HMIS Document

FL-507 CONTINUUM OF CARE

HMIS SECURITY 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

The purpose of this document is to provide details about the Central Florida CoC HMIS Security 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 security 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. Introduction to HMIS Security

The Department of Housing and Urban Development (HUD) requires implementation of security standards. Security standards are directed to ensure the confidentiality, integrity, and availability of all HMIS information; protect against any reasonably anticipated threats or hazards to security; and ensure compliance by end users. Written policies and procedures must comply with all applicable federal law and regulations, and applicable state or local governmental requirements.

1. All administrative, physical, and technical safeguards shall be implemented within six months of initial approval of this security plan.
2. If one or more of these standards cannot be implemented, the Partner Agency and/or HMIS Lead Agency shall justify the implementation delay and produce a plan of action.

5. Administrative Safeguards

The HMIS Advisory Committee will set forth the administrative actions, policies, and procedures required to manage the selection, development, implementation, and maintenance of security measures to protect HMIS information.

HMIS Lead Agency

The HMIS Lead Agency shall uphold the following duties/responsibilities:

- Adherence to the Security Plan.
- Review the Security Plan annually and at the time of any change to the security management process of any HMIS data or technical requirements issued by HUD. In the event that changes are required to the HMIS Security Plan, the HMIS Lead Agency will work with the HMIS Advisory Committee for review, modification, and approval.
- Respond to any security questions, requests, or security breaches to the HMIS Advisory Committee and communication of security-related HMIS information to Partner Agencies within the CoC.

Partner Agency

Each Partner Agency is responsible to uphold the following duties/responsibilities:

- Adherence to the Security Plan.
- Communicate any security questions, requests, or security breaches to the HMIS Lead Agency, and ensure that security-related HMIS information is relayed from the HMIS Advisory Committee to the Partner Agency's end users.
- Participate in security training offered by the HMIS Lead Agency.

Security Awareness training and follow-up

HMIS System Administrators shall ensure that all users receive security awareness training prior to being given access to the HMIS. The HMIS Lead Agency can conduct this training either in person or via on-line module. As part of this security training, the HMIS Policies & Procedures document will be reviewed. The End User License Agreement for each End User will include language that certifies the End User has received this Security Awareness training prior to being issued a license. The HMIS Lead Agency will implement monitoring procedures for all end users in the CoC to ensure they are maintaining Security Training annually.

Procedure for Reporting Security Incidents

Users and Agency liaisons must report all unlawful access of HMIS and unlawful attempted access of HMIS. This includes theft of usernames and passwords. Security incidents must be reported to a HMIS System Administrator. The HMIS System Administrators will use available reports and system tools to determine the extent of the breach of security.

The HMIS Lead Agency must abide by the following policy and chain of communication for reporting and responding to security incidents.

Security Incidents

All HMIS end users are obligated to report to their agency's appointed HMIS Agency liaison and/or direct service supervisor of suspected instances of noncompliance with policies and procedures that may leave HMIS data vulnerable to intrusion. Each Partner Agency is responsible for reporting any security incidents involving the real or potential intrusion of the

HMIS system. The HMIS Lead Agency is responsible for reporting any security incidents involving the real or potential intrusion of the HMIS system to the other member agencies of the CoC via HMIS Advisory Committee communication channels.

Reporting Threshold

HMIS End Users must report any incident in which unauthorized use or disclosure of Personal Identifiable Information (PII) has occurred and any incident in which PII may have been used in a manner inconsistent with the Central Florida HMIS Security Plan. Security breaches that have the possibility to impact the HMIS system must also be reported to the HMIS System Administrators.

Audit Controls

The HMIS software maintains an accessible audit trail that allow any System Administrator to monitor user activity and examine data access for specified users.

Violation of Security Procedures

All potential violations of any security protocols will be investigated and any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to: a formal letter of reprimand, suspension of system privileges, revocation of system privileges and criminal prosecution.

If possible, all confirmed security violations will be communicated in writing by the HMIS Lead Agency to the affected client within 14 days, unless the client cannot be located. If the client cannot be located, a written description of the violation and efforts to locate the client will be prepared by the HMIS System Administrators and placed in the client’s file at the Agency that originated the client’s record.

