VOLUSIA/FLAGLER COUNTY
COALITION FOR THE HOMELESS
HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)
POLICIES AND PROCEDURES
JANUARY 2014 UPDATE

(IN ACCORDANCE WITH THE 2010 AND 2013 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 (the Coalition) is the HMIS Lead, and the HMIS System is ServicePoint™.

An HMIS can be used to integrate and unduplicate data from all of 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 systems enable 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 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 the 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 and 2013 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 the HMIS System 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 and services.

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.

Coalition: the Volusia/Flagler County Coalition for the Homeless, a 503(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. The Coalition operates the homeless Continuum of Care (CoC) for Volusia and Flagler Counties.

Contributing HMIS Organization (CHO): an organization (including its employees, volunteers, affiliates, contractors and associates) that operates a project that contributes data to an 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 related 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 that stores information entered by Participating Agencies thru the HMIS Software.

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

HMIS Software or HMIS System: the ServicePoint™ system licensed by the CoC from Bowman Systems.

HMIS Vendor: Bowman Systems, the licensor of the ServicePoint™ 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 alone 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 the client and program information stored in the HMIS System from unauthorized access, use, or modification.

ServicePoint™: the HMIS Software licensed by the CoC from Bowman Systems.

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

SECTION 1: HMIS GOVERNANCE

HMIS Committee

Policy: The HMIS Committee, representing all stakeholders to this project, will govern and advise on all project activities.

Responsibilities: The HMIS 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 Committee will be established according to the following guidelines:

a. Target for membership will be 17 persons – one from each of the Phase I 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 Committee is fundamentally an advisory committee to the COALITION Board of Directors. However, the COALITION Board delegates decision-making authority to the HMIS Committee on certain key issues, including:

a. Determining the guiding principles that should underlie the implementation activities of the 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 outlined in the *Overview*.

Responsibilities:

1. The Executive Director of the Coalition 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 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 the HMIS System.

c. Working with the HMIS Vendor to audit the usage of the HMIS System and access to the HMIS System 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. Assist Participating Agencies in initial setup of computer for HMIS access.

ii. Conduct on-site follow-up training if needed

iii. Assist with development of program specific interview protocol

iv. Provide follow-up data entry training if needed

v. Review report writer

vi. Provide ongoing 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 by phone 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 the HMIS System and must maintain the agreements, standards and organizational roles on an ongoing basis. The Participating Agency will be granted access to the HMIS System 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 the HMIS System and proper collaboration with HMIS. (See attached Participating Agency Agreement, *Appendix B.*)

3. **Definition of Agency Specific Questions:** The HMIS System allows each agency to define a limited number of questions that are not included in the base HMIS System. The agency is responsible for defining these questions and the Site Technical Administrator is responsible for entering and maintaining them in the HMIS System. The HMIS Project Committee shall define the maximum number of questions that all participating agencies may ask and shall review the questions before they are approved.

4. **Identification of Referral Agencies:** The HMIS System 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 the HMIS System 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 be responsible for creating usernames and passwords and monitoring software access. This person will also be responsible for training new staff persons on how to use the HMIS software system.

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 is complete and signed by Executive Director (or designee).

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

8. **Interagency Data Sharing Agreements:** Interagency 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 system where applicable. (See attached Client Consent Form, *Appendix D*.)

10. **Interview Protocols:** The Participating Agency must identify which data elements it wants to collect in addition to the minimally required data elements established by the HMIS Steering Committee. These data elements will be available in an Interview Protocol format for use with clients during the intake/assessment process.

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 the HMIS System from the HMIS System Administrator.

2. **Access:** The Participating Agency will be granted access to the HMIS System upon execution of a Participating Agency Agreement and the satisfactory completion by new users of HMIS privacy, security and data quality training.

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 the HMIS System 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 the HMIS System.

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 the HMIS System.

2. Establishing and monitoring agency procedures that meet the criteria for access to the HMIS System, as detailed in this document.

3. Any misuse of the HMIS System by Participating Agency staff.

4. Authorizing access to the HMIS System 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. Overseeing the implementation of data security policies and standards.

