Central Florida Continuum of Care
(CoC FL-507)

Homeless Management Information System (HMIS) Policies & Procedures

Prepared by the Homeless Services Network of Central Florida (HMIS Lead Agency)
and the CoC HMIS Advisory Committee

Adopted by the Central Florida Continuum of Care

Re-adopted in full January 2013, with subsequent amendments

Reviewed and current as of July 1, 2017

Central Florida Continuum of Care (CoC FL-507)

HMIS Policies and Procedures

TABLE OF CONTENTS

I. Introduction

The Central Florida Continuum of Care (CoC) is the region's strategic approach to the organization and delivery of services to people who are homeless in Orange, Seminole, and Osceola Counties. The result is a coordinated, multi-agency system of the services ranging from outreach to permanent housing, which addresses many of the housing and supportive services needs of both homeless individuals and families in Central Florida. The Homeless Services Network of Central Florida (HSN) currently serves as the HMIS Lead Agency for the Central Florida CoC.

The Central Florida CoC has implemented a Homeless Management Information System (HMIS) to facilitate the collection of information on homeless individuals and families throughout the region. HMIS data can be employed to better understand the characteristics of homeless persons in the community, improve the delivery of housing and services homeless persons, and document the community's progress in reducing homelessness.

The CoC recognizes the importance of maintaining confidential client records in a secure environment to insure that the information is not misused or accessed by unauthorized people. The following Policies and Procedures have been developed to establish standards for the collection, storage and dissemination of confidential information by the users of the CoC HMIS.

II. Governing Principles

Described below are the overall governing principles upon which all other decisions pertaining to the CoC's HMIS project are based.

The CoC's HMIS will be:

- A confidential and secure environment for the collection and use of client data.
- A benefit to individual clients through enhanced service delivery.
- A tool for the provider agencies in managing programs and services.
- A guide for the CoC and its funders through compilation of aggregate data regarding community resource needs and service delivery.

III. HMIS Benefits

Benefits for service providers:

- Provides online real-time information about client needs and the services available for homeless persons.
- Assures confidentiality by providing information in a secured system.
- Decreases duplicative client intakes and assessments.
- Tracks client outcomes and provides a client history.
- Generates data reports for local use and for state and federal reporting requirements.
- Facilitates the coordination of services within an organization and with other agencies and programs.
- Provides access to a regional database of service providers, allowing agency staff to easily select a referral agency.

Benefits for homeless persons:

- Intake information and needs assessments are maintained historically, reducing the number of times homeless persons must repeat their stories to multiple service providers.
- The opportunity to provide intake and life history one time demonstrates that service providers consider the homeless person's time is valuable and restores some of the consumer's dignity.
- Multiple services can be easily coordinated and referrals streamlined.

Benefits for policy makers:

- Better able to define and understand the extent of homelessness throughout the region.
- Better able to focus staff and financial resources to the agencies and programs in geographical areas where services for homeless persons are needed the most.
- Better able to evaluate the effectiveness of specific interventions and specific programs and services provided.
- Better able to provide the Florida Legislature, Congress, U.S. HUD, the Florida Department of Children and Families, and other state and federal agencies with data and information on the homeless population in Central Florida.
- Better able to meet all federal and other reporting requirements.

IV. HMIS Roles and Responsibilities

HMIS Advisory Committee

1. Implement and continuously improve the CoC's HMIS.
2. Ensure the HMIS scope is in alignment and compliance with the requirements of agencies, HUD and other stakeholder groups.
3. Address any issue that has major implications for the HMIS, such as policy mandates from HUD or performance problems with the HMIS vendor.
4. Reconcile differences in opinions and approaches, and resolve disputes arising from them.
5. Under the oversight of the CoC Board and in accordance with the CoC Governance Charter, develop and implement the CoC's HMIS program.
6. Periodically review, revise, and submit to the CoC Board for approval a privacy plan, a security plan, and a data quality plan for the HMIS.
7. Review and recommend new or revised HMIS policies, procedures, and standard to the CoC Board.
8. Implement CoC-wide strategies to ensure consistent and appropriate participation by recipients and sub-recipients in the HMIS.

HMIS Software Vendor

1. Design the HMIS to meet HUD HMIS Data Standards.
2. Develop a codebook and provide other documentation of programs created.
3. Provide ongoing support to the HMIS Program Manager pertaining to needs of end-users to mine the database, generate reports and other end-user interface needs.
4. Administer the product servers including web and database servers.
5. Monitor access to HMIS through auditing.
6. Monitor functionality, speed and database backup procedures.
7. Provide backup and recovery of internal and external networks.
8. Maintain the system twenty-four hours a day, seven days a week.
9. Communicate any planned or unplanned interruption of service to the HMIS Program Manager.

HMIS Lead Agency:

1. Oversee all contractual agreements with funders, participating organizations and consultants in adherence to adopted HMIS policies and procedures.
2. Monitor compliance and periodically review control decisions.
3. Communicate with participating organization leadership and other stakeholders regarding HMIS.
4. Authorize usage and access to HMIS for users who need access to the system for technical administration, data entry, editing of client records, viewing of client records, report writing, or administration of essential activities associated with carrying out HMIS responsibilities.
5. Develop reports.
6. Mine the database to respond to the information needs of participating organizations, community

stakeholders and consumers.
7. Document work on the database and the development of reports/queries.
8. Provide technical assistance as needed with program sites.
9. Provide training and technical assistance to participating organizations on policies and procedures and system use.
10. Respond to questions from users.
11. Coordinate technical support for system software.
12. Communicate problems with data entry and support data quality to participants.
13. Monitor agency participation including timeliness and completeness of entry.
14. Communicate any planned or unplanned interruption in service.
15. Audit policy and procedure compliance.
16. Serve as the applicant to HUD for any HMIS grants that will cover the Continuum of Care geographic area.
17. Complete an annual security review.

HMIS Agency Administrator:

1. Edit and update agency information in HMIS.
2. Ensure that the Participating Agency obtains a unique user license for each user at the agency.
3. Establish the standard report for each specific program created.
4. Ensure a minimum standard of data quality by answering all the HUD Universal Data Elements for every individual entered into HMIS by the agency.
5. Maintain the HUD required elements for each program.
6. Train new staff persons on HMIS, including reviewing the policies and procedures and any agency policies that impact the security and integrity of client information.
7. Ensure that HMIS access is granted only to staff members that have received training and are authorized to use HMIS.
8. Grant technical access to HMIS for persons authorized by the HMIS Program Manager by creating usernames and passwords.
9. Notify all users at their agency of interruptions in service.
10. Provide a single point of communication between users and HMIS staff
11. Administer and monitor data security policies and standards, including:
    a. User access control
    b. Back-up and recovery of data
    c. Detection of, responding to and reporting of violations of HMIS Policies and Procedures.