Any agency that is found to have consistently and/or flagrantly violated security procedures may have their access privileges suspended or revoked. All sanctions are imposed by the HMIS Lead Agency, and shall be reported to the appropriate funder. All sanctions may be appealed to the HMIS Advisory Committee.

Users who are Clients or have Relatives in HMIS

In order to prevent users from editing their own file or files of immediate family members or friends/acquaintances, all users agree to a conflict of interest statement that is part of the HMIS User Agreement. Users must disclose any potential conflict of interest to their Agency Liaison. Users will be prohibited from making changes to the information in their own file or the files of their immediate family members. If a user is suspected of violating this agreement, the System Administrators will run an audit report to determine if there was an infraction. Infractions will be reported to the Agency Liaison and the end user’s access will be suspended. Disciplinary actions are the responsibility of the end user agency. Access will only be restored at the request of the agency Executive Director or Chief Executive Officer, as applicable.

Security of Content in Reports

General extracts (Excel worksheets, CSV, or any other format) of data from HMIS and any reports generated by any Partner Agency may be made public and/or shared with other agencies and organizations provided the report contains no client identifiers. Any report that includes a client’s name, date of birth, and/or social security number or any combination of data that, taken together, could constitute Personally Identifying Information may not be shared outside of your agency.

Database Integrity

All users must sign and abide by User Confidentiality Standards as outlined in the End User License Agreement. Each Partner Agency HMIS end user is responsible for ensuring compliance with HMIS security standards. Confidentiality of client level information is critical within all agencies, and every effort must be taken to maintain confidentiality and integrity of this information. Any security incidents must be reported immediately to the Partner Agency end user's supervisor and the HMIS Lead Agency, so that appropriate action can be taken. Failure to report security incidents will result in the immediate termination of the end user's access to HMIS.

- A Partner Agency's or an End User's HMIS access may be suspended or revoked for suspected or actual violation of the security protocols.
- All potential violations of any security protocols will be investigated.
- Any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to; a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of employment and criminal prosecution.
- Any Partner Agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.
- The HMIS Lead Agency will impose all sanctions.
- All sanctions can be appealed to the HMIS Advisory Committee.
- Each agency will submit to a security audit and data entry/collection audit to ensure the agency is following HMIS Policies and Procedures and HMIS Security procedures to protect client confidentiality. Audits also include Releases of Information (ROI) and posting of the HMIS privacy statement.

Confidentiality and Security

The importance of the integrity and security of HMIS cannot be overstated. Given this importance, HMIS must be administered and operated under high standards of data quality and security. The HMIS Lead Agency and Participating Agencies are jointly responsible for ensuring that HMIS data processing capabilities, including the collection, maintenance, use, disclosure, transmission and destruction of data, comply with the HMIS privacy, security and confidentiality policies and procedures. When a privacy or security standard conflicts with other Federal, state and local laws to which the Participating Agency must adhere, the Participating Agency must contact the HMIS Lead Agency to collaboratively update the applicable policies for the Participating Agency to accurately reflect the additional protections.

Data Assessments and Access

All HMIS data will be handled according to the following major classifications: Shared or Closed Data. HMIS staff will assess all data, and implement appropriate controls to ensure that data classified as shared or closed are handled as defined below.

Shared Data

Shared data is unrestricted information that has been entered by one provider and is visible to other providers using HMIS. The CoC's HMIS operates as an open system that defaults to allow shared data. Providers have the option of changing their program settings to keep client data closed.

Closed Data

Information entered by one provider that is not visible to other providers using HMIS. Programs serving particularly vulnerable populations (e.g. persons with disabilities, victims fleeing domestic violence, or individuals with HIV/AIDS), if entering client data at all, may do so in a manner that does not share such information with other Participating Agencies.

Procedures for Transmission and Storage of Open or Confidential Data

- Open Data: This is data that does not contain personal identifying information. The data must be handled discreetly, unless it is further classified as Public Data. The data must be stored out of sight, and may be transmitted via internal or first-class mail until it is considered public data.
- Confidential Data at the Agency Level: Confidential data contains personal identifying information. Each agency shall develop rules governing the access of confidential data in HMIS to ensure that those staff needing confidential data access will have access, and access is otherwise restricted. The agency rules shall also cover the destruction of paper and electronic data in a manner that will ensure that privacy is maintained and that proper controls are in place for any hard copy and electronic data that is based on HMIS data.