6. Ensuring the integrity and confidentiality of client-level data entered into the HMIS System.

7. Establishing business controls and practices to ensure organizational adherence to the HMIS Policies and Procedures;

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

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

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

11. 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 the HMIS System within the Participating Agency.

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

Responsibilities:

1. Maintaining agency information.

2. Granting access to the HMIS System for persons authorized by the agency's Executive Director by assigning usernames and passwords.

3. Training new staff persons on the uses of the HMIS System 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 the HMIS System 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 Users

Policy: All Participating Agency staff with a legitimate need to access the HMIS System should 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 the HMIS System only for users who need access to the HMIS System 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 users must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure.

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

Interagency Data Sharing Agreements

Policy: A Participating Agency must complete the Interagency Sharing 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 Interagency Sharing Agreement.

Procedure:

1. Executive Directors 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 the HMIS System are required to provide, in writing, an agreement that has been signed between the Executive Directors of Participation Agencies. See attached Interagency Sharing Agreement.

3. Executive Directors complete the Interagency Sharing Agreement. Each participating agency retains a copy of the agreement and a master is kept on file by the COALITION.

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 consent 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: Accurate, complete, and consistent data collection is required both by HUD 2010 and 2013 Data Standards and to ensure the usefulness of the HMIS System. Participating Agencies must achieve the following level of accuracy:

1. All of the Universal Data Elements listed in Appendix C must be collected, as specified in HUD 2010 and 2013 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 should have null, blank or unknown entries.

Procedure: The HMIS Administrator and the Site Technical Administrator should both perform regular data integrity checks on information entered into the HMIS System to ensure that the standards of accuracy are being met. When there are patterns of errors, HMIS 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 HMIS data.

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 should 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 System 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 the HMIS System 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 Site Technical Administrator will assign user IDs and passwords.

b. User name format: The Site Technical 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, a sequential number should be placed at the end of the above format. Ex. JDoe2, JDoe3.

7. Passwords and Password Resets:

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

b. Each user will be required to enter a User ID with a Password in order to log onto the system.

c. User IDs and Passwords are to be assigned to individuals.

d. The User ID will be the first initial and full last name of the user. If a user has a first initial and last name that is identical to a user already in the system, the User ID will be the first initial and last name plus the number 01.

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 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 User by the Site Technical Administrator. Passwords will be communicated in written or verbal form. The first time, temporary password can be communicated via email. HMIS Staff are not available to agency staff to reset passwords. Only a Site Technical Administrator can reset a password.

g. Forced Password Change will occur every forty-five days once a user account is issued. Passwords will expire and 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.

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

i. Termination or Extended Leave from Employment: The Site Technical Administrator should terminate the rights of a 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 should be inactivated within 24 hours of the start of their leave. The Site Technical Administrator is responsible for removing users from the system. The Site Technical Administrator must update the access list and signed agreement on a quarterly basis.

8. Access Levels: An HMIS system has multiple access levels that reflect the access a user has to client-level paper records. The user's access level should 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. Resource Specialist: allows the 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. A low-level Resource Specialist may be given "read-only" access to data and higher-level Resource Specialists may modify or delete agency and program data. Access may be limited to a particular agency or granted across the entire continuum.

b. Volunteer: may view or edit basic demographic information about clients (the profile screen), but is restricted from viewing detailed assessments. A volunteer can enter new client records, make referrals, or check-in/out a client from a shelter. Normally, this access level allows a volunteer to complete an intake and then refer the client to agency staff or a case manager.

c. Agency Staff: has access to agency and program data, but limited access to client data. Agency Staff can only access basic demographic data on clients. All other screens are restricted, including assessments and case plan records. They have full access to service records and most functions regarding service data. There is no reporting access.

d. Case Manager: has access to all features excluding administrative functions. They have access to all client data, including the assessments and full access to service records. There is full reporting access with the exception of system audit reports.

e. Agency Administrator: has access to all features, including agency level administrative functions. This level can add/remove users for his/her agency and

edit the agency and program data. They have full reporting access, but cannot access certain system-wide administrative functions.

f. **Executive Director:** same access rights as an Agency Administrator, but ranked above Agency Administrator, meaning an Executive Director could grant or terminate an Agency Administrator's rights.

g. **System Operator:** maintains the HMIS Software, but does not have access to any Client or Service Records. Has no access to reporting functions, but does have access to administrative functions. The System Operator sets up new agencies, adds new users, resets passwords, and accesses other system-level options. The System Operator orders additional User Licenses and modifies the License allocations.

h. **System Administrator:** has the same access rights to client information (full access) as Agency Administrator. However, also has full access to administrative functions.

