VOLUSIA/FLAGLER COUNTY COALITION FOR THE HOMELESS (VFCCH)
HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)
POLICIES AND PROCEDURES
2019 UPDATE

(IN ACCORDANCE WITH THE 2010, 2013, 2014 & 2017,2020 HUD DATA STANDARDS)

Overview

A Homeless Management Information System (HMIS) is an information system used to record, analyze, and transmit client and activity data relating to the provision of shelter, housing, and services to individuals and families who are homeless or at risk of homelessness. Title 24 Part 580 of the Code of Federal Regulations requires a Continuum of Care (CoC) to designate a single HMIS as the official system for its geographical area and an HMIS Lead Agency to administer it. In Volusia and Flagler Counties, the Volusia/Flagler County Coalition for the Homeless (VFCCH) is the HMIS Lead, and the HMIS is ServicePoint™.

HMIS can be used to integrate and unduplicate data from all the participating agencies within a CoC. Aggregated HMIS data can help clarify the size, characteristics, and needs of the homeless population at the local, state, and national levels. HMIS enables organizations that operate homeless assistance and homelessness prevention projects to improve case management by collecting information about client needs, goals, and service outcomes. They also help to improve access to timely resource and referral information and to better manage operations.

The Volusia-Flagler HMIS project is governed by the CoC and the HMIS/Coordinated Entry Committee, comprised of representatives from every participating agency, and committed to understanding the gaps in services to consumers of the human service delivery system in an attempt to prevent and end homelessness. This group is committed to balancing the interests and needs of all stakeholders involved: homeless men, women, and children; service providers; and policy makers.

This document contains the policies, procedures, guidelines and standards that govern the operation of HMIS, as well as the roles and responsibilities for the staff of the HMIS Lead and Participating Agencies, in accordance with the HUD 2004, 2010, 2013, 2014, 2017, & 2020 Data and Technical Standards.

TABLE OF CONTENTS

Definitions

Agency Participation Agreement or HMIS Agency Participation Agreement: an agreement confirming the understanding between a Contributing HMIS Organization and the HMIS Lead to use HMIS to:

1. Collect data on the homeless population and the effectiveness of homeless programs and services.
2. Comply with reporting requirements for HUD.
3. Perform case management and referral for homeless programs of homeless

Client: An individual about whom a CHO collects or maintains personally identifiable information:

1. Because the individual is receiving, has received, may receive, or has inquired about assistance from a CHO; or
2. In order to identify needs, or to plan or develop appropriate assistance within the CoC.

Contributing HMIS Organization (CHO): an organization (including its employees, volunteers, affiliates, contractors and associates) that operates a project that contributes data to an HMIS.

End User: An employee, volunteer, affiliate, associate, and any other individual who uses or enters data in HMIS or another administrative database from which data are periodically provided to HMIS.

Homeless Management Information System (HMIS): the information system designated by the CoC to comply with the requirements of the CoC regulation 24 CFR 578. The HMIS is used to record, track, analyze and report client and activity data elated to the provision of shelter, housing and services to individuals and families who are experiencing homelessness or at risk of experiencing homelessness.

HMIS database: the database the stores information entered by Participating Agencies through the HMIS Software.

HMIS Lead: the organization designated by the CoC to administer HMIS on its behalf.

HMIS Software or HMIS: the ServicePoint™ system licensed by the CoC from Wellsky (Formerly Mediware or Bowman Systems.)

HMIS Vendor: Wellsky Systems, the licensor the of the SevicePoint™ system.

HUD: The U.S. Department of Housing and Urban Development.

Participating Agency: an agency authorized by the HMIS Lead to participate in the data collection, analysis and reporting activities of the HMIS Software System.

Protected Identifying Information (PII): information about a project participant that can be used to distinguish or trace the participant's identity, either along or when combined with other personal or identifying information using methods reasonably likely to be used, which is linkable to the project participant.

Security: protection of client and program information stored in HMIS from unauthorized access, use, or modification.

ServicePoint™: the HMIS Software licensed by the CoC from Wellsky (Formerly Mediware and Bowman Systems.)

VFCCH: the Volusia/Flagler County Coalition for the Homeless, a 501(c)(3) corporation designated as the lead agency in the two-county region to apply for and administer state and federal funds allocated to alleviate homelessness. VFCCH operates the homeless Continuum of Care (CoC) for Volusia and Flagler Counties.

Section I: HMIS GOVERNANCE

HMIS Committee

Policy: The HMIS Committee in combination with the Coordinated Entry Committee (HMIS/CE Committee), representing all stakeholders to this project, will govern and advise on all project activities.

Responsibilities: The HMIS/CE Committee advises and supports HMIS operations in the following programmatic areas: security resource development consumer involvement; and quality assurance/accountability.

Procedure:

1. The committee shall meet not less than quarterly.
2. Membership of the HMIS/CE Committee will be established according to the following guidelines:
    a. Target for membership will be an array of stakeholders that represent the CoC: to include one from each of the participating agencies;
    b. There will be a concerted effort to find replacement representatives when participation has been inactive or inconsistent from the organizations involved in the project;
3. The HMIS/CE Committee is fundamentally an advisory committee to the CoHH Board of Directors. However, CoHH Board delegates decision-making authority to the HMIS/CE Committee on certain key issues, including:
    a. Determining the guiding principles that shall underlie the implementation activities of HMIS and participating organizations and service programs
    b. Selecting the minimal data elements to be collected by all programs participating in the HMIS project;
    c. Defining criteria, standards, and parameters for the release of aggregate data and ensuring adequate privacy protection provisions in project implementation.

HMIS Management

Policy: The HMIS Management supports the operations of the HMIS according to the principles outline in the *Overview*.