HMIS End User:

1. Take appropriate measures to prevent unauthorized data disclosure.
2. Report any security violations.
3. Comply with relevant policies and procedures.

4. Input required data field in a timely manner.
5. Inform clients about agency use of HMIS and relevant privacy policies.
6. Take responsibility for any actions undertaken with his or her username and/or password.

V. HMIS Administration Requirements

Participation Agreement Documents

Participating Agencies must complete the following documents:

- HMIS Agency Agreement, which must be signed by each Participating Agency's executive director. The participation agreement states the agency's commitment to adhere to the policies and procedures for effective use of HMIS.
- HMIS End User Agreement must be signed by each authorized End User.

The HMIS Lead Agency will retain the original, signed documents.

User Access to the System

The Participating Agency will work with HMIS Lead Agency staff to determine the appropriate user access level for all staff who will be granted access to HMIS. All HMIS End Users must receive training before access to the system is granted. The HMIS Agency Administrator will generate username and passwords within the administrative function of the software.

Passwords

- Creation: Passwords are automatically generated from the system when a user is created. The HMIS Agency Administrator will communicate the temporary, system-generated password directly to the HMIS End User.
- Use: The HMIS End User (User) will be required to change the password the first time they log onto the system. The password must be at least 8 characters and include two numbers or symbols. Passwords should not be able to be easily guessed or found in a dictionary. Passwords are each User's responsibility and users cannot share passwords. 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. Users are not to store passwords on a personal computer for convenience.
- Expiration: Passwords expire every 45 days. Users may not use the same password consecutively. Passwords cannot be re-used until 2 password selections have expired.
- Unsuccessful log-on: If a User unsuccessfully attempts to log-on 3 times, the User ID will be "locked out," and the User account will be de-activated, rendering the User unable to gain access until his/her password is reset by HMIS staff.

Inputting Data:

Participating Agencies must meet the minimum data entry requirements established by HUD standards. Program entry and exit dates should be recorded upon any program entry or exit on all participants. Entry dates should record the first day of service or program entry with a new program entry date for each

period/episode of service. Exit dates should record the last day of residence in a program's housing before the participant leaves the shelter or the last day a service was provided.

Tracking of Unauthorized Access

Any suspicion of unauthorized activity should be reported to the HMIS Lead Agency.

Agency HMIS Administrators

Agencies with 10 or more users may designate one person to be an Agency HMIS Administrator. HMIS Support Specialists must undergo a criminal background check. Agencies with fewer than 10 users may forego designating an HMIS Support Specialist. CoC HMIS staff will perform Agency Administrator responsibilities for all other agencies.

Agency HMIS Administrators will be responsible for creating usernames and passwords, and monitoring HMIS access by users at their agency. This person will also be responsible for training new agency staff persons on how to use HMIS.

Client Consent Forms

In addition to posting their agency's Privacy Notice, agencies must ask clients to sign the CoC's HMIS Release of Information (ROI) form. This form allows clients to authorize the electronic sharing of their personal information with other agencies that participate in HMIS when data sharing is appropriate for client service.

HMIS Software Vendor Requirements

Physical Security: Access to areas containing HMIS equipment, data and software will be secured.

Firewall Protection: The vendor will secure the perimeter of its network using technology from firewall vendors. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

User Authentication: Users may only access HMIS with a valid username and password combination that is encrypted via SSL for Internet transmission to prevent theft. If a user enters an invalid password three consecutive times, they are automatically shut out of that HMIS session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Application Security: HMIS users will be assigned a system access level that restricts their access to appropriate data.

Database Security: Wherever possible, all database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a minimal number of access points; as with production servers, production databases do not share a master password database.

Technical Support: The vendor will assist HMIS Lead Agency to resolve software problems, make necessary

modifications for special programming, and will explain system functionality to HMIS Program Manager.

Technical Performance: The vendor maintains the system, including data backup, data retrieval and server functionality/operation. Upgrades to the system software will be continuously developed and implemented.

Hardware Disposal: Data stored on broken equipment or equipment intended for disposal will be destroyed using industry standard procedures.

VI. 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 Assessment 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 according to the following procedures.

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 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 site, 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.

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

Aggregated Public Data

Information published according to the "Reporting Parameters and Guidelines" section of these Policies and Procedures.

Unpublished Restricted Access Data

Information scheduled, but not yet approved, for publication. Examples include draft reports, fragments of data sets, and data without context or data that have not been analyzed.

Procedures for Transmission and Storage of 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.

VII. Data Reporting Parameters and Guidelines

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.

Baseline Privacy Policy

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 their personal information as described in this notice when they seek assistance from an agency using HMIS and provide the agency with their personal information.

Your personal information may also be collected from:

- Additional individuals seeking services with a client
- Other private organizations that provide services and participate in HMIS

Clients must be able to access the Use and Disclosure of Personal Information policy found below.

Use and Disclosure of Personal Information

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

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

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 regularly 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 including, but not limited to, other agencies and programs participating in the CoC's HMIS.
c. Government agencies including, but not limited to HUD, DCF, and the Social Security Administration
d. Telephone directories and other published sources

5. We post a sign at all client intake desks or other locations explaining the reasons we ask for personal information. The sign says: We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless individuals, and to better understand the need of homeless individuals. We only collect information that we consider to be appropriate.

How We Use and Disclose Personal Information

1. We may or may not use or disclose personal information for activities described in this part of the notice. 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 homeless service organizations that may have separate privacy policies and that may allow different uses and disclosures of the information. These organizations include, but are not limited to, other agencies and programs participating in the CoC's HMIS.
    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 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
        i. 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
        ii. 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
        i. under any of these circumstances:

1. where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law
2. if the individual agrees to the disclosure, or
3. to the extent that the disclosure is expressly authorized by statute or regulation, and
    a. we believe the disclosure is necessary to prevent serious harm to the individual or other potential victims, or
    b. 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

ii. 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:
    1. we, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm, or
    2. 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
    i. conducted by an individual or institution that has a formal relationship with the HMIS Lead Agency if the research is conducted either:
        1. 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 the HMIS Program Administrator (if not the individual conducting the research), or
        2. by an institution for use in a research project conducted under a written research agreement approved in writing by the designated HMIS Administrator;

    And

    ii. any written research agreement:
        1. must establish rules and limitations for the processing and security of PPI in the course of the research
        2. must provide for the return or proper disposal of all PPI at the conclusion of the

research

3. must restrict additional use or disclosure of PPI, except where required by law
4. must require that the recipient of data formally agree to comply with all terms and conditions of the agreement, and
5. 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:
    i. in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena
    ii. if the law enforcement official makes a written request for PPI that:
        1. is signed by a supervisory official of the law enforcement agency seeking the PPI
        2. states that the information is relevant and material to a legitimate law enforcement investigation
        3. identifies the PPI sought
        4. is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and
        5. states that de-identified information could not be used to accomplish the purpose of the disclosure.
    iii. if we believe in good faith that the PPI constitutes evidence of criminal conduct that occurred on our premises
    iv. 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 may or may not consist only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics, or
    v. if
        1. 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
        2. 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.
j. to comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

2. Before we make any use or disclosure of your personal information that is not described here, we will

attempt to seek your consent first.

