FL-507 CONTINUUM OF CARE
HMIS PRIVACY & SECURITY PLAN

Homeless Services Network of Central Florida
4065-D L.B. McLeod Road
Orlando, FL 32811
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 Privacy and Security Plan. This document is a standalone document that refers to other Central Florida CoC HMIS documents, including the HMIS Policies manual.

2. Glossary

This glossary 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 Administrator (AA)	A person designated by a CoC Member Agency Executive Director/Chief Executive Officer 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 ServicePoint license. This can include Agency Administrators.
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

3. Introduction to HMIS Privacy and Security

The Department of Housing and Urban Development (HUD), with the HMIS Interim Rule, 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.

4. 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:

- The HMIS Lead Agency will 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.
- The HMIS Lead Agency must adhere to the Security Plan.
- 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:

- All Partner Agencies within the CoC must adhere to the Security Plan.
- Communication of 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 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 Administrators should report all unlawful access of HMIS and unlawful attempted access of HMIS. This includes theft of usernames and passwords. Security incidents should be reported to a System Administrator. The CoC System Administrator will use the HMIS User Audit Trail Report to determine the extent of the breach of security.

The HMIS Lead Agency should 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 Administrator 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 Privacy and Security Policies. Security breaches that have the possibility to impact the HMIS system must also be reported to the CoC HMIS Lead Agency's System Administrator.

Audit Controls

Mediware Information Systems maintains an accessible audit trail within ServicePoint tools that allow any System or Agency 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 CoC HMIS Lead Agency's System Administrator 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 CoC, and shall be reported to the appropriate funder. All sanctions may be appealed to the HMIS Advisory Committee.

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 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 should be taken to maintain confidentiality and integrity of this information. Any security incidents should 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 ServicePoint.

- 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 HMIS Privacy and 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 should 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.

5. Baseline Privacy Policy

HMIS Privacy Notice Posting

A privacy notice is required to be posted within each Partner Agency that uses HMIS in the presence of clients. 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.

Collection of Personal Information

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

- 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 must be able to access 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.
   - 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. (Personal information released for research and statistical purposes will be anonymous.)
- 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 organization or institution. All research projects must be conducted under a written research agreement approved in writing by the designated agency administrator or executive director.

  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 CoC's HMIS Lead Agency should 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 should 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 owner/Participating Agency where the data was collected.
- 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 written 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 HMIS access.

Complaints and Accountability

Client questions or complaints about the privacy and security policies and practices may be submitted to the agency where the client receives services. Complaints specific to HMIS should be submitted to the HMIS agency administrator 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 procedure as outlined in the agency's handbook.

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 User License Agreement, which includes a statement describing this limitation, and report any potential conflict of interest to their Agency Administrator. 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.

6. Disaster Recovery

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

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

- Database tape backups occur nightly.
- Tape backups are stored offsite.
- Seven day backup history is stored locally on instantly accessible Raid 10 storage.
- One month backup history is stored off site.
- Access to Mediware Information Systems emergency line to provide assistance related to "outages" or "downtime" twenty four hours a day.
- Data is backed up locally on instantly accessible disk storage every twenty four hours.
- The application server is backed up off-site, out-of-state, on a different internet provider and on a separate electrical grid via secured Virtual Private Network (VPN) connection.
- Backups of the application site are near-instantaneous (no files older than five minutes).
- The database is replicated nightly at an off-site location in case of a primary data center failure.
- Priority level response (ensures downtime will not exceed four hours).

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. Mediware Information Systems support staff helps manage communication or messaging to the System Administrators as progress is made to address the service outage.

7. 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. ServicePoint, 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 ServicePoint be current with all recommended patches and operating system software updates installed.

User Authentication - Passwords

Mediware Information System's ServicePoint 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 should 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: Any passwords that are written down 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 forty five days. End users may not use the same password consecutively. Passwords cannot be re-used until two password selections have expired.

Unsuccessful login: If an end user unsuccessfully attempts to log-on three 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. Requests for password reset should be sent to the designated Agency Administrator and to the HMIS Lead Agency (HSN) 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 WPA2 security and the network is password protected.

8. Physical Safeguards

Physical Access to Systems with Access to HMIS Data

Confidentiality of client-level information is key within all agencies, and every effort should be taken to maintain confidentiality and integrity of this information. All client files, or print-outs of client level information, should 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 should be taken to ensure that computers and data are secure and not usable by unauthorized individuals. After 10 minutes or less, workstations should 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 should 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 should be called in advance to ensure the fax is properly managed upon receipt.
- When finished faxing, copying or printing, all documents containing PII should 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 should 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.

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