

## *Individual User Agreement*

### INDIANAPOLIS HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

\_\_\_\_\_  
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 HMIS. 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.

Indianapolis HMIS users have a responsibility to ensure that client data is only used to the ends made known to clients and that 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 (CHIP) 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 by not transmitting Protected Personal Information (PPI) across a public network or distributing such information through email. PPI is any information that allows identification of an individual directly or indirectly; can be manipulated by a reasonably foreseeable method to identify a specific individual, or; can be linked with other available information to identify a specific client.



- 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 and the HMIS Privacy Notice.
- I will provide reasonable accommodation to persons with disabilities and persons that do not speak English to ensure that they understand the HMIS 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 with 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 and the HMIS Administrator at CHIP.

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

\_\_\_\_\_  
Signature, Indianapolis HMIS User

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature, Partner Agency Site Administrator

\_\_\_\_\_  
Date