Responsibilities:

1. The Executive Director of VFCCH is responsible for:
    - **a.** Oversight of all contractual agreements with funders;
    - **b.** Maintenance of written Policies and Procedures;
    - **c.** Establishing meeting and training schedules;
    - **d.** Adherence by participating agencies to the policies and procedures, as determined by the HMIS/CE Committee.
2. The HMIS System Administrator is responsible for:
    - **a.** Oversight of all day-to-day operations including technical infrastructure; planning, scheduling, and meeting project objectives; system administration; coordination with the HMIS Vendor; security; initial orientation of new agency staff.
    - **b.** Working with the HMIS Vendor to monitor the functions, performance and security of HMIS.
    - **c.** Working with the HMIS Vendor to audit the usage of HMIS and access to HMIS and the HMIS Database
    - **d.** Developing reports to present HMIS data
    - **e.** Working closely with data analysts to develop queries
    - **f.** Providing technical assistance to Participating Agencies, including on-site training
    - **g.** Technical support on a planned schedule with each Participating Agency as follows:
        - **i.** Conduct follow-up training if needed
        - **ii.** Assist with development of program specific interview protocol
        - **iii.** Provide follow-up data entry training if needed
        - **iv.** Provide on-going technical assistance as needed for implementation, reporting, training of new staff, raw data analysis, and post disaster recovery.

Requests for technical support shall be made to the System Administrator by the Agency's Executive Director or the Site Technical Administrator. The System Administrator will respond to requests for support within one business day.

SECTION 2: PARTICIPATION REQUIREMENTS

Requirements for all Participating Agencies

Policy: Participating Agencies must meet the following prerequisites before using HMIS and must maintain the agreements, standards and organizational roles on an ongoing basis. The Participating Agency will be granted access to HMIS upon execution of a Participating Agency Agreement and the satisfactory completion by new users of HMIS privacy, security and data quality training.

1. **On Site Security Assessment Meeting:** An on-site security assessment meeting must be held prior to implementation of HMIS at any agency. Participants shall include Agency Executive Director or authorized designee, and Site Technical Administrator and HMIS staff member.

2. **Participation Agreement:** Each Agency is required to sign an HMIS Participating Agency Agreement stating its commitment to implement policies and procedures for effective use of HMIS and proper collaboration with HMIS. (See attached Participating Agency Agreement, ***Appendix B***.)

3. **Definition of Agency Specific Questions:** HMIS allows each agency to define a limited number of questions that are not included in the base HMIS. The agency is responsible for defining these questions and the System Administrator is responsible for entering and maintaining them in HMIS.

4. **Identification of Referral Agencies:** HMIS provides a resource directory component that tracks service referrals for clients. Each Participating Agency shall compile a list of referral agencies and verify that the information has been entered into HMIS by the HMIS System Administrator.

5. **Identification of Site Technical Administrator:** The Participating Agency must designate one key staff person to serve as Site Technical Administrator. This person will also be responsible for additional training new staff persons on how to use the HMIS software as it pertains to their projects.

6. **Training:** The Site Technical Administrator and designated staff persons must attend HMIS training. Note: Participating Agency Staff will **NOT** be allowed to attend training until ALL Information Security paperwork, including passing a Level 2 Background Screening in accordance with Florida Administrative Code, is complete and signed by Executive Director (or designee).

7. **Conversion:** Any conversion or bridging of client data by the Participating Agency to VFCCH's HMIS software must be pre-arranged with the HMIS System Administrator. The data must be cleaned and tested prior to conversion.

8. **Coordinated Entry Data Sharing Agreements:** Coordinated Entry Data Sharing Agreements must be established between any service program where sharing of client level information will take place.

9. **Client Consent:** Client Consent Forms must be created for clients to authorize the sharing of their personal information electronically with other Participating Agencies through the HMIS software where applicable. (see attached Client Consent Form, ***Appendix C***)

HMIS Licensing and Support

1. **Software Licensing and Technical Support:** The Participating Agency will be authorized to purchase licenses for the HMIS Software and will receive technical support for HMIS from the HMIS System Administrator.

2. **Access:** The Participating Agency will be granted access to HMIS upon execution of a Participating Agency Agreement and the satisfactory completion by new users (end user) of HMIS privacy, security and data quality training, and only after Level II Background Screenings through DCF have been completed and the end-user has been deemed eligible by the Department of Children and Families (DCF) Clearing Housing shall access to HMIS be granted.

   An end-user who is found ineligible through the DCF Level II Background Screening process **will not** be granted access into HMIS until an exemption is obtained through the DCF.

Participating Agency Executive Director

Policy: The Executive Director of each Participating Agency will be responsible for oversight of all agency staff that generate or have access to client-level data stored in HMIS to ensure adherence to the HMIS operating procedures outlined in this document.

Purpose: To describe the role of the agency Executive Director with respect to oversight of agency personnel in the protection of client data within HMIS.

Responsibility: The Participating Agency's Executive Director is responsible and shall be held liable for:

1. All activity associated with agency staff access and use of HMIS.
2. Establishing and monitoring agency procedures that meet the criteria for access to HMIS, as detailed in this document.
3. Any misuse of HMIS by Participating Agency staff.
4. Authorizing access to HMIS based solely upon need, and only for those staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.
5. Ensure new users (end-users) shall have a Level II Background Screening through DCF and provide documentation to HMIS System Administrator stating that the end-user has been deemed eligible by the Department of Children and Families (DCF) Clearing Housing shall access to HMIS be granted.

   An end-user who is found ineligible through the DCF Level II Background Screening process **will not** be granted access into HMIS until an exemption is obtained through the DCF.
6. Overseeing the implementation of data security policies and standards.
7. Ensuring the integrity and confidentiality of client-level data entered into HMIS.
8. Establishing business controls and practices to ensure organizational adherence to the HMIS Policies and Procedures.

