



HMIS Document

FL-507 CONTINUUM OF CARE HMIS PRIVACY PLAN

Homeless Services Network of Central Florida
142 E. Jackson St.
Orlando, FL 32801
Phone: (407) 893-0133
Fax: (407) 893-5299
www.hsncfl.org

Table of Contents

1. Purpose	3
2. Scope	3
3. Acronyms & Definitions	4
4. Baseline Privacy Policy	5
HMIS Privacy Notice Posting	5
Collection of Personal Information	5
Use and Disclosure of Personal Information	5
Inspection and Correction of Personal Information	7
Limits on Collection of Personal Information	7
Limits on Partner Agency Use of HMIS Client Information	8
Data Release Criteria	8
Data Release Process	8
Complaints and Accountability	9
Use of a comparable database by Victim Service Providers	9
User Conflict of Interest	9
Data Retention	9
5. Appendices	10
Document History	10

1. Purpose

The purpose of this document is to provide details about the Central Florida CoC HMIS Privacy Plan. This is a standalone document that refers to other Central Florida CoC HMIS documents, including the HMIS Policies & Procedures manual.

This document describes standards for the privacy of personal information collected and stored in the Central Florida Homeless Management Information System (HMIS), as well as personal information collected for the purposes of the Coordinated Entry System for the Central Florida Continuum of Care (CoC).

This plan seeks to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data.

2. Scope

This document applies to all active HMIS Users working with FL-507 projects that participate in HMIS. All HMIS Users with access to HMIS Data must follow the guidelines outlined in this plan.

3. Acronyms & Definitions

This list includes a list of terms that will be used throughout this document and by the HMIS staff.

HUD	Acronym used to refer to the Department of Housing and Urban Development
HSN	Acronym for Homeless Services Network
HMIS	Acronym for Homeless Management Information System
HIPAA.....	Acronym for Health Information Portability and Accountability Act
CoC	Acronym for Continuum of Care
Agency Liaison (AL)	A person designated by a CoC Member Agency who acts as a liaison and contact person to the HMIS staff.
System Administrators	Staff at the HMIS Lead Agency who are responsible for overseeing HMIS users and system use/access within the Central Florida Continuum of Care. The System Administrators allow user HMIS access, provide end user training, ensure user compliance with HMIS policies and procedures, and make policy recommendations to the Central Florida Continuum of Care HMIS Advisory Committee.
Partner Agency.....	An agency who has signed all HMIS agreements and who is actively entering data into the HMIS system
MOU	Acronym for Memorandum of Understanding
ROI.....	Acronym used to refer to a Release of Information
HMIS User	Any system user who has an active HMIS software license. This can include Agency Liaisons.
VI-SPDAT.....	An acronym used to refer to the Vulnerability Index – Service Prioritization Assistance Tool. This is the standardized assessment chosen by the CoC to identify individual clients with the highest needs for housing.
VI-FSPDAT	An acronym used to refer to the Vulnerability Index – Family Service Prioritization Assistance Tool. This is the standardized assessment chosen by the CoC to identify client families with the highest needs for housing.
Open Data.....	This is data that does not contain personal identifying information and visible by all providers using HMIS.
Closed Data.....	This is data entered by one provider that is not visible to other providers using HMIS.
Aggregated Public Data	De-identified data available to the public.
Unpublished Restricted Access Data	Information scheduled, but not yet approved, for publication

4. Baseline Privacy Policy

HMIS Privacy Notice Posting

A privacy notice is required to be posted within clear view of clients at each Partner Agency. It identifies privacy controls and restrictions on the use of data. It also emphasizes the clients' right to receive services even if they choose not to participate in HMIS. The HMIS Privacy Notice is available from HSN upon request. This policy may be amended at any time, and amendments can impact data collected and entered in HMIS prior to the date of the amendment.

Collection of Personal Information

Personal information will be collected for HMIS only when it is needed to provide services for another specific purpose of the agency where a client is receiving services, or when it is required by law. The purposes for collecting personal information may include:

- To provide or coordinate services for clients
- To find programs that may provide additional client assistance
- To comply with government and grant reporting obligations
- To assess the state of homelessness in the community, and to assess the condition and availability of affordable housing to better target services and resources

Only lawful and fair means are used to collect personal information.

Personal information is collected with the knowledge and consent of clients. It is assumed that clients consent to the collection of their personal information when they seek assistance from an agency using HMIS and provide the agency with their personal information.

Personal information may also be collected from:

- Additional individuals seeking services with a client
- Other private organizations that provide services and participate in HMIS
- Government agencies including, but not limited to HUD, DCF, and the Social Security Administration
- Telephone directories and other published sources

Upon request, clients will be given access to the Use and Disclosure of Personal Information policy found below.