  Whenever confidential data is accessed:
  - Hard copies shall be shredded when disposal is appropriate. Hard copies shall be stored in a secure environment that is inaccessible to the general public or staff not requiring access.
  - Hard copies shall not be left out in the open or unattended.
  - Electronic copies shall be stored only where the employee can access the data.
  - Electronic copies shall be stored where a password is required to access the data if on shared server space.

Procedures for Transmission and Storage of Public Data

All public data must be classified as aggregated public or unpublished restricted access data.

- Aggregated Public Data: Security controls are not required.
- Unpublished Restricted Access Data:
  - Draft or Fragmented Data – Accessible only to authorized HMIS staff and agency personnel. Requires auditing of access and must be stored in a secure out-of-sight location. Data can be transmitted via e-mail, internal departmental or first class mail. If mailed, data must be labeled confidential.
  - Confidential Data: Requires encryption at all times. Must be magnetically overwritten and destroyed. Hard copies of data must be stored in an out-of-sight secure location.

6. Technical Safeguards

Desktop/System Security

Each Partner Agency must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a Partner Agency's networks, desktops, laptops, mini-computers, mobile devices, mainframes and servers. The software used for HMIS is accessed over the Internet; a broadband Internet connection is necessary. To maintain security, we recommend devices used to access HMIS be current with all required patches and operating system software updates installed.

User Authentication - Passwords

The HMIS software requires a user authentication system consisting of a username and a password. Every licensed end user is required to have a unique User ID and password, and account sharing is not allowed under any circumstances. Passwords must be at least eight characters long and meet reasonable industry standard requirements.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Information specifically pertaining to end user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual end users must not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

Creation: Passwords are automatically generated from the system when a user is created. The System Administrator will communicate the system-generated password to the user.

Use: The end user will be required to change the password the first time they log into the system. The password must be at least eight characters and alphanumeric. Passwords must not be able to be effortlessly guessed or found in a dictionary. Passwords are the individual's responsibility and end users cannot share passwords. End users may not keep written copies of their password in a publicly accessible location.

Storage: Passwords are to be stored securely and must be inaccessible to other persons. End users are not to electronically store passwords on a computer for easier log on.

Expiration: HMIS passwords expire every ninety days. End users may not use the same password consecutively. Passwords cannot be re-used until six password selections have expired.

Unsuccessful login: If an end user unsuccessfully attempts to log-on six (6) times, the end user account will be locked and access permission will be revoked rendering the end user unable to gain access until the password is reset. If the user has setup an appropriate security question, the user has the ability to reset their own password. If not, requests for password reset must be sent to the HMIS System Administrators by emailing: hmis@hsncfl.org.

Virus Protection

A Partner Agency must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed. A Partner Agency must regularly update virus definitions from the software vendor.

Firewalls

A Partner Agency must protect HMIS systems from malicious intrusion behind a secure firewall and have anti-virus and anti-spyware applications installed. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall as long as the server has a firewall.

If computers are networked with wireless connections, it is recommended that you have up to date and industry standard security and the network is password protected.

7. Physical Safeguards

Physical Access to Systems with Access to HMIS Data

Confidentiality of client-level information is key within all agencies, and every effort must be taken to maintain confidentiality and integrity of this information. All client files, or print-outs of client level information, must be kept in a secure location accessible only to allowed Partner Agency staff. A Partner Agency must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff is not present, steps must be taken to ensure that computers and data are secure and not usable by unauthorized individuals. After 10 minutes or less, workstations must automatically turn on a password protected screen saver when the workstation is temporarily not in use. If staff from a Partner Agency will be gone for an extended period of time, staff must log off the data entry system and shut down the computer or lock the computer in which a password is required for access. Client level information, however, needs to be made available and accessible to Partner Agency HMIS end-users when needed during the course of their work day.

Hard Copy Security

A Partner Agency must secure any paper or other hard copy containing personal protected information that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms. A Partner Agency must supervise at all times any paper or other hard copy generated by or for HMIS that contains PII when the hard copy is in a public area. When Partner Agency staff is not present, the information must be secured in areas that are not publicly accessible.

