HMIS Manual and Agency MOU

FL-510

The HMIS system used by the HMIS Lead, Changing Homelessness, Inc. (HMIS Lead, CHI) 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.

This manual applies to the COC, the Lead Agency, the Agency partners, the Agency Users, and any other entity authorized to use the HMIS.

User Agency Policy

HUD Regulations and Authority

Partner User Agencies who use HMIS and each User within any Agency are bound by the Standard Operating Procedures (SOPs) of HMIS and all relevant HUD, VA, ESG regulations and the regulations of any other local, state, and federal authority by statute or order. By signing this agreement, you are agreeing to read the SOPs (as they are provided), realize their importance in the HMIS, and to conduct your agency's 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 should be re-read at least annually. Agency staff should also be encouraged to read and re-read applicable policies as they are provided. Failure to comply with the HMIS policy and procedures may result in disciplinary action from the Lead Agency, including being barred from the system. Users are bound by their Agency policies in addition to the policies set forth in this agreement.

HMIS Lead, CHI Regulations and Authority

As a member agency using the HMIS system, it is your responsibility to follow all directives of the HMIS Lead, CHI. The Data Committee is responsible for providing congruent policies that would support HUD regulations. As a member of the Northeast Florida CoC, your agency is bound by the committee's directives just as they are by HUD directives. Your use of the system constitutes such an agreement on your agency's part. Failure to comply with HMIS standards will initiate corrective action which could lead up to defunding of your COC, VA, or ESG Program.

Client Release and Data Ownership

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 Northeast Florida CoC. User shall insure that the HMIS ***Notice of Uses and Disclosures*** was reviewed with the Client.

Data within the system is owned by the Client. The agency who enters information into the system does so at the behest of the Client. The data is not owned by the agency. The data is not owned by the HMIS Lead. It is the Clients' data. No policy or provision should be written or propagated the detriment of the Clients' wishes.

My Agency and its Personnel Responsibilities

HMIS System and Intent

The intention of the HMIS system is to correctly capture all Client data at the time of interaction with the Client. Agency processes, culture, and management should be reflective of this intent. Using the HMIS system as a data capture methodology post Client interaction invites errors. All data entered into the system (especially personally identifiable information or PIM) should be corroborated with other legal sources such as state or federal issued Identification.

Our Northeast Florida CoC's goal is 100% data accuracy. No policy or provision should be written or propagated the detriment of this goal. While HMIS Lead, CHI agrees and understands this is a culture change from previous systems, only by inputting accurate data can we accomplish the goals of housing and other outcome based measurements.

Access and Expectations and Confidentiality

Your individual usernames and passwords give you access to HMIS. These will be assigned to you and your agency personnel.

As an agency, you agree to maintain the confidentiality of Client information in HMIS in the following manner:

- My agency and its personnel will not allow sharing of usernames and passwords and take all necessary means to maintain security within my agency. I understand any employee found using another's password or log in credentials will be barred from use from the HMIS system.
- My agency and its personnel will not allow use of the browser capacity to remember passwords: my personnel will enter the password each time they log on to HMIS.
- My agency and its personnel will not disclose, view or obtain the database information other than that is necessary to perform my agency's job.
- My agency and its personnel understands that the only individuals who may directly access HMIS Client information are authorized users with a signed user agreement on file, and we will take these steps to prevent casual observers from seeing or hearing HMIS Client information within my agency.
- My agency and its management will encourage agency employees to log off of HMIS before leaving their work area, or make sure that the HMIS database has "timed out" before leaving their work area. I will not allow unattended computers that have HMIS "open and running".
- My agency and its personnel 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.
- My agency and its personnel will keep unauthorized persons not authorized to use HMIS from viewing it within my agency.
- My agency and its personnel 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.
- My Agency and its personnel will properly destroy hard copies (i.e. secure shredding) of HMIS information when they are no longer needed unless they are required to be retained in accordance with applicable law.
- My Agency and its personnel will not discuss HMIS confidential Client information with staff, Clients, or Client family members in a public area.
- My Agency and its personnel will not leave messages on answering machines or voicemail systems that contain HMIS confidential Client information.
- My Agency and its personnel will keep speaker volumes low so that HMIS confidential information left by callers is not overheard by the public or unauthorized persons.
- As the agency representative, 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 agency's access to HMIS may be terminated and I may be subject to further disciplinary action as defined in the Lead Agency's personnel policy.
- If I notice or suspect any security breach, I will notify the HMIS Administrator within 24 hours.
- I give HMIS Lead, CHI and its employees, delegates, assigns, or contractor's access to the data entered by my agency on behalf of our Clients for the purposes of administration, backup, security, necessary reporting, transition, training and any other needs as defined by funders or grantors to meet grant agreement conditions.