Use and Disclosure of Personal Information

This policy explains why an agency collects personal information from clients. Personal information may be used or disclosed for activities described below. Client consent to the use or disclosure of personal information for the purposes described below, and for reasons that are compatible with purposes described below but not listed, is assumed. Clients must give consent before their personal information is used or disclosed for any purpose not described here.

1) Personal information may be used or disclosed for the following purposes:

- To provide or coordinate services to individuals. Client records are shared with other organizations that may have separate privacy policies and that may allow different uses and disclosures of the information. If clients access services at one of these other organizations, they will be notified of the agency's privacy and sharing policy. These organizations include, but are not limited to, other agencies and programs participating in the CoC's HMIS. A current list of Partner Agencies can be found at <https://www.hmiscfl.org/partnering-agencies/>.
- For functions related to payment or reimbursement for services

- To carry out administrative functions such as legal audits, personnel, oversight, and management functions.
- For research and statistical purposes.
- For academic research conducted by an individual or institution that has a formal relationship with the CoC, based on recommendations from the HMIS Advisory Committee. The research must be conducted by an individual employed by or affiliated with the academic institution. All research projects must be conducted under a written research agreement approved in writing by the Chief Executive Officer or the Chief Operating Officer of the CoC Lead Agency.

The written research agreement must:

- Establish the rules and limitations for processing personal information and providing security for personal information in the course of the research.
 - Provide for the return or proper disposal of all personal information at the conclusion of the research.
 - Restrict additional use or disclosure of personal information, except where required by law.
 - Require that the recipient of the personal information formally agree to comply with all terms and conditions of the written research agreement, and
 - Cannot be a substitute for approval of the research project by an Institutional Review Board, Privacy Board or other applicable human subjects' protection institution if appropriate.
- When required by law. Personal information will be released to the extent that use or disclosure complies with the requirements of the law.
 - To avert a serious threat to health or safety if:
 - 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.
 - The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
 - To report to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence, information about an individual reasonably believed to be a victim of abuse, neglect or domestic violence. When the personal information of a victim of abuse, neglect or domestic violence is disclosed, the individual whose information has been released will promptly be informed, except if:
 - it is believed that informing the individual would place the individual at risk of serious harm, or
 - a personal representative (such as a family member or friend) who is responsible for the abuse, neglect or other injury is the individual who would be informed, and it is believed that informing the personal representative would not be in the best interest of the individual as determined in the exercise of professional judgment.
- 2) For a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
- In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer or a grand jury subpoena. The HMIS Lead Agency must be notified within twenty-four (24) hours of receiving this court ordered disclosure.

If the law enforcement official makes a written request for personal information, the written request must meet the following requirements:

- Is signed by a supervisory official of the law enforcement agency seeking the personal information.
- States that the information is relevant and material to a legitimate law enforcement investigation.
- Identifies the personal information sought.
- Is specific and limited in scope to the purpose for which the information is sought.
- The HMIS Lead Agency is notified within twenty-four (24) hours regarding this written request for personal information.
- If it is believed that the personal information constitutes evidence of criminal conduct that occurred at the agency where the client receives services.
- If the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to a 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 (threats against the President and others), and 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.
- For law enforcement or another public official authorized to receive a client's personal information to conduct an immediate enforcement activity that depends upon the disclosure. Personal information may be disclosed when a client is incapacitated and unable to agree to the disclosure if waiting until the individual is able to agree to the disclosure would materially and adversely affect the enforcement activity. In this case, the disclosure will only be made if it is not intended to be used against the individual.
- To comply with government reporting obligations for HMIS and for oversight of compliance with HMIS requirements.

Inspection and Correction of Personal Information

Clients may inspect and receive a copy of their personal information maintained in HMIS. The agency where the client receives services will offer to explain any information that a client may not understand.

If the information listed in HMIS is believed to be inaccurate or incomplete, a client may submit a verbal or written request to have his/her information corrected. The client must provide proof that the data is inaccurate. Inaccurate or incomplete data may be deleted, or marked as inaccurate or incomplete, and supplemented with additional information.

A request to inspect or copy one's personal information may be denied if:

- The information was compiled in reasonable anticipation of litigation or comparable proceedings.
- The information was obtained under a promise of confidentiality and if the disclosure would reveal the source of the information.
- The life or physical safety of any individual would be reasonably endangered by disclosure of the personal information.
- If a request for inspection access or personal information correction is denied, the agency where the client receives services will explain the reason for the denial. The client's request and the reason for the denial will be included in the client's record.
- Requests for inspection access or personal information correction may be denied if they are made in a repeated and/or harassing manner.