3. You have a right to an accounting of disclosures of your personal protected information. To obtain an accounting of how your PPI may have been disclosed, contact Homeless Services Network as outlined in the section regarding Privacy Grievances.

Inspection and Correction of 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. You have the right to receive these confidential communications from us as well as the right to receive them through alternative means.
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, you must submit your request in writing.
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 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.
3. We may keep information for a longer period if required to do so by statute, regulation, contract, or other requirement.

Complaints and Accountability

1. We accept and consider questions or complaints about our privacy and security policies and practices. If you think we may have violated your privacy rights or you disagree with a decision we made about access to your "Personal Protected Information" you may complete a Privacy Grievance Form, available from any staff member.
    a. It is against the law for any agency to take retaliatory action against you if you file this grievance. You can expect a written response within 30 days.
    b. Grievances may be submitted in writing and mailed or hand-delivered to: Homeless Services Network of Central Florida, 4065-D, L.B. McLeod Road, Orlando, FL 32811.
2. 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.

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.

Security Procedure Training for Users

All users must receive security training prior to being given access to HMIS. Security training will be covered during the new user training for all new users. All users must receive on-going annual training on security procedures from the HMIS Lead Agency.

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 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 HMIS Lead Agency staff 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 HMIS Lead Agency staff. All sanctions may be appealed to the Executive Director of the CoC Lead Agency.

Procedure For Reporting Security Incidents

Users and HMIS Support Specialists 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 the HMIS Program Manager. The HMIS Program Manager will use the HMIS user audit trail report to determine the extent of the breach of security.

Disaster Recovery Plan

The CoC's HMIS is covered under Bowman Systems' Disaster Recovery Plan. Due to the nature of technology, unforeseen service outages may occur. In order to assure service reliability, Bowman 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 Bowman Systems emergency line to provide assistance related to "outages" or "downtime" 24 hours a day.
- Data is backed up locally on instantly-accessible disk storage every 24 hours.
- The application server is backed up offsite, 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 5 minutes).
- The database is replicated nightly at an offsite location in case of a primary data center failure.
- Priority level response (ensures downtime will not exceed 4 hours).

Standard Data Recovery

The CoC's HMIS database is stored online, and is readily accessible for approximately 24 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 internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Our Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary Core routers are configured with redundant power supplies, and are

configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup units that are connected in turn to electrical circuits, which are connected to a building generator.

All client data is backed-up online and stored on a central file server repository for 24 hours. Each night a tape backup is made of the client database and secured in a bank vault.

Historical data can be restored from tape as long as the data requested is newer than 30 days old. As a rule, the data can be restored to a standby server within four hours without affecting the current live site. Data can then be selectively queried and/or restored to the live site.

For power outage, HMIS is backed up via battery back-up units, which are connected via generator-backed up electrical circuits. For a system crash, a system restore will take four hours. There is potential for some small data loss (data that was entered between the last backup and when the failure occurred) if a tape restore is necessary. If the failure is not hard drive related, the data restore time will possibly be shorter as the drives themselves can be repopulated into a standby server.

All major outages are immediately brought to the attention of executive management. Bowman Systems support staff helps manage communication or messaging to the HMIS Program Manager as progress is made to address the service outage.

VIII. Data Requirements

Data Collection Protocol

Participating Agencies are responsible for asking all clients a minimum set of questions for use in aggregate analysis. These questions are included in custom assessments that are created by HMIS System Administrators. The required data elements depend on the program. The mandatory data elements in each assessment are displayed in red text and/or specific text indicating that the field is required.

Programs that do not adhere to the minimum data entry standards will be notified of their deficiencies and given appropriate training on how to correctly enter data. Programs that do not meet minimum data entry standards will have HMIS access suspended until such time that HMIS staff believes the program could begin to correctly enter information. After the two initial warnings from HMIS staff, a program still not adhering to the minimum data entry requirements will be made permanently inactive, and licenses will be revoked until the agency can demonstrate to HMIS staff that it is capable of maintaining minimum data requirements.

HMIS staff will submit a report to the CoC annually that identifies the degree to which each all agencies within the CoC are meeting the minimum data entry standards.

The HMIS Program Manager must identify the assessments and requirements for each program, and properly set up each program in the HMIS software.

While HMIS databases are required to have the capacity to accept XML imports, the HMIS Lead Agency and the CoC reserve the right to not allow XML imports into the CoC's HMIS. Allowing XML imports may adversely impact data integrity and may also increase the likelihood of duplication of client files in the system.

Data Integrity And Reliability

Guidelines clearly articulating the minimum expectations for data entry for all programs entering data in HMIS will be defined in Agency Agreements. HMIS Support Specialists must ensure that the minimum data elements are fulfilled for every program.

Participating Agencies are responsible for the overall quality, accuracy and completeness of data entered by their staff for their clients. HMIS staff will monitor data collection for random variables and hold Participating Agencies accountable for not entering required data.

SECTION IX

HMIS-Related Forms

<u>Note:</u> Some formatting has been lost upon incorporation of forms into this document.

Please contact HSN for official copies of all forms.

HOMELESS SERVICES NETWORK HMIS – Partner Agency Agreement

The Homeless Services Network Homeless Management Information System ("HMIS") 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.

Ultimately, when used correctly and faithfully by all involved parties, the HMIS is designed to benefit multiple stakeholders, including provider agencies, persons who are homeless, funders and the community through improved knowledge about people who are homeless, their services and service needs and a more effective and efficient service delivery system.

_____, ("Agency") has elected to participate in the Homeless Services Network HMIS.

Agency and Homeless Services Network agree as follows:

Section 1 - General Understandings

1. In this Agreement, the following terms will have the following meanings:
   a. "Client" refers to a consumer of services;
   b. "Partner Agency" refers generally to any Agency participating in Homeless Services Network HMIS.
   c. "Agency staff" refers to both paid employees and volunteers of an Agency.
   d. "HMIS" refers to the Homeless Services Network HMIS system.
   e. "Enter(ing)" or "entry" refers to the entry of any Client information into the HMIS.
   f. "Shar(e)(ing)," or "Information Shar(e)(ing)" refers to the sharing of information which has been entered in the HMIS with another Partner Agency.
   g. "Homeless Services Network HMIS Advisory Group" refers to Homeless Services Network's HMIS advisory body. The Advisory Group is comprised of representatives from Homeless Services Network's Continuum of Care and at large members. The Advisory Group serves in a consultative and counseling capacity to Homeless Services Network's role as the HMIS administrator.
   h. "Identified Information" refers to Client data that can be used to identify a specific Client. Also referred to as "Confidential" data or information.
   i. "De-identified Information" refers to data that has specific Client demographic information removed, allowing use of the data ***without identifying*** a specific Client. Also referred to as "non-identifying" information.
2. Agency understands that when it enters information into the HMIS, such information will be available to the Homeless Services Network staff who may review the data to administer HMIS; to conduct analysis; and to prepare reports which may be submitted to others in de-identified form ***without*** individual identifying Client information.
   a. Agency understands that Agency will have the ability to indicate whether information Agency entered into HMIS may be shared with and accessible to Partner Agencies in HMIS system. Agency is responsible

for determining and designating in HMIS whether information may or may not be shared.