9. Communication of security requirements to agency custodians and users.

10. Authorizing data access to agency staff and assigning responsibility for custody of the data.

11. Monitoring compliance with HMIS and data access rules, and periodically reviewing control decisions.

12. Immediately informing the HMIS System Administrator of any personnel changes for agency staff with access to the HMIS data including hiring, termination or resignations, so that security of the data and the system can be maintained.

Participating Agency Site Technical Administrator

Policy: Every Participating Agency must designate one person to be the Site Technical Administrator with responsibility for the administration of HMIS within the Participating Agency.

Purpose: To outline the role of the Site Technical Administrator.

Responsibilities:

1. Maintaining agency information.
2. Granting access to HMIS for persons authorized by the agency's Executive Director.
3. Training new staff persons on the uses of HMIS including review of the Policies and Procedures in this document and any agency policies which impact the security and integrity of client information.
4. Ensuring that access to HMIS is only granted to authorized staff members after they have received training and satisfactorily demonstrated proficiency in use of the software and understanding of the Policies and Procedures and agency policies referred to above.
5. Notifying all users in their agency of interruptions in service.
6. Implementation of data security Policy and Standards, including:
    a. Administering agency-specified business and data protection controls
    b. Administering and monitoring access control
    c. Providing assistance in the backup and recovery of data
    d. Detecting and responding to violations of the Policies and Procedures or agency procedures
7. In the event that a Site Technical Administrator is unable to perform his or her duties, the HMIS System Administrator will assist the agency's Executive Director as needed.

System End-Users

Policy: All Participating Agency staff with a legitimate need to access HMIS shall be granted such access, but only for the purpose of performing the data management tasks associated with their areas of responsibility.

Procedure: The Participating Agency agrees to authorize use of HMIS only for end-users who need access to HMIS for data entry, editing of client records, viewing of client records, report writing, administration or other essential functions associated with carrying out the activities of the Participating Agency. Such end-users must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure.

Responsibility: End-Users are responsible for protecting institutional information to which they have access and for reporting security violations. End-Users must comply with the data security Policy and Standards as described in these Policies and Procedures. End-Users are responsible for their actions and for any actions undertaken with their usernames and passwords.

Coordinated Entry Data Sharing Agreements

Policy: A Participating Agency must complete the Coordinated Entry Agreement prior to sharing any Protected Identifying Information with other Participating Agencies.

Responsibility:

1. Role of Executive Director: The Executive Director is responsible for abiding by all the policies stated in any Sharing Agreement.

Procedure:

1. Executive Directors of Participating Agency wishing to participate in a data sharing agreement shall contact HMIS staff to initiate the process.
2. Written Agreement: Participating Agencies wishing to share information electronically through HMIS are required to provide, in writing, an agreement that has been signed between the Executive Directors of Participation Agencies. See attached Coordinated Entry Agreement.
3. Executive Directors complete the Coordinated Entry Agreement. Each participating agency retains a copy of the agreement and a master is kept on file by the VFCCH.
4. Site Technical Administrators receive training on the technical configuration to allow data sharing.
5. Each Client whose record is being shared must agree via a written client release of information form to have their data shared. A client must be informed what information is being shared and with whom it is being shared.

Accuracy of Data Entry

Policy: Accuracy, complete, and consistent data collection is required both by HUD Current Data Standards and to ensure the usefulness of HMIS. Participating Agencies must achieve the following level of accuracy.

1. All the Universal Data Elements listed in ***Appendix B*** must be collected, as specified in HUD Current Data Standards.
2. All names must be accurate.
3. *Program Entry Date* and *Program Exit Date* must be entered and must record the first day and last day of program service.
4. No more than 5% of data fields shall have null, blank or unknown entries.

Procedure: The HMIS Administrator and the Site Technical Administrator shall both perform regular data integrity checks on information entered into HMIS to ensure that the standards of accuracy are being met. When there are patterns of errors, HMIS end-users will be required to correct the data collection and data entry techniques and will be monitored for compliance. All HMIS users must make corrections where possible to improve the accuracy of HMIS data.

All End-Users, including Site Administrators, receive New User Training, Annual Refresher Training, Refresher Training, and System Update Training.

Site Administrators receive additional Reports Training and shall run reports every two weeks.

The HMIS System Administrator or HMIS Support Staff will provide additional training when requested or when an issue has been identified. When deemed necessary, a corrective action letter will be issued with 30-days to comply with timeline for corrective action. Failure to comply with required corrections and updates to client data may result in one of the following:

1. CoC may lose future HUD, DCF, or other grant funding due to incorrect/bad data
2. End-User locked out of HMIS
3. Agency loses funding

Information Security Protocols

Policy: Participating Agencies shall comply with minimum information security protocols to protect the confidentiality and integrity of the data. Access to client data will be tightly controlled, using security technology and restrictive access policies. Only individuals authorized to review and edit individual client data will have access to that data.

Procedure: The HMIS Vendor, HMIS Lead, and each Participating Agency will employ a variety of technical and procedural methods to ensure confidentiality and integrity of the client data:

1. **User Accounts:** User Accounts shall not be re-assigned or shared except as authorized by the HMIS System Administrator.
2. **Physical Access Restrictions:** No unsecured workstation where the HMIS Software is being used shall be left unattended. **Physical access to workstations shall be restricted so that clients and staff who are not authorized to access the HMIS cannot gain access to workstations or view records showing on screens.**
3. **Client Consent:** Client record disclosure shall be made only with written consent of the client.
4. **Reporting:** Reports generated by users of HMIS shall be subject to the same security protocols as HMIS data. Each agency is responsible for developing a secure method for storing reports.
5. **Data Disposal:** The Participating Agency agrees to dispose of documents that contain Protected Identifying Information by shredding paper records, deleting any information from diskette before disposal, and deleting any copies of client level data from the hard drive of any machine before transfer or disposal of property. The HMIS System Administrator is available to consult on appropriate processes for disposal of electronic client level data.
6. **User Access:**
    a. **Assigning User IDs and access levels:** User access and user access levels will be authorized by the Executive Director of the Participating Agency in consultation with

the Site Technical Administrator. The HMIS System Administrator will assign End-User IDs and passwords.

b. **User name format:** The HMIS System Administrator will create all user IDs using the first initial of first name and last name. Example John Doe's user ID would be jdoe. In the case where there are two people with the same first initial and last name, an additional character with be added to differentiate between users.