- You agree that failure to provide access to all documentation including financial, contractual, and other data necessary to accomplish monitoring as described above could result in your agency being denied access to the system as well as having your HUD grant re-captured.

Agency Code of Ethics Towards Client Data

- Agencies and their personnel must be prepared to answer Client questions regarding HMIS.
- Agencies and their personnel 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.
- Agencies and their personnel must allow Client to change their information sharing preferences at the Client's request.
- Agencies and their personnel must not decline services to a Client or potential Client if that person refuses to allow sharing of information within HMIS
- Agencies and their personnel 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.
- Agencies and their personnel 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.
- Agencies and their personnel will not use HMIS database for any violation of any law, to defraud any entity or conduct any illegal activity.

Support – Remote Access

I agree, as an authorized representative of my agency, to allow HMIS Lead, CHI and its authorized employees to remotely support my HMIS users through a program called LogMeIn Rescue. This program will allow HMIS Lead, CHI to remotely log in, control, and manipulate an HMIS User's computer. LogMeIn Rescue provides SSL encryption security for the connection. HMIS Lead, CHI will only use this connection when authorized by you signing this agreement and your user requesting such assistance. HMIS Lead, CHI will use this connection to train, correct, or configure HMIS and HMIS data only. HMIS Lead, CHI will never use this service for any other purpose and the User from your agency may disconnect this temporary connection at any time. Users from your agency are encouraged to minimize windows containing any personal or confidential agency information before contact HMIS Lead, CHI for support via LogMeIn Rescue.

Support – Data Accuracy and Verification

I, or a designated employee, agree to verify data reports as provided to my agency by HMIS Lead, CHI. My agency is ultimately responsible for correcting errors within data. HMIS Lead, CHI, and the administrative users in my agency has access to run APR, AHAR, or other data reports and will routinely verify data. HMIS Lead, CHI will, from time to time, send data reports to my agency for verification. I, or a designated employee will work with agency staff and HMIS Lead, CHI staff to correct any data errors.

Client Data

Upon Client written request, agency and its personnel 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. Agencies and their personnel 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: HMIS Lead, CHI 660 Park Street Jacksonville, FL 32204. The Northeast Florida CoC will bring your complaint to the HMIS Lead, Data Quality and Performance Standards, which will attempt a voluntary resolution of the complaint.

Renewability

Agreements relative to HMIS will be renewable each year contingent upon the agency completing any required recertification requirements. The agreement requires that your agency is a member in good standing of the Northeast Florida CoC with all member fees paid. This Agreement may be terminated by Agency or HMIS Lead, CHI (due to but not limited to termination of employment, security violation, etc.). If this Agreement is terminated, the agency and its users will no longer have access to HMIS.

Additional Guidance on Managing the HMIS within Your Agency

This additional guidance provides additional guidance for managing HMIS within each partner agency and addressing the roles and responsibilities of partner agencies within the HMIS network.