Section 2 - Confidentiality

1. Agency will not
   a. enter information into HMIS which it is not authorized to enter; and
   b. will not designate information for sharing which Agency is not authorized to share, under any relevant federal, state, or local confidentiality laws, regulations or other restrictions applicable to Client information. By entering information into HMIS or designating it for sharing, Agency represents that it has the authority to enter such information or designate it for sharing.
2. Agency represents that: *(check applicable items)*
3. it is _____; is not _____a "covered entity" whose disclosures are restricted under HIPAA (45 CFR 160 and 164);
   a. it is _____; is not _____ a program whose disclosures are restricted under Federal Drug and Alcohol Confidentiality Regulations: 42 CFR Part 2;
   b. If Agency is subject to HIPAA, (45 CFR 160 and 164) or 42 CFR Part 2, a fully executed *Business Associate or Business Associate/Qualified Service Organization Agreement* must be attached to this agreement before information may be entered. Sharing of information will not be permitted otherwise.
   c. If Agency is subject to any laws or requirements which restrict Agency's ability to either enter or authorize sharing of information, Agency will ensure that any entry it makes and all designations for sharing fully comply with all applicable laws or other restrictions.
4. To the extent that information entered by Agency into HMIS is or becomes subject to additional restrictions, Agency will immediately inform Homeless Services Network in writing of such restrictions.

Section 3 - Display of Notice

Pursuant to the notice published by the Department of Housing and Urban Development ("HUD") on July 30, 2004, Agency will prominently display at each intake desk (or comparable location) a Privacy Notice that explains the reasons for collecting Client identified information in the HMIS and the client rights associated to providing Agency staff with their identified data. Agency will post its Privacy Notice document prominently to ensure client's understanding of their rights. The current form is available from Homeless Services Network and is incorporated into this Agreement and may be modified from time to time by Homeless Services Network.

Section 4 - Information Collection, Release and Sharing Consent

1. **Collection of Client Identified Information**: An agency may collect client identified information only when appropriate to the purposes for which the information is obtained or when required by law. An Agency must collect client information by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.
2. **Obtaining Client Consent:** In obtaining Client consent, Agency will post its Privacy Notice at each intake desk (or comparable location). Consent of the individual for data collection may be inferred from the circumstances of the collection.

a. If a Client withdraws or revokes consent for Client identified information collection, Agency is responsible for immediately making appropriate data entries in HMIS to ensure that Client's personal identified information will not be shared with other Partner Agencies or visible to the Agency staff within the system.

b. This information is being gathered for the collection and maintenance of a research database and data repository. The consent implied is in effect until the client revokes the consent in writing.

3. **Designation for Sharing:** Prior to designating any information for sharing, Agency will provide the Client with a copy of the Homeless Services Network *Client Release and Sharing of Information* form. The current form is available from Homeless Services Network and is incorporated into this Agreement and may be modified from time to time by Homeless Services Network. Following an explanation of the data use, the Agency will obtain the informed consent of the Client by having the Client sign the Homeless Services Network *Client Release and Sharing of Information* form**.**

   a. If a Client does not sign the release/sharing form as described above, information may not be shared with other Partner Agencies**. It is the responsibility of Agency entering information about a Client to determine whether consent has been obtained; to make appropriate entries in HMIS to either designate the information as appropriate for sharing or prohibit information sharing; to implement any restrictions on information sharing; and to implement any revocation of consent to information sharing.**

   b. Agency will keep all copies of the *Client Release and Sharing of Information* form signed by Clients for a period of seven years. Such forms will be available for inspection and copying by Homeless Services Network at any time.

Section 5 - No Conditioning of Services

Agency will not condition any services upon or decline to provide any services to a Client based upon a Client's refusal to sign a *Client Release and Sharing of Information* form for the sharing of identified information or refusal to allow entry of identified information into HMIS.

Section 6 - Re-release Prohibited

Agency agrees not to release any Client identifying information received from HMIS to any other person or organization without written informed Client consent, or as required by law.

Section 7 - Client Inspection/Correction

Agency will allow a Client to inspect and obtain a copy of his/her own personal information except for information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding. Agency will also allow a Client to correct information which is inaccurate. Corrections will be made by way of a new entry which is in addition to but is not a replacement for an older entry.

Section 8 - Security

Agency will maintain security and confidentiality of HMIS information and is responsible for the actions of its users and for their training and supervision. Agencies will follow the *Homeless Services Network Security Policy* which is available from Homeless Services Network and is incorporated into this agreement and may be

modified from time to time. Among the steps Agency will take to maintain security and confidentiality are:

1. **Access:** Agency will permit access to HMIS or information obtained from it only to authorized Agency staff who need access to HMIS for legitimate business purposes (such as to provide services to the Client, to conduct evaluation or research, to administer the program, or to comply with regulatory requirements). Agency will limit the access of such staff to only those records that are immediately relevant to their work assignments.
2. **User Policy:** Prior to permitting any user to access HMIS, Agency will require the user to sign a *User Policy, Responsibility Statement & Code of Ethics* ("User Policy") which is available from Homeless Services Network and is incorporated into this agreement and may be amended from time to time by Homeless Services Network. Agency will comply with, and enforce the User Policy and will inform Homeless Services Network immediately in writing of any breaches of the User Policy.
3. **Computers:** Security for data maintained in the Homeless Services Network HMIS depends on a secure computing environment. Computer security is adapted from relevant provisions of the Department of Housing and Urban Development's (HUD) *"Homeless Management Information Systems (HMIS) Data and Technical Standards Notice"* (Docket No. FR 4848- N-01; see http://www.hud.gov/offices/cpd/homeless/hmis). Agencies are encouraged to directly consult that document for complete documentation of HUD's standards relating to HMIS. Agency will allow access to HMIS only from computers which are:
   a. physically present on Agency's premises;
   b. owned by Agency; or
   c. approved by Agency for the purpose of accessing and working with HMIS; and
   d. protected from viruses by commercially available virus protection software,
   e. protected with a software or hardware firewall,
   f. maintained to insure that the computer operating system running the computer used for the HMIS is kept up to date in terms of security and other operating system patches, updates, and fixes,
   g. accessed through web browsers with 128-bit encryption. Some browsers have the capacity to remember passwords, so that the user does not need to type in the password when returning to password-protected sites. This default shall ***not*** be used with respect to the Homeless Services Network HMIS; the end-user is expected to physically enter the password each time he or she logs on to the system,
   h. staffed at all times when in public areas. When computers are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not publicly accessible. These steps should minimally include: Logging off the data entry system, physically locking the computer in a secure area, or shutting down the computer entirely,
4. **Passwords:** Agency will permit access to HMIS only with use of a User ID and password which the user may not share with others. Written information pertaining to user access (e.g. username and password) shall not be stored or displayed in any publicly accessible location. Passwords shall be at least eight characters long and meet industry standard complexity requirements, including, but not limited to, the use of at least one of each of the following kinds of characters in the passwords: Upper and lower-case letters, and numbers and symbols. Passwords shall not be, or include, the username, or the HMIS name. In addition, passwords should not consist entirely of any word found in the common dictionary or any of the above