7. **Passwords and Password Resets:**

a. End-User IDs and Passwords are to be assigned to individuals and not shared.

b. Unique ID Password: Authorized users will be granted a unique end-user ID and password.

c. Each end-user will be required to enter an end-user ID with a Password in order to log onto the system.

d. The end-user ID will be the first initial and full last name of the user. If an end-user has a first initial and last name that is identical to a user already in the system, the end-user ID will include an additional character to differentiate.

e. The Password must be no less than eight and no more than sixteen characters in length and must include at least two numbers.

f. Discretionary Password Reset: Initially each end-user will be given a password for one time use only. The first or reset password will be automatically generated by HMIS and will be issued to the end-user by the HMIS System Administrator. Passwords will be communicated in written or verbal form.

g. If a Password is forgotten and the user has not been locked out, the user can now reset their own password by clicking on the link that says, "Forgot Password", and follow the instructions.

h. Forced Password Change will occur every forty-five days, randomly, once an end-user account is issued. Passwords will expire, and end-users will be prompted to enter a new password. Users may not use the same password consecutively but may use the same password more than once.

i. Unsuccessful logon: If an end-user unsuccessfully attempts to log on three times, the end-user ID will be "locked out", access permission revoked and unable to gain access until their password is reset in the manner stated above.

j. Termination or Extended Leave from Employment: The HMIS System Administrator shall terminate the rights of an end-user immediately upon termination from their current position. If a staff person is to go on leave for a period of longer than 45 days, their password shall be inactivated within 24 hours of the start of their leave.

a. The HMIS System Administrator is responsible for removing user end-users from the system. It is the responsibility of the Site Executive Director, or their designee, to notify the HMIS System Administrator within 24 hours when an HMIS end-user no longer requires HMIS access so the end-user account can be deactivated.

8. Access Levels: HMIS has multiple access levels that reflect the access a user has to client-level paper records. The end-user's access level shall be need-based. Need exists only for those staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities. Examples of access levels:

a. Read Only End-User: Allows the end-user to search the database of area agencies and programs and view the detail screens for each agency or program. Access to client or service records is not given.

b. Case Manager III: Will allow access to all features excluding administrative functions. They have access to all client data, including the assessments and full access to service records.

c. HMIS Site Administrator: Will allow access to all features, including agency level administrative functions. They have full reporting access but cannot access certain system-wide administrative functions. Can have access to 3rd party reporting capability in HMIS.

d. HMIS System Administrator: Will have full access to all Administrative Functions. The HMIS System Administrator maintains the HMIS Software and has access to all

reporting functions. The HMIS System Administrator will set-up new agencies, adds new users, resets passwords, and accesses other system-level options. The HMIS System Administrator orders additional User Licenses and modifies the License allocations.

9. **Location Access:** Access to HMIS will only be allowed from computers specifically identified by the Executive Director and Site Technical Administrator of the Participating Agency. Access to HMIS from unauthorized locations will be grounds for termination of HMIS software user rights.

10. **Access to Data:**

    a. **Raw Data:** Users who have been granted access to the HMIS Report Writer tool have the ability to download and save client level data to a local computer. Once this information has been downloaded from the HMIS server in raw format, the Participating Agency is responsible for the security of this data. A Participating Agency that downloads data must develop a protocol to protect this downloaded data.

    b. **Agency Policies Restricting Access to Data:** Per the HMIS Security Plan, the Participating Agencies shall establish internal access to data protocols. These policies shall include who has access, for what purpose, and how they can transmit this information. Issues to be addressed include storage, transmission and disposal of these data.

    c. **Access to Continuum-wide Data:** Access will be granted based upon policies developed by HMIS Project Committee.

11. **Access to Client Paper Records:** Participating Agencies will establish procedures to handle access to client paper records. To this end, the following procedures will be followed:

    a. Identify which staff has access to the client files, paper records, and for what Purpose. Staff shall only have access to records of clients which they directly work with or for data entry Purposes.

    b. Identify how and where client paper records are stored.

c. Develop Policy regarding length of storage and disposal procedure of client files paper records.

d. Develop Policy on disclosure of information contained in client files paper records.

12. Data Classification: All data must be classified onto one of the following categories:

a. Public Data: information that is aggregated and already published.

b. Internal Data: information scheduled, but not yet approved, for publication. Examples include draft reports, fragments of data sets, or data without context.

c. Restricted Data: information not ever scheduled for publication. Examples include data sets that are unassociated with any official project or data that have not been analyzed.

d. Confidential Data: information that identifies clients contained within the database. Examples include social security number, name, address, or any other information that can be leveraged to identify a client.

13. Physical Access Control:

a. Physical access to the system data processing areas, equipment and media must be limited. Access must be controlled for the transportation of data processing media and other computing resources. The level of control is contingent on the level of risk and exposure to loss.

b. Personal computers, software, documentation and electronic storage devices shall be secured by means that are proportionate to the threat and exposure to loss. Available precautions include equipment enclosures, lockable power switches, equipment identification and fasteners to secure the equipment.

c. The HMIS System Administrator and the Site Technical Administrators within Participating Agencies will determine the physical access controls appropriate for their organizational setting based on HMIS security policies, standards and guidelines.

d. All those granted access to an area or to data are responsible for their actions. Additionally, those granting another person access to an area are responsible for that person's activities.

e. Printed versions of confidential data shall not be left unsecured and open to unauthorized access.

f. Media (i.e. any form of data storage, including but not limited to magnetic, electronic, optical, or paper) containing personal identifying data will not be shared without the client's written consent.

