in Indianapolis that provide housing and related services.

We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless individuals, and to better understand the need of homeless individuals. We only collect information that we consider to be appropriate.

We may use or disclose your information to provide you with services. We may also use or disclose it to comply with legal and other obligations. We assume that you agree to allow us to collect information and to use or disclose it as described in the full notice. You can inspect personal information about you that we maintain. You can also ask us to correct inaccurate or incomplete information. You can ask us about our privacy policy or practices. We respond to questions and complaints. Read the full notice for more details. Anyone can have a copy of the full notice upon request.

Privacy Notice

Indianapolis Homeless Management Information System

Full Notice

Effective 10/1/2009
Version 1.2

A. What This Notice Covers

1. This notice describes the privacy policy and practices of the Indianapolis Homeless Management Information System (HMIS) and [Agency Name]. Our main office is at [Address, email/web address, telephone.]
2. The policy and practices in this notice cover the processing of protected personal information for clients of [Name of Participating Organization]. If this agency is a covered entity under HIPAA, you may have additional rights regarding your protected health information and these rights will be described to you in the agency's Notice of Privacy Practices under HIPAA
3. Protected Personal information (PPI) is any information we maintain about a client that:
    a. allows identification of an individual directly or indirectly
    b. can be manipulated by a reasonably foreseeable method to identify a specific individual, **or**
    c. can be linked with other available information to identify a specific client. When this notice refers to personal information, it means PPI.
4. We adopted this policy because of standards for Homeless Management Information Systems issued by the Department of Housing and Urban Development. We intend our policy and practices to be consistent with those standards. See 69 Federal Register 45888 (July 30, 2004).
5. This notice tells our clients, our staff, and others how we process personal information. We follow the policy and practices described in this notice.
6. We may amend this notice and change our policy or practices at any time. Amendments may affect personal information that we obtained before the effective date of the amendment.
    a. Amendments to this privacy notice will be approved by the HMIS System Administrator.

7. We give a written copy of this privacy notice to any individual who asks.
8. We maintain a copy of this privacy notice on the HMIS website at www.chipindy.org.

B. How and Why We Collect Personal Information

1. We collect personal information only when appropriate to provide services or for another specific purpose of our organization or when required by law. We may collect information for these purposes:
    a. to provide or coordinate services to clients
    b. to locate other programs that may be able to assist clients
    c. for functions related to payment or reimbursement from others for services that we provide
    d. to operate our organization, including administrative functions such as legal, audits, personnel, oversight, and management functions
    e. to comply with government reporting obligations
    f. when required by law

2. We only use lawful and fair means to collect personal information.
3. We normally collect personal information with the knowledge or consent of our clients. If you seek our assistance and provide us with personal information, we assume that you consent to the collection of information as described in this notice.
4. We may also get information about you from:
    a. Individuals who are with you
    b. Other private organizations that provide services
    c. Government agencies
    d. Telephone directories and other published sources, including internet directories
    e. Other organizations with whom we have a formal partnership

5. We post a sign at our intake desk or other location explaining the reasons we ask for personal information. The sign says:

When you request services from this agency, we enter information about you and members of your family that are with you into a computer system called Indianapolis Homeless Management Information System (HMIS). The HMIS is used by many social service agencies in Indianapolis that provide housing and related services.

We collect personal information directly from you for reasons that are discussed

in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless individuals, and to better understand the need of homeless individuals. We only collect information that we consider to be appropriate.

We may use or disclose your information to provide you with services. We may also use or disclose it to comply with legal and other obligations. We assume that you agree to allow us to collect information and to use or disclose it as described in the full notice. You can inspect personal information about you that we maintain. You can also ask us to correct inaccurate or incomplete information. You can ask us about our privacy policy or practices. We respond to questions and complaints. Read the full notice for more details. Anyone can have a copy of the full notice upon request.