spelled backwards. The use of 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. Passwords and user names shall be consistent with guidelines issued from time to time by HUD and/or Homeless Services Network.

5. **Training/Assistance:** Agency will permit access to HMIS only after the authorized user receives appropriate training. Agency will conduct ongoing basic confidentiality training for all persons with access to HMIS and will train all persons who may receive information produced from HMIS on the confidentiality of such information. Agency will participate in such training as is provided from time to time by Homeless Services Network. Homeless Services Network will be reasonably available during its defined weekday business hours for technical assistance (i.e. troubleshooting and report generation).
6. **Records:** Agency and Homeless Services Network will maintain records of any disclosures of Client identifying information either of them makes of HMIS information for a period of seven years after such disclosure. On written request of a Client, Agency and Homeless Services Network will provide an accounting of all such disclosures within the prior seven-year period. Homeless Services Network will have access to an audit trail from HMIS so as to produce an accounting of disclosures made from one Agency to another by way of sharing of information from HMIS.

Section 9 - Information Entry Standards

1. Information entered into HMIS by Agency will be truthful, accurate and complete to the best of Agency's knowledge.
2. Agency will ***not*** solicit from Clients or enter information about Clients into the HMIS database unless the information is required for a legitimate business purpose such as to provide services to the Client, to conduct evaluation or research, to administer the program, or to comply with regulatory requirements.
3. Agency will only enter information into HMIS database with respect to individuals which it serves or intends to serve, including through referral.
4. Agency will enter information into the HMIS database within one month of data collection.
5. Agency will not alter or over-write information entered by another Agency.

Section 10 - Use of Homeless Services Network HMIS:

1. Agency will not access identifying information for any individual for whom services are neither sought nor provided by the Agency. Agency may access identifying information of the Clients it serves and may request via writing access to statistical, non-identifying information on both the Clients it serves and Clients served by other Homeless Services Network HMIS participating agencies.
2. Agency may report non-identifying information to other entities for funding or planning purposes. Such non-identifying information shall not directly identify individual Clients.
3. Agency and Homeless Services Network will report only non-identifying information in response to requests for information from HMIS.
4. Agency will use HMIS database for its legitimate business purposes only.
5. Agency will not use HMIS in violation of any federal or state law, including, but not limited to, copyright, trademark and trade secret laws, and laws prohibiting the transmission of material, which is threatening, harassing, or obscene.

6. Agency will not use the HMIS database to defraud federal, state or local governments, individuals or entities, or conduct any illegal activity.

Section 11 - Proprietary Rights of the Homeless Services Network HMIS:

1. Agency shall not give or share assigned passwords and access codes for HMIS with any other Agency, business, or individual.
2. Agency shall take due diligence not to cause in any manner, or way, corruption of the HMIS database, and Agency agrees to be responsible for any damage it may cause.

Section 12 - HMIS Advisory Group

Homeless Services Network will consult with the Advisory Group from time to time regarding issues such as revision to the form of this Agreement. Written Agency complaints that are not resolved may be forwarded to the HMIS Advisory Group, which will try to reach a voluntary resolution of the complaint.

Section 13 - Limitation of Liability and Indemnification

No party to this Agreement shall assume any additional liability of any kind due to its execution of this agreement of participation in the HMIS system. It is the intent of the parties that each party shall remain liable, to the extent provided by law, regarding its own acts and omissions; but that no party shall assume additional liability on its own behalf or liability for the acts of any other person or entity except for the acts and omissions of their own employees, volunteers, agents or contractors through participation in HMIS. The parties specifically agree that this agreement is for the benefit of the parties only and this agreement creates no rights in any third party.

Section 14 - Limitation of Liability

Homeless Services Network shall not be held liable to any member Agency for any cessation, delay or interruption of services, nor for any malfunction of hardware, software or equipment.

Section 15 - Disclaimer of Warranties

Homeless Services Network makes no warranties, express or implied, including the warranties or merchandise ability and fitness for a particular purpose, to any Agency or any other person or entity as to the services of the HMIS system to any other matter.

Section 16 - Additional Terms and Conditions

1. Agency will abide by such guidelines as are promulgated by HUD and/or HSN from time to time regarding administration of the HMIS.
2. Agency and HSN intend to abide by applicable law. Should any term of this agreement be inconsistent with applicable law, or should additional terms be required by applicable law, Agency and HSN agree to modify the terms of this agreement so as to comply with applicable law.
3. Neither HSN nor Agency will transfer or assign any rights or obligations regarding HMIS without the written consent of either party.
4. Agency agrees to indemnify and hold HSN and its agents and staffs harmless from all claims, damages,

costs, and expenses, including legal fees and disbursements paid or incurred, arising from any breach of this Agreement or any of Agency's obligations under this Agreement.

5. This Agreement will be in force until terminated by either party. Either party may terminate this agreement at will with twenty-one (21) days written notice. Either party may terminate this agreement immediately upon a material breach of this Agreement by the other party, including but not limited to the breach of the CoC HMIS security policies by Agency.
6. If this Agreement is terminated, Agency will no longer have access to HMIS. HSN and the remaining Partner Agencies will maintain their right to use all of the Client information previously entered by Agency except to the extent a restriction is imposed by Client or law.
7. Copies of Agency data will be provided to the Agency upon written request of termination of this agreement. Data will be provided on mutually agreed upon media. Unless otherwise specified in writing, copies of data will be delivered to Agency within twenty-eight (28) calendar days of receipt of written requests for data copies.