g. All data must be classified public, internal, restricted, or confidential:

i. **Public Data:** Security controls are not required.

ii. **Internal Data**: Accessible only to internal employees. No auditing is required. No special requirements around destruction of these data are required. These data must be stored out of site and can be transmitted via internal or first-class mail.

iii. **Restricted Data:** Need to know access only. Requires auditing of access and must be stored in a secure location. There are not special requirements around destruction of these data. If data is mailed internally, the envelope must be labeled confidential; can be mailed first class.

iv. **Confidential Data:** Requires encryption at all times. Hard copies of these data shall never be produced. Must be magnetically overwritten and the destruction must be verified by HMIS System Administrator. This data can only be delivered by hand to data owner.

h. All data must be handled according to its classification. Failure to handle data properly is a violation of this Policy.

i. Magnetic media containing HMIS data which is released and/or disposed of by the Participating Agency and HMIS shall first be processed to destroy any data residing on that media.

14. Logical Access:

a. To prevent unauthorized use, access to computing, data communications and sensitive data resources of HMIS will be controlled limited to a user's need-to-know and need-to-use. Access is controlled through user identification and authentication. Users are responsible and accountable for work done under their personal identifiers. Access control violations must be monitored, reported and resolved.

b. All Participating Agency staff user accounts are the responsibility of the Site Technical Administrator.

c. All system accounts will be the responsibility of the HMIS System Administrator.

User Accounts

Policy: Site Technical Administrators at Participating Agencies, the HMIS System Administrator, and the HMIS Vendor must monitor access to HMIS as follows:

1. The HMIS System Administrator must regularly review end-user access privileges and remove identification codes and passwords from their systems when end-users no longer require access.

2. The HMIS System Administrator must implement discretionary access controls to limit access to HMIS information when available and technically feasible.

Procedures:

1. Access to computer terminals within restricted areas shall be controlled through a password or through physical security measures.
2. Each user shall have a unique End-User ID.
3. Passwords are the individual's responsibility, and **end-users shall not share passwords**.
4. End-Users may have to change passwords when a password expires and/or must do so at least every forty-five days if chosen randomly. They must contact the HMIS System Administrator who will assign a Temporary Password and an e-mail will be sent with Instructions to change. A password cannot be re-used until 2 password selections have expired.
5. Passwords shall be devised so they are not able to be easily guessed or found in a dictionary. The password format is alphanumeric and must contain at least two numbers.
6. Any passwords written down shall be securely stored and inaccessible to other persons.
7. **Users shall not store passwords on a personal computer for easier log on**.

Auditing: Monitoring, Violations and Exceptions

Policy: The HMIS System Administrator will monitor access to HMIS to prevent violations of information security protocols.

Violations: Any exception to the Data Security Policies and Standards not approved by the HMIS/CE Committee is a violation and will be reviewed for appropriate disciplinary action that could include termination of employment or criminal prosecution.

Exceptions: All exceptions to these Standards must be requested in writing by the Executive Director of the Participating Agency and approved by the Executive Director as appropriate as well as HMIS/CE Committee and HMIS System Administrator.

Procedure:

1. Monitoring compliance is the responsibility of the HMIS Systems Administrator in consultation with the HMIS/CE Committee.
2. All end-users and custodians are obligated to report any suspected instances of non-compliance or known security violations to the Site Technical Administrator and/or HMIS System Administrator as appropriate.
3. The HMIS/CE Committee and the HMIS System Administrator will review violations and recommend corrective and disciplinary actions.
4. The HMIS Vendor will maintain accurate logs of all changes made to the information contained within the database to maintain an audit trail of all authorized and unauthorized changes to client records. The HMIS System Administrator shall have access to those logs.

Data Integrity Controls

Policy: Controls must exist to ensure accurate and consistent data.

Responsibility: Adherence to these controls is the responsibility of the HMIS Vendor as well as ALL END-USERS of HMIS.

Procedure:

1. Data integrity controls must encompass both manual and electronic processing. Errors, duplications, omissions and intentional alterations shall be discovered and investigated. Many data integrity controls will reside within the application or system.
2. The HMIS Software will enforce referential integrity rules and constraints.
3. Only authorized personnel are permitted access to HMIS.

Right to Deny User and Participating Agency Access

Policy: Participating Agency or individual access may be suspended or revoked for suspected or actual violation of the security protocols.

Purpose: To outline consequences for failing to adhere to information security protocols. Serious or repeated violation by end-users of the system may result in the suspension or revocation of an end-user's license and/or agency's access.

Procedure:

1. All potential violations of any security and data integrity protocols will be investigated.
2. Any end-user found to be in violation of security and data integrity protocols will be sanctioned accordingly by VFCCH as per the governance of the Commission on Homelessness and Housing. Sanctions may include but are not limited to:
    a. Corrective action plan
    b. Formal letter of reprimand
    c. Suspension of system privileges
    d. Revocation of system privileges
    e. Criminal prosecution
    f. Users in violation may also be sanctioned by their agencies, which may include termination.
3. Any agency that is found to have consistently and/or flagrantly violated security protocols and/or data integrity may have its access privileges suspended or revoked, and funding sources may be notified.
4. All sanctions are imposed by the Executive Director of VFCCH.
5. Sanctions may be appealed to the HMIS/CE Committee.

Maintenance of On-Site Computer Equipment

Policy: Participating Agencies commit to a reasonable program of data and equipment maintenance in order to sustain an efficient level of system operation and must meet the technical standards for minimum computer equipment configuration, and internet connectivity.

Responsibility: The Executive Director of each Participating Agency or designee will be responsible for the maintenance and disposal of on-site computer equipment and data used for participation in the HMIS Project including the following:

1. Computer Equipment: The Participating Agency is solely responsible for maintenance of on-site computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for utilization in the HMIS Project.