Limits on Collection of Personal Information

Only personal information relevant for the purpose(s) for which it will be used will be collected. Personal information must be accurate and complete.

Client files not used in seven years may be made inactive in HMIS. The HMIS Lead Agency will check with agencies before making client files inactive. Personal information may be retained for a longer period if required by statute, regulation, contract or another obligation.

Limits on Partner Agency Use of HMIS Client Information

The Central Florida CoC HMIS is an open data system. This system allows Partner Agencies to share client information in order to coordinate services for clients. However, Partner Agencies may not limit client service or refuse to provide service in a way that discriminates against clients based on information the Partner Agency obtained from HMIS. Partner Agencies may not penalize a client based on historical data contained in HMIS.

Data Release Criteria

Data will be released only in aggregate, or in anonymous client-level data formats, for any purpose beyond those specified in the Use and Disclosure of Personal Information section of this manual, such that the identity of any individual or household cannot be determined. Parameters of the release of aggregate data (i.e., where the data comes from, what it includes and what it does not include) will be presented to each requestor of aggregate data.

Data Release Process

Individual funded programs may use data for internal reporting, program management, and performance measurement on an as needed basis. Beyond individual agency reports on its funded programs, the CoC must approve all data for public classification and release within their coverage area.

All open data will be handled according to the following classifications - Public Data, Internal Data, and Restricted Data - and must be handled according to the following procedures.

Principles for Release of Data

- Only de-identified aggregated data will be released except as specified below.
- No identified client data may be released without informed consent unless otherwise specified by Florida State and Federal confidentiality laws. All requests for such information must be addressed to the HMIS Lead Agency.
- Program specific information used for annual grant program reports and program specific information included in grant applications is classified as public information. No other program specific information will be released without client consent.
- There will be full access to aggregate data included in published reports.
- Reports of aggregate data may be made directly available to the public.
- The parameters of the aggregated data, that is, where the data comes from and what it includes will be presented with each report.
- Data will be mined for agencies requesting reports on a case-by-case basis.
- Requests must be written with a description of specific data to be included and for what duration of time. Requests are to be submitted 30 days prior to the date the report is needed. Exceptions to the 30-day notice may be made.
- The HMIS Lead Agency reserves the right to deny any request for aggregated data, except in circumstances and under conditions approved by the CoC.

Release of Data for Grant Funders

Entities providing funding to agencies or programs required to use HMIS will not have automatic access to HMIS. Access to HMIS will only be granted by the HMIS Lead Agency when there is a voluntary, written agreement in place between the funding entity and the

agency or program. Funding for any agency or program using HMIS cannot be contingent upon establishing a voluntary written agreement allowing the funder access to HMIS.

Complaints and Accountability

Client questions or complaints about the privacy policies and practices may be submitted to the agency where the client receives services. Complaints specific to HMIS must be submitted to the HMIS agency liaison and program director. If no resolution can be found, the complaint will be forwarded to the System Administrators and the agency's executive director. If there is no resolution, the HMIS Advisory Committee will oversee final arbitration. All other complaints will follow the agency's grievance.

All HMIS users (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy notice. Users must receive and acknowledge receipt of a copy of this privacy notice.

Use of a comparable database by Victim Service Providers

Victim service providers, private nonprofit agencies whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking, must not directly enter or provide data into HMIS if they are legally prohibited from participating in HMIS. Victim service providers that are recipients of funds requiring participation in HMIS, but are prohibited from entering data in HMIS, must use a comparable database to enter client information. A comparable database is a database that can be used to collect client-level data over time and generate unduplicated aggregated reports based on the client information entered into the database. The reports generated by a comparable database must be accurate and provide the same information as the reports generated by HMIS.

User Conflict of Interest

Users who are also clients with files in HMIS are prohibited from entering or editing information in their own file. All users are also prohibited from entering or editing information in files of immediate family members. All users must sign the HMIS End User Agreement, which includes a statement describing this limitation, and report any potential conflict of interest to their Agency liaison. The System Administrator may run the audit trail report to determine if there has been a violation of the conflict of interest agreement.

Data Retention

Personal information that has not been accessed within the seven year period following the creation or last edit dates are subject to deletion from HMIS. Personal information may be kept for a longer period if required by statute, regulation, contract, or other similar requirement.

5. Appendices

Document History

Date of Revision	Document Version #	Revision Notes
2018/03/27	1.0	First Release of Document
2018/03/30	1.1	Updated Style formatting of document
2022/04/12	1.2	Updated to improve ROI and client consent policies
2022/05/17	1.3	Separate Privacy and Security Plan into separate documents
2023/01/11	1.4	Updated to include HUD TA recommendations