Section 17 - Signatory Page

Agency Name _____ **Agency Address** _____ _____	**Homeless Services Network of Central Florida, Inc.** 4065 L.B. McLeod Road Suite D Orlando, FL 32811
Agency Executive Director _____ (print) _____ _____ (signature) Date	**HSN Executive Director** _____ (print) _____ _____ (signature) Date

CENTRAL FLORIDA CONTINUUM OF CARE

AGENCY ADMINISTRATOR AGREEMENT

All HMIS participating agencies must designate and staff one HMIS Agency Administrator. Agency Administrator requirements and responsibilities include, but are not limited to, the following:

- Has completed, at minimum, general Client Point training.
- Ensure that all Agency users have signed End User Agreement documents on file.
- Ensure that all Users complete an annual End User Certification Test, which includes Privacy and Security training.
- Ensure that all Users have completed workflow training and related updates, and have documentation of training.
- Ensure that the Agency is in compliance with the CoC Data Security standards.
- Ensure that the Agency is in compliance with the HMIS Policies and Procedures, has completed the Compliance Checklist, and is responsible for returning it to the local Lead Agency System Administrator.
- Ensure that all Users have submitted a criminal background check to the local Lead Agency System Administrator.

The original Agency Administrator Agreement shall be kept on file at the Agency. Forms completed by individuals no longer employed by the Agency shall be kept on file for a minimum of five years.

The CoC makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold the CoC harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in the; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold the CoC harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Bowman Information Systems, by the Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. The CoC shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of the CoC. The CoC agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of the CoC.

This agreement is in effect for a period of one (1) year after date of signing. Agency Administrators are

required to complete HMIS End User Certification testing and to document compliance monitoring annually, at which time a new agreement will be provided. Failure to participate in annual Certification and/or maintain a current agreement may result in immediate termination or suspension of the user's ServicePoint license and access to ServicePoint. Failure to comply with the provisions of this Agency Administrator Agreement is grounds for immediate termination. Your signature below indicates your agreement to comply with this Agency Administrator Agreement.

Employee Printed Name	Agency Executive Director Name
Employee Signature	Agency Executive Director Signature
Date (mm/dd/yy)	Date (mm/dd/yy)

Central Florida Continuum of Care
Agency HMIS Audit Checklist

____ Has completed and submitted Policies and Procedures Compliance Checklist

____ Has completed annual Privacy and Security Checklist

____ All End Users have executed End User Agreement

____ Agency has conducted criminal background checks on all end users

____ HUD Public Notice is posted and visible to clients

____ Has HMIS Privacy Notice and is available to clients

____ Has HMIS Privacy Policy which details the procedures of the Privacy Notice

____ HMIS Privacy Policy includes a remote access plan

____ Hard copy data is secure

____ HMIS workstations are password protected

____ HMIS workstations have time scheduled locked settings

____ All clients are entered into the System within 48 hours of intake

____ All End Users have received a copy of the HUD Data Elements

____ Staff members have been trained on the HUD definition of homelessness and understand the priority of homelessness documentation

____ Agency has process to ensure clients name is spelled properly and DOB is accurate

____ End Users are updated client information as required for program type through Interim Reviews and Follow Ups

____ Agency Admins or assigned staff are running monthly data quality reports and making corrective action in accordance with the requirements of the CoC Policies and Procedures

____ All End Users have had at least general ClientPoint training

CoC Security Officer Agreement

Name: _____

Agency Name: _____

All HMIS participating agencies must designate and staff one HMIS Security Officer. Security Officer requirements and responsibilities include, but are not limited to, the following:

- Ensures that all staff using the system complete annual privacy and security training. Training must be provided by the CoC designated trainers and be based on the CoC Privacy and Security standards.

- Conducts an annual security review of the agency that includes reviewing compliance with the Privacy and Security sections of the CoC Homeless Management Information System (HMIS) Operating Policy and Procedure. The Agency must document the findings of the review on the Privacy and Security Checklist and submit the findings to the local Lead HMIS System Administrator no later than December 31st of each year.

- Notifies the local Lead Agency System Administrator when a staff person leaves the organization or when revision of the user's access level is needed because of a change in job responsibilities. The notification must be made within 48 hours of the change.

- Reports any security or privacy incidents to the local Lead HMIS System Administrator for the CoC Jurisdiction. The System Administrator investigates the incident including running applicable audit reports. If the System Administrator and Security Officer determine that a breach has occurred and/or the staff involved violated privacy or security guidelines, the System Administrator will report to the chair of the CoC. A Corrective Action Plan will be implemented. Components of the Plan must include, at minimum, supervision and retraining. It may also include removal of HMIS license, client notification if a breach has occurred, and any appropriate legal action.

The original Security Officer Agreement shall be kept on file at the Agency. Forms completed by individuals no longer employed by the Agency shall be kept on file for a minimum of five years.

The CoC makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold the CoC harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in the ; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold the CoC harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Bowman Information Systems, by the Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. The CoC shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of the CoC. The CoC agrees to hold the Agency harmless from any damages, liabilities, claims or expenses

caused solely by the negligence or misconduct of the CoC.

This agreement is in effect for a period of one (1) year after date of signing. Security Officers are required to complete HMIS End User Certification testing and documented Privacy & Security compliance monitoring annually, at which time a new agreement will be provided. Failure to participate in annual Certification, Privacy & Security monitoring, and/or maintain a current agreement may result in immediate termination or suspension of the user's ServicePoint license and access to ServicePoint. Failure to comply with the provisions of this Security Officer Agreement is grounds for immediate termination. Your signature below indicates your agreement to comply with this Security Officer Agreement.

Employee Printed Name	Agency Official Printed Name
Employee Signature	Agency Official Signature
Date (mm/dd/yy)	Date (mm/dd/yy)

CONSENT TO SHARE PROTECTED PERSONAL INFORMATION

The CoC FL-507 HMIS is a local electronic database that securely record information (data) about clients accessing housing and homeless services within the Seminole, Osceola and Orange Counties. This organization participates in the HMIS database and shares information with other organizations that use this database. This information is utilized to provide supportive services to you and your household members.

What information is shared in the HMIS database? We share both Protected Personal Information (PPI) and general information obtained during your intake and assessment, which may include but is not limited to:

- Your name and your contact information
- Your social security number
- Your birthdate
- Your basic demographic information such as gender and race/ethnicity
- Your history of homelessness and housing (including your current housing status, and where and when you have accessed services)
- Your self-reported medical history, including any mental health and substance abuse issues
- Your case notes and services
- Your case manager's contact information
- Your income sources and amounts; and non-cash benefits
- Your veteran status
- Your disability status
- Your household composition
- Your emergency contact information
- Any history of domestic violence
- Your photo (optional)

How do you benefit from providing your information? The information you provide for the HMIS database helps us coordinate the most effective services for you and your household members. By sharing your information, you may be able to avoid being screened more than once, get faster services, and minimize how many times you tell your 'story.' Collecting this information also gives us a better understanding of homelessness and the effectiveness of services in your local area.