2. Internet Connection: Use of HMIS requires a high-speed internet connection. The Participating Agency is solely responsible for ensuring network and internet connectivity.

3. Software: The HMIS System Administrator will assist Participating Agency staff in reporting problems with the HMIS Software to the HMIS Vendor.

Computer Virus Prevention

Policy: HMIS staff and each participating agency will take all necessary precautions to prevent any destructive or malicious program or malware from being introduced onto any computer used to access HMIS.

Procedure:

1. No un-scanned media will be introduced onto computers used to access HMIS.
2. Any computer used to access HMIS must have anti-virus software installed. Anti-virus definitions must be updated at least weekly.

SECTION 3: TRAINING

Policy: HMIS staff will maintain an on-going training schedule for Participating Agencies and all end-users must undergo security training before gaining access to the system.

Procedure: HMIS staff will prepare, publish and deliver a training program for the Participating Agencies' end-users.

Training will consist of:

1. HMIS-New User Training
   - **a.** Security
   - **b.** Ethics and Confidentiality
   - **c.** Timeliness
   - **d.** Workflows
   - **e.** Data Quality

2. Site Administrator Training
   - **a.** Review of HMIS Project data and reports for incorrect and/or insufficient data.
   - **b.** Site Administrator to correct and/or distribute reports to End-Users for updates and corrections.

3. Refresher/Overview Training
   - **a.** Assist end-users who are having issues entering, updating and correcting data in HMIS.
   - **b.** Every year, October 1, HUD issues changes and/or additional Universal Data Elements (UDE's) that must be captured in HMIS for the following fiscal year.
   - **c.** End-Users are subject to lock out of HMIS if **Mandatory Training** is not completed.

4. Approved Training:
   - **a.** Reporting
   - **b.** Coordinated Entry
   - **c.** Training that arises due to changes in funding and/or grant requirements

5. Cancellation: Participating Agencies must contact the HMIS System Administrator training coordinator within 24 hours if they are unable to attend.

SECTION 4: DATA RELEASE PROTOCOLS

Data Release Authorization and Distribution

Policy: Only de-identified data in aggregate format will be publicly released.

Procedure:

1. There will be full access to aggregate data for the all participating agencies.
2. Aggregate data will be available in the form of an aggregate report or as a raw data set.
3. Aggregate data may be made publicly available in the future.

Confidentiality and Informed Consent

Policy: To ensure client privacy, all Participating Agencies agree to abide by all privacy protection Standards and agree to uphold all Standards of privacy as established by HUD, the CoC and the HMIS/CE Committee.

Procedure:

1. **Confidentiality/Client Consent:** Informed Consent: An oral explanation shall be provided to clients when information is gathered for non-shared records. The explanation shall inform the client that the client's information will be entered into a computerized record keeping system. The Participating Agency will provide an oral explanation of the HMIS project and the terms of consent. The agency is responsible for ensuring that this procedure takes place prior to every client interview. The oral explanation shall contain, at a minimum, the following information:
    a. **What is HMIS?**
        i. HMIS is a Homeless Management Information System web-based information system that homeless services agencies across the nation are required to use if they receive HUD, CoC, or ESG funding to capture information about the clients who are homeless or at risk of homelessness they serve.
    b. **Why does this agency use HMIS?**
        i. To understand client needs

ii. To help plan programs so there are appropriate resources for the people we serve.

iii. To make it easier for clients to access resources throughout the area served by the CoC without having to complete the same paperwork over again.

iv. To provide referral to services offered by participating agencies.

v. To access information to assist clients in obtaining resources that will help them.

vi. To identify gaps

vii. To develop information to shape public policy to end homelessness.

2. **Security:** Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records.

3. **Privacy Protection:**

   a. The client signs a Release of Information (ROI), for every agency project they have accessed. Agency end-users must explain that the Homeless Management Information System is an open system which means agencies can see any/and UDE's, SPDAT's, Documents, etc. The only agency we share this data with is **Housing and Urban Development (HUD)** outside of that agency, no one else is privy to HMIS client data.

   b. The client has the right to not answer any question, unless entry into a program/project or receipt of a specific service requires the information.

   c. Client information is stored in encrypted form in the HMIS database.

   d. The client has the right to know which agency has accessed, added to, deleted, or edited the client's HMIS record.

   e. Client information transferred over the internet will be sent over a secure connection.

4. **Written Client Consent:**

   a. Each Client whose record is being shared electronically with other HMIS Participating Agency will sign A Release of Information (ROI), per program/project they access, and is a consent form to have their data shared only with participating HMIS Agencies.

b. A client must be informed about what information is being shared and with whom it is being shared.

c. Release of Information: The Participating Agency agrees not to release client identifiable information to any other organization pursuant to federal and state law without proper client consent. (see attached Client Consent Form, ***Appendix C*** and attached List of HMIS participating agency vs. non-HMIS – ***subject to change***)

5. Federal/State Confidentiality Regulations:

a. The participating Agency will uphold Federal and State Confidentiality regulations to protect client records and privacy.

b. Consent by Client: In addition, the Participating Agency will only release client records with written consent by the client, unless otherwise provided for in the regulations.

c. Federal Confidentiality Rules: The Participating Agency will abide specifically by the Federal confidentiality rules as contained in 42 CFR Part 2 regarding disclosure of alcohol and/or drug abuse records. In general terms, the Federal rules prohibit the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this Purpose. The Participating Agency understands that the Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.

d. State of Florida Confidentiality Rules: The Participating Agency will abide specifically by State of Florida general laws 163. In general, this law provides guidance for release of client level information including who has access to client records, for what purpose and audit trail specifications for maintaining a complete and accurate record of every access to, and every use of, any personal data by persons or organizations.

e. Unnecessary Solicitation: The Participating Agency will not solicit or input information from clients unless it is essential to provide services or conduct evaluation or research.

f. Encryption: The HMIS Software Vendor will store all client information in an encrypted state.

g. Authorization: All Protected Identifying Information will be inaccessible and is prohibited from accessing to end-users who have not been authorized by the client and the Participating Agency.