C. How We Use and Disclose Personal Information

1. We use or disclose personal information for activities described in this part of the notice. We may or may not make any of these uses or disclosures with your information. We assume that you consent to the use or disclosure of your personal information for the purposes described here and for other uses and disclosures that we determine to be compatible with these uses or disclosures:

   a. to **provide or coordinate services** to individuals; data may be shared with other HMIS participating agencies (a copy of participating agencies can be found at www.chipindy.org)

   b. for functions related to **payment or reimbursement for services**

   c. to **carry out administrative functions** such as legal, audits, personnel, oversight, and management functions

   d. to **create de-identified (anonymous) information** that can be used for research and statistical purposes without identifying clients

   e. **when required by law** to the extent that use or disclosure complies with and is limited to the requirements of the law

   f. to **avert a serious threat to health or safety** if

      (1) we believe that 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

   g. to **report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority** (including a social

service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence

(1) under any of these circumstances:

(a) where the disclosure **is required** by law and the disclosure complies with and is limited to the requirements of the law

(b) if the individual agrees to the disclosure, **or**

(c) to the extent that the disclosure is **expressly authorized** by statute or regulation, **and**

(I) we believe the disclosure is necessary to prevent serious harm to the individual or other potential victims, **or**

(II) if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought **is not intended to be used against the individual** and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

and

(2) when we make a permitted disclosure about a victim of abuse, neglect or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:

(a) we, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm, **or**

(b) we would be informing a personal representative (such as a family member or friend), and we reasonably believe the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment.

h. for **academic research purposes**

(1) conducted by an individual or institution that has a formal relationship with the CHO if the research is conducted either:

(a) by an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a designated CHO program administrator (other than the individual conducting the research), **or**

(b) by an institution for use in a research project conducted under a written research agreement approved in writing by a designated CHO program administrator.

and

(2) any written research agreement:

(a) must establish rules and limitations for the processing and security of PPI in the course of the research

(b) must provide for the return or proper disposal of all PPI at the conclusion of the research

(c) must restrict additional use or disclosure of PPI, except where required by law

(d) must require that the recipient of data formally agree to comply with all terms and conditions of the agreement, **and**

(e) is not a substitute for approval (if appropriate) of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

i. to a law enforcement official **for a law enforcement purpose** (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:

(1) in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena

(2) if the law enforcement official makes a **written request** for PPI that:

(a) is signed by a supervisory official of the law enforcement agency seeking the PPI

(b) states that the information is relevant and material to a legitimate law enforcement investigation

(c) identifies the PPI sought

(d) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, **and**

(e) states that de-identified information could not be used to accomplish the purpose of the disclosure.

(3) if we believe in good faith that the PPI constitutes **evidence of criminal conduct** that occurred on our premises

(4) in response to an oral request for the purpose of **identifying or locating a suspect, fugitive, material witness or missing person** and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics, **or**

(5) if

(a) the official is an authorized federal official seeking PPI for the provision of **protective services to the President** or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by

22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others), **and**

(b) the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

and

j. to comply with **government reporting obligations** for homeless management information systems and for oversight of compliance with homeless management information system requirements.

D. How to Inspect and Correct Personal Information

1. You may inspect and have a copy of your personal information that we maintain. We will offer to explain any information that you may not understand.
2. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
3. To inspect, get a copy of, or ask for correction of your information, contact your agency case manager and ask, either orally or in writing, to view, either on the screen or a printed copy, your information contained in the HMIS.
4. We may deny your request for inspection or copying of personal information if:
   a. the information was compiled in reasonable anticipation of litigation or comparable proceedings
   b. the information is about another individual (other than a health care provider or homeless provider)
   c. the information was obtained under a promise or confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information, **or**
   d. disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.
5. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial
6. We may reject repeated or harassing requests for access or correction.

E. Data Quality

1. We collect only personal information that is relevant to the purposes for which we plan to use it. To the extent necessary for those purposes, we seek to maintain only personal information that is accurate, complete, and timely.
2. We are developing and implementing a plan to dispose of personal information not in current use seven years after the information was created or last changed. As an alternative to disposal, we may choose to remove identifiers from the information.
3. We may keep information for a longer period if required to do so by statute, regulation, contract, or other requirement.

F. Complaints and Accountability

1. We accept and consider questions or complaints about our privacy and security policies and practices.
    a. Any questions or complaints regarding our privacy and security policies and practices should be addressed to the following:
        i. HMIS Site Administrator, [Agency name and address and phone number]. The HMIS Site Administrator will respond in writing within 30 days to the question or complaint.
        ii. If the response from the HMIS Site Administrator is unsatisfactory, your original questions and/or complaints, along with the response from the HMIS Site Administrator, should be forwarded to the HMIS System Administrator, 1100 W 42nd Street, Suite 350, Indianapolis, IN 46208, 317-630-0856. The HMIS System Administrator will respond in writing within 30 days to the question or complaint.
2. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy notice. Each staff member must receive and acknowledge receipt of a copy of this privacy notice.

G. Privacy Notice Change History

1. Version 1.2, Effective 10/1/2009, Amended Policy