Who can have access to your information? Organizations that participate in the HMIS database can have access to your data. These organizations may include homeless service providers, housing groups, healthcare providers, and other appropriate service providers.

How is your personal information protected? Your information is protected by the federal HMIS Privacy Standards and is secured by passwords and encryption technology. In addition, each participating organization has signed an agreement to maintain the security and confidentiality of the information. In some instances, when the participating organization is a health care organization, your information may be protected by the privacy standards of the Health Insurance Portability and Accountability Act (HIPAA).

By signing below, you understand and agree that:

- You have the right to receive services, even if you do not sign this consent form.
- You have the right to receive a copy of this consent form.
- Your consent permits any participating organization to add to or update your information in HMIS, without asking you to sign another consent form.
- This consent is valid for seven (7) years from the date the PPI was created or last changed.
- You may revoke your consent at any time, but your revocation must be provided either in writing or by completing the *Revocation of Consent* form. Upon receipt of your revocation, we will remove your PPI from the shared HMIS database and prevent further PPI from being added. The PPI that you previously authorized to be shared cannot be entirely removed from the HMIS database and will remain accessible to the limited number of organization(s) that provided you with direct services.
- The Privacy Notice for the CoC FL-507 HMIS contains more detailed information about how your information may be used and disclosed. A copy of this notice is available upon request.
- No later than five (5) business days of your written request, we will provide you with:
- A correction of inaccurate or incomplete PPI
- A copy of your consent form
- A copy of your HMIS records; and
- A current list of participating organizations that have access to your HMIS data.
- Aggregate or statistical data that is released from the HMIS database will not disclose any of your PPI.
- You have the right to file a grievance against any organization whether or not you sign this consent.
- You are not waiving any rights protected under Federal and/or Florida law.

SIGNATURE AND ACKNOWLEDGEMENT

Your signature below indicates that you have read (or been read) this client consent form, have received answers to your questions, and you freely consent to have your information, and that of your minor children (if any), entered into the HMIS database. You also consent to share your information with other participating organizations as described in this consent form.

☐ **I consent to sharing my photograph. (Check here)**

Client Name: _____DOB: _____ Last 4 digits of SS_____

Signature _____ Date _____

☐ **Head of Household (Check here)**

Minor Children (if any):

Client Name: _____ DOB: _____ Last 4 digits of SS _____ Living with you? (Y/N)

Client Name: _____ DOB: _____ Last 4 digits of SS _____ Living with you? (Y/N)

Client Name: _____ DOB: _____ Last 4 digits of SS _____ Living with you? (Y/N)

_____ _____

Print Name of Organization Staff

_____ _____

Signature of Organization Staff Date

Central Florida Continuum of Care HMIS
HMIS End User Agreement

For: _____ From: _____
User's Full Name (print name) Agency Name (print name)

User Responsibilities

1. Users must be prepared to answer Client questions regarding HMIS.
2. Users must faithfully respect Client preferences with regard to the entry and sharing of Client information within HMIS.

Users must accurately record Client's preferences by making the proper designations as to the sharing of Client information and/or any restrictions on the sharing of Client information.

3. Users must allow Client to change his or her information sharing preferences at the Client's request.
4. Users must not decline services to a Client or potential Client if that person refuses to allow entry of information into HMIS or to share their personal information with other agencies via HMIS.
5. The User has primary responsibility for information entered by the User. Information Users enter must be truthful, accurate and complete to the best of User's knowledge.
6. Users will not solicit from or enter information about Clients into HMIS unless the information is required for a legitimate business purpose such as to provide services to the Client.
7. Users will not use HMIS database for any violation of any law, to defraud any entity, or conduct any illegal activity.
8. Upon Client's written request, users must allow a Client to inspect and obtain a copy of the Client's own information maintained within HMIS. Information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding need not be provided to Client.
9. Users must permit Clients to file a written complaint regarding the use or treatment of their information within HMIS.

Clients may file a written complaint with either the Partner Agency or Homeless Services Network (at P.O. Box 547068, Orlando, FL 32854-7068).

10. Users may not retaliate against a Client for filing a complaint.
11. Users are responsible for obtaining and maintaining their own HMIS account security.
12. Users will not share access to their HMIS accounts with anyone.
13. Users will take reasonable means to keep chosen passwords physically secure.
14. Users will only view, obtain, disclose, or use the database information that is necessary to perform their jobs.
15. Users understand that only authorized individuals may directly access HMIS Client information and will take the following

steps to prevent casual observers from accessing HMIS Client information:

a. Users will log off the HMIS before leaving their work area, or make sure that the HMIS database has "timed out" before leaving their work area.
b. Users will not leave unattended any computer that has HMIS "open and running".
c. Users will keep their computer monitors positioned so that persons not authorized to use HMIS cannot view the screen.

d. Users will store hard copies of HMIS information in a secure file and not leave such hard copy information in public view.
e. Users will properly destroy paper copies of HMIS information when they are no longer needed unless they are required to be retained in accordance with applicable law.
f. Users will not discuss HMIS confidential Client information with staff, Clients, or Client family members in a public area.
g. Users will not discuss HMIS confidential Client information on the telephone in any areas where the public might overhear my conversation.
h. Users will not leave messages on an agency's voice mail system that contains HMIS confidential Client information.
i. Users will take steps to ensure HMIS confidential information left by callers is not overheard by the public or unauthorized persons.
16. Users must 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, access to the HMIS may be terminated and users may be subject to further disciplinary action as defined in the Partner Agency's personnel policy.
17. If users notice or suspect a security breach, they will immediately notify the Director of their Agency and the Homeless Services Network HMIS Administrator.

User Agreement: I understand and agree to comply with all the statements listed above.

User Signature	Date	User's Full Name (please print)
		User's Job Title
Witness Signature	Date	Witness Full Name (please print)

Central Florida Continuum of Care
Privacy and Security Checklist

Agency Name: _____

Security Officer Name: _____

_____ (Int.) Agency has the HUD Public Notice posted in an area visible to clients.

Finding(s): _____

_____

Corrective Action(s): _____

_____

Deadline for Completion: _____

_____ (Int.) Agency has an HMIS Privacy Notice that complies with the requirements set forth by the CoC HMIS Operating Policies and Procedures, and is available to all clients.

Finding(s): _____

_____

Corrective Action(s): _____

_____

Deadline for Completion: _____

_____ (Int.) Agency has a copy of the HUD Public Notice and the Privacy Notice on its website.

Finding(s): _____

_____

Corrective Action(s): _____

Deadline for Completion: _____

_____ (Int.) Client files with hard copy data that includes client identifying information is protected behind one lock, at minimum, from unauthorized access.