Hard copies of data stored or intended to be stored in HMIS, regardless of whether the data has yet been entered into HMIS, will be treated in the following manner:

- Records shall be kept in individual locked files or in rooms that are locked when not in use.
- When in use, records shall be maintained in such a manner as to prevent exposure of PII to anyone other than the user directly utilizing the record.
- Employees shall not remove records or other information from their places of business without permission from appropriate supervisory staff unless the employee is performing a function which requires the use of such records outside of the Partner Agency's place of business and where return of the records by the close of business would result in an undue burden on staff.
- When staff remove records from their places of business, the records shall be maintained in a secure location and staff must not re-disclose the PII contained in those records except as permitted by these policies and procedures.
- Faxes, photocopies or other printed documents containing PII shall not be left unattended.
- When faxing PII, the recipients must be called in advance to ensure the fax is properly managed upon receipt.
- When finished faxing, copying or printing, all documents containing PII must be removed from the machines immediately.
- When or if the hard copy of PII information is no longer needed, such as reports printed or any other form of written, typed or printed copies, they must be shredded; these copies may not be disposed of in the garbage.

Contracts and Other Arrangements

- The HMIS Lead Agency shall retain copies of all contracts and agreements executed as part of the administration and management of the HMIS and are required to comply with the requirements of the HMIS security standards.

8. Disaster Recovery

The Disaster Recovery plan for HMIS data is the responsibility of our HMIS Vendor, which hosts and houses the data on remote servers. In the event of disaster, the HMIS Lead Agency and System Administrators will coordinate with our HMIS Vendor to ensure that HMIS is functional and that data is restored as quickly and efficiently as possible. The HMIS Lead Agency will communicate to Partner Agencies when data becomes accessible following a disaster.

Central Florida's HMIS is covered under our HMIS Vendor Disaster Recovery Plan. Due to the nature of technology, unforeseen service outages may occur. In order to assure service reliability, our HMIS Vendor provides the following disaster recovery plan. Plan highlights include:

- HMIS Vendor will delete and remove customer data upon contract termination or upon request from our customers.
- HMIS Vendor maintains backups of client data for disaster recovery and data consistency purposes. Database backups will be purged at customer request or will automatically age out and be removed after 8 weeks.
- HMIS Vendor maintains app consistent server instance backups for the space of 30 days for disaster recovery purposes. These backups will be removed permanently at the end of their 30-day cycle and cannot be purged beforehand but are never accessed except for use in disaster recovery scenarios.
- All client data is kept on a secure network that limits access using the Principle of Least Privilege.
- The secured network is hosted in Azure's cloud solution and access to the network is behind a virtual Private Network (VPN) using Azure Active Directory authentication with multi-factor authentication enabled.
- Customer data kept on the network is secured against anonymous access using Active Directory authentication. Access for viewing or managing the data and is granted using Principle of Least Privilege.
- All data is encrypted in transit using strong cyphers and TLS protocol with 3rd party CA issued certificates from GoDaddy, a highly trusted CA.
- All data is encrypted at rest using Azure disk encryption and platform managed keys.
- HMIS Vendor employees are trained to be sensitive to PII and report any unsecured PII that may be transmitted accidently via corporate communication channels for immediate purge and reporting to the client.
- Transmittal of PII to the client outside of the application at the client's request takes place through highly secured file sharing platforms requiring authenticated access.

Standard Data Recovery

Central Florida's HMIS database is stored online, and is readily accessible approximately twenty four hours a day. Tape backups of the database are kept for approximately one month. Upon recognition of a system failure, HMIS can be copied to a standby server. The database can be restored, and the site recreated within three to four hours if online backups are accessible. As a rule, a tape restoration can be made within six to eight hours. On-site backups are made once daily. A restore of this backup may incur some data loss between when the backup was made and when the system failure occurred.

All major outages are immediately brought to the attention of executive management. Our HMIS Vendor support staff helps manage communication or messaging to the System Administrators as progress is made to address the service outage.

9. 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	Updated to improve disaster recovery information
2022/12/29	1.4	Updated per HUD TA recommendations