Partner Agency

Partner Agency is ultimately responsible for ensuring all users within the agency abide by all policies stated in this agreement.
Agrees to:

- Take full responsibility for data entered and ensuring 100% accuracy of that data and for all users entering data within their agency
- Support the culture of entering data at Client contact.
- Have active users attend update trainings and stay current with the HMIS Policies & Procedures.
- Have a designated user or trainer communicate updated HMIS information to all staff and volunteer users at their agency and have this person be a “train the trainer” resource for your agency.
- Select an executive level representative to attend 100% of the HMIS Lead, CHI Executive Committee meetings.
- Be responsible for maintaining all records and files for 7 years after last update.
- Be responsible for archiving or properly disposing (according to HMIS/HUD and agency policy) of aging file records (anything over 7 years).
- Be responsible for system cleansing when decommissioning computers that have accessed HMIS.
- Be responsible for prohibiting the transfer of data to external media (such as: cd, thumb drive, external hard drive, etc.).
- Notify the HMIS Administrator within 24 hours in the event of a breach of system security or Client confidentiality.
- Complete the technology profile form (Executive/IT)
- Complete the Agency Profile form (Executive)
- Provide HMIS System Administrator with a copy of the agency’s policies and procedures to protect hard copy PPI information generated.

Due to the "live" aspect of the system, partner agencies must agree to consistently (within 24 hours of Client interaction) enter information into the HMIS database and shall strive for real-time, or close to real-time data entry.

Any Agency found to have had breaches of system security and/or Client confidentiality shall enter a period of probation, during which technical assistance shall be provided to help the Agency prevent further breaches. Probation shall remain in effect until the HMIS System Administrator has evaluated the Agency's security and confidentiality measures and found them compliant with the policies stated in this Agreement and the Agency Agreement. Subsequent violations of system security may result in suspension from the system. The HMIS Administrator can be reached at HMIS@ChangingHomelessness.org.

Agency's Responsibilities

Responsible for defining the necessary data elements as determined by their funder(s) for their particular program(s) and communicating that information to HMIS Lead, CHI .
Agrees to:

- Designate the Agency Administrator for their program
- Assign and register Basic Users
- Notify HMIS Lead, CHI of any reporting program change as soon as reasonably possible, but within 30 days
- Notify HMIS Lead, CHI of any bed inventory change as soon as reasonably possible, but within 30 days
- Notify HMIS Lead, CHI of system use for non-homeless Clients
- Work with HMIS Lead, CHI to determine program specific data elements
- Maintain data quality at satisfactory level (99%) Universal/Program
- Maintain bed lists (including actual bed count and Clients in beds)
- Notify HMIS Lead, CHI IMMEDIATELY (before end of same day) when a user is terminated or willingly leaves their position or takes a leave of absence (including maternity leave). If agency has an Agency Administrator in place, Agency Administrator is responsible for notifying HMIS Lead, CHI .
- Submit special projects in writing
- Review agency technology for compliance – ensuring they meet HUD HMIS standards
- Notify the HMIS Lead, CHI when program is not compliant with standards
- Notify HMIS Lead, CHI of APR due dates (if applicable)
- Initiate APR assistance (if applicable)
- Generate APR periodically and verify information
- Sign off and being compliant with the HMIS Lead, CHI Privacy Notice
- Adhere to the Program Compliance Checklist v 1.0, annually
- HMIS Readiness Profile for each program
- Act as initial HMIS contact for HMIS Lead, CHI
- Document HMIS issues and escalate issues to System Administrator when applicable
- Be knowledgeable of basic ClientTrack workflow flow
- Update agency's Newflash within the HMIS system
- Generate monthly Bed list Reports (if applicable)
- Comprehend monthly reports (including data quality) for data cleanup
- Initiate data cleanup with appropriate agency staff
- Notify HMIS Lead, CHI of data issues associated with monthly reports
- Notify HMIS Lead, CHI when an employee leaves the agency (termination or willingly).