Interview Protocol and Universal Data Elements

Policy: Participating Agencies that collect client data through HMIS will do so according to an approved Interview Protocol that includes collection of the Universal Data Elements.

Purpose: To ensure the existence of approved interview protocols to be used by agency staff in the collection of client data through the system.

Commitment to Use of the Interview Protocol:

1. **Universal Data Elements:** The Participating Agency is responsible for ensuring that all clients are asked the set of questions to gather Universal Data Elements (see ***Appendix B***) for use in HMIS case management. These questions are available in an Interview Protocol format.

2. **Customization:** Participating Agencies may customize Interview Protocol format to meet case management needs. Participating Agencies shall work with the HMIS staff to develop a customized agency Interview Protocol or like format that contains the required Universal Data Elements.

3. **Data Entry and Data Maintenance:** Participating Agencies also agree to enter Universal Data Elements into HMIS.

Client Right to Access and Right to Deny Access to Protected Identifying Information

Policy: The HMIS retains the authority to deny access to all Protected Identifying Information contained within the system, except to the client for his/her own data. Any client may obtain, within seven business days, a printed copy of his/her own records contained in the HMIS, including a logged audit trail of changes to those records, providing the request is made in writing, and signed by the individual whose record is being requested.

Responsibility: Each Participating Agency shall designate an individual or individuals within that Agency who will be responsible for reviewing requests for release of information, and if appropriate, for granting authorization.

Procedure: Requests can only be considered for information entered by an individual agency. If services have been received from multiple agencies, the individual must request specific information entered by each specific agency. The Participating Agency may, at their own discretion, charge the client a nominal fee, not to exceed $1.00 per page, for generating a printed copy of the client's own HMIS record. If the purpose is so the client can apply for or access services outside of the HMIS Network, the Participating Agency will, upon the client's written consent, provide a complimentary copy of all or part of the client's record and also bear the cost of mailing or delivery directly to the requested service provider. No client shall have access to another 'clients records in HMIS, except if the client is also an authorized user with a Participating Agency, and then only to the extent determined by that user's security level which shall be designated by the user's Agency.

Any request for Protected Identifying Information from any person, agency, or organization other than the client himself/herself will (may) be forwarded to the HMIS System Administrator, HUD, HMIS/CE Committee for review.

Appendix A
CoC Coordinated Entry Agency Agreement

CONTINUUM OF CARE COORDINATED ENTRY AGREEMENT
BY AND BETWEEN
VOLUSIA-FLAGLER CONTINUUM OF CARE
AND
_____

This Agreement is between the FL504 VOLUSIA/FLAGLER CONTINUUM OF CARE and the Volusia Flagler County Coalition for the Homeless, Inc., a 501c3 nonprofit corporation, designated collaborative applicant and HMIS lead agency, hereinafter referred to as "CoC", and _____ ("Agency"). This Agreement is effective on the date of execution below and will remain in effect for three (3) years, unless terminated by either party with ninety (90) day written notice to the contact and address listed below. The CoC reserves the right to request Agency to enter into revisions or addendums to this Agreement as the coordinated assessment and service delivery system is implemented in Volusia and Flagler Counties, the geographic designation of the CoC.

In accordance with the U.S. Department of Housing and Urban Development (HUD) 24 CFR Part 578 that sets forth the requirement that homeless Continuums of Care develop a centralized or coordinated entry process to in aid in the operations of housing and supportive services programs to prevent and end homelessness, the parties agree as follows:

CoC and **Agency** agree to participate in the development and operations of a coordinated entry service delivery process for homeless intervention and homeless prevention services in Volusia and Flagler Counties, State of Florida.

The CoC will facilitate, maintain, evaluate and refine the coordinated entry system to include: intake, assessment, and referrals for individuals and families at-risk of or experiencing homelessness to increase access to prevention, outreach, short, medium, and long term housing, and supportive or ancillary services or benefits, including but not limited to medical care, mental health care, substance abuse treatment, day care, employment, SSI/SSDI, TANF, Snaps benefits, educational programs, or any other cash or noncash benefits.

The parties acknowledge that the objectives of the coordinated entry system include but are not limited to the following outcomes:

- Reduce the length of time clients remain homeless; the CoC through prioritization will rapidly exit people from their homelessness to stable housing
- Reduce Returns to Homelessness
- Reduce the Number of Homeless Persons
- Increase Employment and Income Change for Persons Residing in Homeless Housing Programs
- Reduce the Number of Individuals and Households Homeless for the First Time
- Prevent Returns to Homelessness

- Increase Housing Placement from Street Outreach
- Increase thoroughness in reaching homeless clients; ensures that the CoC identify the most vulnerable and ensure that the hardest to serve get served
- Collaborate with key stakeholders to set quantifiable performance goals; successful outcome measures and timeliness for success; uses HMIS data and shares/analyzes data in a transparent process

The coordinated entry system includes a comprehensive, coordinated process for people to receive outreach, prevention, housing, and/or other related services. Recent national research has highlighted coordinated entry as a key factor in the success of homelessness prevention and recovery, including but not limited to:

(a) Street Outreach programs that prioritize and target the most vulnerable unsheltered homeless and subpopulations such as chronic, veterans, and unaccompanied youth, including Projects for Assistance in Transition to Homeless (PATH) and other outreach programs.

(b) Diversion: a strategy that prevents **homelessness** for people seeking shelter by helping them identify immediate alternate housing arrangements and, if necessary, connecting them with services and financial assistance to help them return to permanent housing.

(c) Coordinated entry or intake for all individuals and families seeking homeless prevention and homeless housing and services, including implementation of a universal intake form.

(d) A region-wide process involving the coordination of nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve veterans, and homeless and formerly homeless individuals.