Finding(s): _____

Corrective Action(s): _____

Deadline for Completion: _____

_____ (Int.) Offices that contain client files are locked when not occupied.

Finding(s): _____

Corrective Action(s): _____

Deadline for Completion: _____

_____ (Int.) Client files are not left visible for unauthorized individuals.

Finding(s): _____

Corrective Action(s): _____

Deadline for Completion: _____

_____ (Int.) Agency has adopted the PromisSE Release of Information and requests this from every client.

Finding(s): _____

_____

Corrective Action(s): _____

_____

Deadline for Completion: _____

_____ (Int.) HMIS workspaces are configured to support privacy of client interaction and privacy of data entry.

Finding(s): _____

_____

Corrective Action(s): _____

_____

Deadline for Completion: _____

_____ (Int.) User accounts and passwords are not shared between End Users, or left visible for others to see.

Finding(s): _____

_____

Corrective Action(s): _____

_____

Deadline for Completion: _____

_____ (Int.) End Users do not save HMIS reports with identifying client information on portable media.

Finding(s): _____

Corrective Action(s): _____

_____

Deadline for Completion: _____

_____ **(Int.)** **All HMIS workstations, including laptops and remote workstations, have virus protection and automatic updates.**

Finding(s): _____

_____

Corrective Action(s): _____

_____

Deadline for Completion: _____

_____ **(Int.)** **All HMIS workstations, including laptops and remote workstations, are protected by a Firewall.**

Finding(s): _____

_____

Corrective Action(s): _____

_____

Deadline for Completion: _____

_____ **(Int.)** **End Users are not accessing the HMIS on a public computer, or from an internet connection that is not secured.**

Finding(s): _____

_____

Corrective Action(s): _____

Deadline for Completion: _____

_____ (Int.) Agency has a documented plan for remote access if End Users are accessing the HMIS outside of the office setting.

Finding(s): _____

Corrective Action(s): _____

Deadline for Completion: _____

Security Officer Printed Name	Agency Official Printed Name
Security Officer Signature	Agency Official Signature
Date (mm/dd/yy)	Date (mm/dd/yy)

Central Florida Continuum of Care (CoC FL-507)
Homless Management Information Systems (HMIS)
Self-Monitoring Tool

Purpose: To ensure the integrity of HMIS and to protect the clients and agencies served by HMIS, each agency participating in the CoC FL-507 HMIS - whether or not the agency receives HUD funding – must periodically review its HMIS practices and evaluate its compliance with applicable HUD requirements and CoC FL-507 policies.

Instructions:
The HMIS Agency Administrator must personally complete the self-monitoring process below, and then sign and return this form to the HMIS Lead Agency (HSN) **by April 30 and October 31** of each year. (Note: Completion of this self-monitoring process is separate and distinct from any monitoring of HMIS-related activity that may be conducted by the HMIS Lead (HSN) during on-site monitoring visits or via remote access.

Compliance Standard	For each compliance standard, check the box that BEST describes the agency's status				
	Currently in Compliance	Will Be in Compliance within 7 Days	Need Help to Comply	Cannot/ Will Not Comply	N/A
Administrative Oversight					
1. Agency's chief executive has read, signed and agrees to the CoC FL-507 HMIS Agency Agreement.					
2. Agency has designated a single HMIS Agency Administrator who oversees and coordinates all efforts to ensure: • Compliance by Agency with the HMIS Agency Agreement • Compliance by HMIS Users with the User Agreement, • Availability of training and technology needed for Agency participation in HMIS. Agency has also provided the name and contact information for the current Agency Administrator to the HMIS Lead (HSN).					
3. Agency has ensured that User Agreements for all HMIS Users are up to date and on file with HMIS Lead (HSN).					
4. Agency Administrator regularly reviews and, when requested, responds to communications from the HMIS Lead (HSN).					
5. Agency informs HSN of new programs or grants received that require additional CoC compliance and/or training.					
Data Completeness and Quality					
6. Agency collects and enters data into HMIS: a. for all clients (whenever relevant to and appropriate for inclusion in HMIS) in all households served, including project entry, project exit and all services. b. using all HUD- and CoC-required Data Elements. c. in a manner that is as close to real time as possible, but no later than 30 days after the collection of information/occurrence of the event to be entered.					
7. Agency received a grade of "B" or higher on a Data Quality Report Card (252) run within the last 14 days.					

Compliance Standard	For each compliance standard, check the box that BEST describes the agency's status				
	Currently in Compliance	Will Be in Compliance within 7 Days	Need Help to Comply	Cannot/ Will Not Comply	N/A
8. Agency runs & reviews the set of data completeness, quality and accuracy monitoring reports required under any CoC-related contract(s) for funding. Agency takes steps to promptly correct any identified concerns or deficiencies.					
9. Agency uses a specific procedure to ensure that all names are spelled properly and DOBs are correct.					
10. Agency has trained all HMIS Users on the HUD definition of homelessness and the priority of documenting each client's status in that regard.					
Privacy, Security and Confidentiality					
11. Each HMIS User has read and the Agency as a whole is in compliance with privacy- and security-related standards and requirements found in the CoC's HMIS Policies and Procedures.					
12. Agency displays the privacy notice and requirements found in the CoC's HMIS Policies and Procedures, and provides a copy to clients upon request.					
13. Agency has either: • Conducted a Level 1 or higher background check (i.e., criminal history check) on each HMIS User; OR • Required each HMIS User to obtain a Level 1 or higher background check from an independent source.					
14. Agency ensures that a signed HMIS Release of Information is obtained for every client for which the Agency may share personally identifiable information with external entities.					
15. Agency ensures that all computer stations, laptops and mobile devices on which HMIS is accessed: a. are private and secure. b. automatically locks HMIS after a time					
16. Agency requires that each HMIS User log out after each session.					
17. Agency strictly limits access to information entered into HMIS to authorized personnel only.					
18. Each HMIS User (including those with read-only access) has a unique user name/password. Agency strictly prohibits the sharing of user names/passwords.					
19. Agency strictly prohibits HMIS Users from using "auto-fill" and using any other password storage methods that may compromise the security of HMIS data.					
20. HMIS Lead (HSN) is notified immediately whenever an incident of unauthorized access to or inappropriate use of HMIS data is discovered by or reported to the Agency.					
21. HMIS Lead (HSN) is notified immediately whenever any HMIS User is terminated from the Agency or otherwise loses authorization to use HMIS.					

Please explain any compliance issues identified above, and provide any additional questions, requests or comments below:

Certification

I certify that the information provided above regarding our agency's compliance with HMIS-related requirements and standards is true and accurate. I further certify that I personally conducted or oversaw the HMIS compliance self-monitoring of the agency and its HMIS practices.

Print Name: _____ Title: _____

Signature: _____ Date: _____