



**USER HMIS AGREEMENT**

The HMIS system used by the Changing Homeless, Inc. (CHI- as HMIS Lead) is an information system that maintains information regarding the characteristics and service needs of Clients for a variety of reasons, including the provision of more effective and streamlined services to Clients and the creation of information which communities can use to determine the use and effectiveness of services. The user noted below has been designated by CHI as a representative able to use the HMIS.

Name (Last, First, MI):		
Work Location Address:		Location Zip:
2nd Work Location Address:		Location Zip:
3rd Work Location Address:		Location Zip:
Job Title:		
Email Address:		
Office Phone:		
Cell Phone:		
Model this user after:		(First and Last Name)
Is this a super user?		(yes or no)
Is this a case manager?		(yes or no)
Supervisor:		

## 1. User Policy

Partner Agencies who use HMIS and each User within any Partner Agency is bound by the Standard Operating Procedures (SOPs) of HMIS. By signing this agreement, you are agreeing to read the SOPs, realize their importance in the HMIS, and to conduct your work according to what is described in these SOPs. All SOPs (new and revised) must be read within 10 working days of the notice of revision. All SOPs must be read at least annually. Failure to comply with the HMIS policy and procedures may result in disciplinary action from the Partner Agency. Users are bound by their Agency policies in addition to the policies set forth in this agreement.

It is a Client's decision about which information, if any, is to be shared with any other Partner Agencies. **Notice of Uses & Disclosures** shall be signed by Client and fully reviewed with Client in a manner to insure that Client fully understood the information (e.g. securing a translator if necessary) before any identifiable Client information is designated in HMIS for sharing with any Partner Agencies or the Coalition. User shall insure that the HMIS **Notice of Uses and Disclosures** was reviewed with the Client.

## 2. User Responsibility

Your username and password give you access to HMIS.

Initial each item below to indicate your understanding and acceptance of the proper use of your username and password. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination from HMIS access, and may result in disciplinary action from the Partner Agency as defined in the Partner Agency's personnel policies.

I agree to maintain the confidentiality of Client information in HMIS in the following manner:

\_\_\_\_\_ My username and password are for my use only and will not be shared with anyone. I will take reasonable means to keep my password secure.

\_\_\_\_\_ I will not use the browser capacity to remember passwords: I will enter the password each time I log on to HMIS.

\_\_\_\_\_ I will only view, obtain, disclose, or use the database information that is necessary to perform my job.

\_\_\_\_\_ I understand that the only individuals who may directly access HMIS Client information are authorized users, and I will take these steps to prevent casual observers from seeing or hearing HMIS Client information.

\_\_\_\_\_ I will log off of HMIS before leaving my work area, or make sure that the HMIS database has "timed out" before leaving my work area. I will not leave unattended any computer that has HMIS "open and running".

\_\_\_\_\_ I will apply my agency's privacy and confidentiality requirements for all information entered in or obtained from HMIS whether transmitted by oral, written, or digital means.

\_\_\_\_\_ I will keep my computer monitor positioned so that persons not authorized to use HMIS cannot view it.

\_\_\_\_\_ I will store hard copies of HMIS information in a secure file and not leave such hard copy information in public view on my desk, or on a photocopier, printer or fax machine.

\_\_\_\_\_ I will properly destroy hard copies (i.e. shredding) of HMIS information when they are no longer needed unless they are required to be retained in accordance with applicable law.

\_\_\_\_\_ I will not discuss HMIS confidential Client information with staff, Clients, or Client family members in a public area.

\_\_\_\_\_ I will not leave messages on answering machines or voicemail systems that contain HMIS confidential Client information.

\_\_\_\_\_ I will keep answering machine volume low so that HMIS confidential information left by callers is not overheard by the public or unauthorized persons.

\_\_\_\_\_ I understand that a failure to follow these security steps appropriately may result in a breach of Client HMIS confidentiality and HMIS security. If such a breach occurs, my access to HMIS may be terminated and I may be subject to further disciplinary action as defined in the partner agency's personnel policy.

\_\_\_\_\_ If I notice or suspect a security breach, I will immediately notify the Director of my Agency and CHI.

### 3. User Code of Ethics

- Users must be prepared to answer Client questions regarding HMIS.
- Users must faithfully respect Client preferences with regard to the sharing of Client information within HMIS. Users must accurately record Client's preferences by making the proper designations as to sharing of Client information and/or any restrictions on the sharing of Client information.
- Users must allow Client to change his or her information sharing preferences at the Client's request.
- Users must not decline services to a Client or potential Client if that person refuses to allow sharing of information within HMIS
- Users have primary responsibility for information entered by the User. Information Users enter must be truthful, accurate and complete to the best of User's knowledge.
- Users will not solicit from or enter information about Clients into HMIS unless the information is required for a legitimate business purpose such as to provide services to the Client.

Users will not use HMIS database for any violation of any law, to defraud any entity or conduct any illegal activity. \_\_\_\_\_

Upon Client written request, users must allow a Client to inspect and obtain a copy of the Client's own information maintained within HMIS. Information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding need not be provided to Client. Users must permit Clients to file a written complaint regarding the use or treatment of their information within HMIS. Complaints must be submitted in writing to the Agency HMIS Administrator: CHI, HMIS Administrator 660 Park Street Jacksonville, FL 32204. The Coalition will bring your complaint to the CHI HMIS Data Committee, which will attempt a voluntary resolution of the complaint.

This Agreement will be renewable each year contingent upon the user completing the required recertification requirements. This Agreement may be terminated by Agency or HMIS (due to but not limited to termination of employment, security violation, etc.). If this Agreement is terminated, User will no longer have access to HMIS.

**Signed,**

\_\_\_\_\_  
User Signature

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

### 3. AGENCY CERTIFICATION

As an authorized representative of my agency, I certify to CHI that the above employee has a background check on file that complies with my agency's requirements and shows this employee (user) to have no convictions on record that show any violations of the crimes described in Florida Statutes in this or any state for:

- Fraudulent Practices - Chapter 817
- Computer-Related Crimes – Chapter 815
- Forgery and Counterfeiting – Chapter 831
- Violations Involving Checks and Drafts – Chapter 832
- Defamation; Libel; Threatening Letters and Similar Offenses – Chapter 836
- Perjury - Chapter 837
- Offenses Concerning Racketeering and Illegal Debts – Chapter 895
- Offenses Related to Financial Transactions – Chapter 896
- Any other Felony offense that, in a reasonable person's mind would create a security risk for the HMIS system.

Agencies that have employees with background offenses can obtain permission for them to use HMIS as a 'read-only' system.

Agencies may also request a compliance variance on a case by case basis for any employee whose felony conviction is more than 10 years old.

For the purposes of this provision, no felony record with a disposition where the record has been sealed or expunged or where there was any other disposition where adjudication of guilt was withheld shall be considered to violate the above requirements.

Agency must maintain a current background check on file at the agency and will make said record available as a part of monitoring and auditing of agency documentation if requested by the HMIS Administrator or HMIS Lead.

Signed,

\_\_\_\_\_  
Authorized Agency Signature

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

Approved:

\_\_\_\_\_  
HMIS Representative Signature

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date