- Work with agency/program data entry staff to address data entry/data security issues
- Enforce data quality and completeness as determined by funding sources
- Responsible for co-administering Provider and Program set-up with HMIS Lead, CHI
- Responsible for co-administering and maintaining Bedlist(s)
- Maintain, review, administer Provider and Program security
- Run outstanding referral report daily

Privacy and Practices HMIS

1. This notice describes the privacy policy and practices of Changing Homelessness, Inc, specifically in regard to the Homeless Management Information Network program. Our mailing address is: 660 Park Street, Jacksonville, FL 32204.
2. The policy and practices in this notice cover the processing of protected personal information for Clients participating in the Homeless Management Information Network for Northeast Florida.
3. Protected Personal information (PPI or PMI) 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.
7. We give a written copy of this privacy notice to any individual who asks.

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 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 (identify)
   c. Government agencies (identify)
   d. Telephone directories and other published sources

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

   "We collect personal information only when appropriate. We may use or disclose your information to organizations that may 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 this 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."

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 We share Client records with other organizations that may have separate privacy policies and that may allow different uses and disclosures of the information.
   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.

k. to allow for the checking of our records against other CoCs funded through the same funding source to determine Clients' eligibility for additional services.

2. Before we make any use or disclosure of your personal information that is not described here, we seek the Client's consent first. This could include communication through email, a phone call, a meeting and written approval.

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, ask any staff member for access.
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.

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 intend for all data to be 100% accurate, entered timely, and verified by alternative sources where possible.
3. 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.
4. We may keep information for a longer period if required to do so by statute, regulation, contract, or other requirement.

Complaints and Accountability

We accept and consider questions or complaints about our privacy and security policies and practices. Complaints must be submitted in writing to this Agency and to:

Changing Homelessness
HMIS Administrator
660 Park Street
Jacksonville, FL 32204

The Administrator will attempt to resolve your complaint. Should further review be required your complaint will be escalated to the HMIS Lead, CHI and the Data Quality and Performance Standards Committee to determine a voluntary resolution of the complaint. Resolution of the complaint will be provided in writing to the agency and the individual filing the complaint. This Agency and HMIS Lead, CHI is prohibited from retaliating against you for filing a complaint.

1. 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.

Privacy Notice Change History

1. Version 1.0. June 1, 2012. Initial Policy
2. Version 2.0 October 1, 2014 Updated HMIS Data Standards
3. Version 3.0 October 1, 2015 Updated HMIS Data Standards
4. Version 4.0 March 4, 2020 Updated HMIS Data Standards

Agency Compliance Checklist

Agency:

Requirement	Description	Response	Assessment	Status
Privacy: Posted Notice	Does the agency have the privacy notice (short version) posted at the point of intake?	Yes	Location(s)_____ -Includes purpose for data collection □Yes □ No -Copy available: □ Yes □ No	Agency Initial ____ Date _____ HMIS Initial _____ Date _____
		No	No posted sign at intake desk	
Privacy: Notice Available	Does the agency have the privacy notice (full version) form available for the Client?	Yes	-Includes purpose for data collection □Yes □ No -Copy Available □Yes □ No	Agency Initial ____ Date _____ HMIS Initial _____ Date _____
		No		
User Authentication	Does the agency abide by the HMIS policies for unique user names & passwords? *8-16 characters, at least 2 numeric values, not a word found in the dictionary or a name*	Yes	Agency abides by HMIS policy □Yes □ No Users are aware not to share username & passwords □Yes □ No Users are aware not to keep username & password in public location □Yes □ No	Agency Initial ____ Date _____ HMIS Initial _____ Date _____
		No	Agency does not abide by HMIS user authentication policy.	
Virus Protection	Do all computers have virus protection with automatic update?	Yes	Spot check several computers Virus software & version_____ Auto-update turned on □Yes □ No Date last updated: __/__/__ Person responsible for updating: _____	Agency Initial ____ Date _____ HMIS Initial _____ Date _____
		No	No virus protection installed	

Agency:

Requirement	Description	Response	Assessment	Status
Firewall	Does the agency have a firewall on the network &/or workstation(s) to protect the HMIS systems from outside intrusion?	Yes	Single Computer Agencies: -Individual workstation □Yes □ No Version_____ Networked (Multiple Computer) Agencies: -Network Firewall □Yes □ No Version_____	Agency Initial ____ Date _____ HMIS Initial _____ Date _____
		No	Individual workstation or network firewall not active.	
Workstation Authentication	Does the HMIS utilize certificates, filter by IP or another model to control access to designated workstations?	Yes	Controls Active	Agency Initial ____ Date _____ HMIS Initial _____ Date _____
		No	Not active.	
Physical Access	Are all HMIS workstations in secure locations or are they manned at all times if they are in publicly accessible locations?	Yes	All workstations are in secure locations (i.e. – locked offices) □Yes □ No All workstations are manned at all times □Yes □ No All workstations have password protected workstations □Yes □ No	Agency Initial ____ Date _____ HMIS Initial _____ Date _____
		No	Not all workstations are manned at all times or in secure locations.	

PPI Storage	Does the agency dispose of or remove identifiers from a Client record after a specified period of time? *Minimum Standard: 7 yrs after PPI was last changed if record is not in current use*	Yes	Has procedure? □Yes □ No Describe procedure: _____ _____	Agency Initial ____ Date _____ HMIS Initial _____ Date _____
		No	No procedure available.	

Agency:

Requirement	Description	Response	Assessment	Status
Data Disposal	Does the agency have the policies & procedures to dispose of hard copy PPI or electronic media? *Personal Protected Information (i.e.- name, social security number, date of birth)*	Yes	The agency shreds all hardcopy PPI before disposal □Yes □ No The agency reformats before disposal: -Disks □Yes □ No -CD's □Yes □ No -Computer Hard-drives □Yes □ No -Other Media (jump drives, tapes, etc.) □Yes □ No	Agency Initial ____ Date _____ HMIS Initial _____ Date _____
		No	The agency does not have policies & procedures for data disposal.	

Hard Copy Data	Does the agency have procedures in place to protect hard copy PPI information generated from or for the HMIS?	Yes	Has procedure that includes: 1. Security of hard copy files -Locked drawer/file cabinet □Yes □ No -Locked office □Yes □ No 2. Procedure for Client data generated from HMIS -Printed screen shots □Yes □ No -HMIS Client reports □Yes □ No -Downloaded data (i.e. – to excel) □Yes □ No Copy of policy/procedure available □Yes □ No Agency staff have received training on hard copy data protections □Yes □ No	Agency Initial ____ Date _____ HMIS Initial _____ Date _____
		No	No procedure available.	

Note

Notes:

Agency:

Requirement	Description	Response	Assessment	Status
File Review	Does the agency maintain physical files per HMIS standards?	Yes No	□ Release of Information □ Uses & Disclosures	Agency Initial ____ Date _____ HMIS Initial _____ Date _____

Notes:

USER AGENCY CERTIFICATION

As an authorized representative of my agency, I certify to the HMIS Administrator that employee(s) accessing the HMIS system has a current background check (within the last five (5) years) on file that complies with agency 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.

Agency Agreement and Understanding:

Our agency agrees to be bound by this agreement between HMIS Lead, CHI (HMIS Lead) and our agency.

We agree that we will work toward compliance and that we will seek out guidance, help and assistance from our HMIS Lead when needed.

We also agree that the intention of this document is to provide the best possible outcomes for the Clients who reside in our service area. If we, as a participating agency, are not meeting the needs of our Clients, we agree that the HMIS Lead my, at its sole discretion, inactivate our use of this system and may place our agency on corrective agency up to and including defunding our COC Program in part of whole.

Entire Agreement:

This is the entire agreement between HMIS Lead, CHI and our agency. If any part of the agreement is found to be in violation of law, the remainder of the agreement will remain in force.

Modifications to this agreement can only be made in writing and no verbal consent can be given to waive any of the provisions of this agreement.

Signed,

_____	_____	_____
Authorized Agency Signature	Print Name	Date

Approved:

_____	_____	_____
HMIS Lead, CHI System Administrator	Print Name	Date