Agency agrees to provide outreach, prevention, housing and/or supportive services to clients referred through the CoC coordinated entry system from all participating agencies and organizations, in accordance with requirements of programs operated by the agency that are funded to serve the homeless or those at risk of homelessness.

The CoC will provide **Agency** and other providers and partners training and tools, manual or digital, to document referrals and outcomes for individuals and families served via the Homeless Management Information System or comparable database. The CoC may require reasonable fees for these services.

Agency agrees to participate in training and use tools, materials, and policies and procedures established by the CoC in the provision of the following services, as applicable to its services and programs:

A. Prevention/Rapid Rehousing - rent/mortgage assistance, utility assistance, and other expense allowable under State of Florida or U. S. Department of Housing and Urban Development or other federal agency regulations, including arrearages, security deposits, credit repair, moving costs, legal expenses.

B. Short, Medium, and Long-term Housing – emergency, transitional, permanent supportive housing

C. Medical, Mental Health or Substance Abuse treatment.

The CoC will produce and present reports to **Agency** showing the clients served, types of programs, and outcomes achieved in accordance with the Federal Strategy to Prevent and End Homelessness and the HEARTH Act. The CoC may require reasonable fees for these services.

The term of this agreement shall commence on the date of the signatures below.

IN WITNESS THEREOF, the parties have executed this Agreement.

FL-504 CoC Collaborative Applicant / (CA)	**AGENCY:**
Volusia-Flagler Coalition for the Homeless, Inc.	**_____**
Address:	**Address:**
P. O. Box 309	**_____**
Daytona Beach, FL 32115	**_____**
Signature: _____	**Signature: _____**
Print Name: Jeff White	**Print Name: _____**
Title: Executive Director	**Title: _____**
Date: _____	**Date: _____**

Appendix B

Universal Data Elements

Universal Identifier Elements

3.01 Name

3.02 Social Security Number

3.03 Date of Birth

3.04 Race

3.05 Ethnicity

3.06 Gender

3.07 Veteran Status

Universal Project Stay Elements

3.08 Disabling Condition

3.10 Project Start Date

3.11 Project Exit Date

3.12 Destination

3.15 Relationship to Head of Household

3.16 Client Location

3.20 Housing Move-In Date

3.917 Prior Living Situation

Common Program Specific Data Elements

4.02 Income and Sources

4.03 Non-Cash Benefits

4.04 Health Insurance

4.05 Physical Disability

4.06 Developmental Disability

Common Program Specific Data Elements

4.07 Chronic Health Condition

4.08 HIV/AIDS

4.09 Mental Health Problem

4.10 Substance Abuse

4.11 Domestic Violence

4.12 Current Living Situation

4.13 Date of Engagement

4.14 Bed-Night Date

4.19 Coordinated Entry Assessment

4.20 Coordinated Entry Event

Appendix C

Commission on Homelessness for Volusia and Flagler Counties
CLIENT CONSENT FOR HMIS DATA SHARING

I, _____, understand and acknowledge that the
Print client name
_____will be sharing data in the Homeless
Print name of agency

Management Information System (HMIS), with the following agency __**Volusia Flagler County Coalition for the Homeless (HMIS Lead Agency) / HUD,** and other **HMIS participating agencies** in a closed database.
I give my permission and authorize the sharing of information and records on the services provided to me between these participating agencies. The information shared by these agencies will be included in the HMIS database and will be used by these agencies to:

- Provide individual case management
- Produce aggregate-level reports regarding total services provided
- Track program-level outcomes
- Identify unfilled service needs in Volusia and Flagler counties
- Plan for new services in Volusia and Flagler counties
- Allocate resources among agencies that provide services to the homeless

I understand and agree to the following sharing of information by my initials:

____ Census information (name, birth date, gender, race, social security number, residential information, phone number and family information.

____ Financial information (income verification, public assistance payments and allowances, food stamp allotments etc.)

____ Medical information related to treatment that I am seeking and receiving, (including psychological records and evaluations, vocational assessment, care coordinators recommendations and direct observations and employment status etc.)

____ HIV/AIDS diagnosis

____ Mental health diagnosis, treatment plan, progress in treatment, discharge

____ Substance abuse diagnoses, treatment plan, progress in treatment, discharge

I understand that I have the right to make a written request for information in the Coalition for the Homeless HMIS relating to the provision of services to me.

I understand that this release can be revoked by me in writing at any time and that the revocation must be signed and dated by me. I understand that these agencies may already have taken action in reliance upon prior consent. This consent will remain valid for one year from the date signed.

I understand that my records are protected by federal, state and local regulations governing confidentiality of client records and cannot be disclosed without my written consent unless otherwise required or permitted by law.
Additionally, I understand that participation in the HMIS data sharing is optional and that I may be able to access service for which I am eligible if I choose not to participate in HMIS data sharing.

I have had this form read or explained to me as needed.

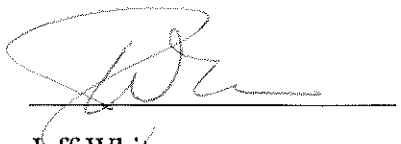
_____ _____
Client signature Date

_____ _____
Witness signature Date

HMIS Participating Agencies (updated July 2019)

Catholic Charities - St. Augustine
Catholic Charities of Central Florida
City of New Smyrna Beach
Clear Health Alliance
Community Life Center
Family Renew Community
Halifax Urban Ministries
Healthy Start of Flagler and Volusia Counties
Neighborhood Center of West Volusia
New Hope Human Services
Salvation Army
Stewart Marchman Act
VCan2020
Volusia County Government
Volusia Flagler County Coalition for the Homeless

The HMIS Policies and Procedures was reviewed and approved by the Collaborative Applicant for the HUD FL-504 CoC on October 22, 2019.



Jeff White
Collaborative Applicant
Volusia/Flagler County Coalition for the Homeless