9. **Location Access:** Access to the HMIS system 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 system user rights.

10. **Access To Data:**

a. **User Access:** Users will only be able to view data for their own Participating Agency unless a data sharing agreement has been executed. This restriction is enforced by the HMIS Software and the HMIS Vendor.

b. **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 from the Report Writer must develop a protocol to protect this downloaded data.

c. **Agency Policies Restricting Access to Data:** The Participating Agencies shall establish internal access to data protocols. These policies should 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.

d. **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 paper records and for what Purpose. Staff should 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 paper records.

    d. Develop Policy on disclosure of information contained in client 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 diskettes 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 should 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 is 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 should 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 should 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 the HMIS System 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 System as follows:

1. Site Technical Administrators at Participating Agencies and the HMIS System Administrator must regularly review user access privileges and remove identification codes and passwords from their systems when users no longer require access.

2. Site Technical Administrators at Participating Agencies and the HMIS System Administrator must implement discretionary access controls to limit access to HMIS information when available and technically feasible.

3. The HMIS Vendor must audit all access to the HMIS System and maintain audit records for at least six months. Site Technical Administrators and the HMIS System Administrator will regularly review the audit records for evidence of violations or system misuse.

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 User ID.

3. Passwords are the individual's responsibility, and users shall not share passwords.

4. Users shall select and change their own passwords, and must do so at least every forty-five days. 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 the HMIS System to prevent violations of information security protocols.

Violations: Any exception to the data security policies and Standards not approved by the HMIS System Administrator 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 Committee and HMIS System Administrator.

Procedure:

1. Monitoring compliance is the responsibility of the HMIS Systems Administrator in consultation with the HMIS User Group.

2. All users and custodians are obligated to report any suspected instances of noncompliance or known security violations to the Site Technical Administrator and/or HMIS System Administrator as appropriate

3. The HMIS Project Group 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 users of the HMIS System.

Procedure:

1. Data integrity controls must encompass both manual and electronic processing. Errors, duplications, omissions and intentional alterations should 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 the HMIS System.

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 users of the system may result in the suspension or revocation of an agency's access.

Procedure:

1. All potential violations of any security protocols will be investigated.

2. Any user found to be in violation of security protocols will be sanctioned accordingly by the Coalition. Sanctions may include but are not limited to: a formal letter of reprimand, suspension of system privileges, revocation of system privileges, and criminal prosecution. 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 may have its access privileges suspended or revoked, and funding sources may be notified.

4. All sanctions are imposed by the Executive Director of the Coalition.

5. Sanctions may be appealed to the HMIS 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 the HMIS System 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 the HMIS System.

Procedure:

1. No unscanned media will be introduced onto computers used to access the HMIS System.

2. Any computer used to access the HMIS System must have anti-virus software installed. Anti-virus definitions must be updated at least weekly.

SECTION 3: TRAINING

Policy: HMIS staff will maintain an ongoing training schedule for Participating Agencies and all 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' users. The schedule will be published and offered on a regular basis. The training will consist of:

1. Basic: Introduction to HMIS
   - **a.** Introduction to the HMIS Project
   - **b.** Review of applicable policies and procedures
   - **c.** Connecting to the Internet
   - **d.** Logging on to HMIS
   - **e.** Entering client information including demographic, services, bed register, HUD worksheet and goals and outcomes.
   - **f.** Ethics and confidentiality

2. Intermediate: Site Technical Administrator Training
   - **a.** Overview of HMIS Project
   - **b.** Review of agency technical infrastructure including roles and responsibilities
   - **c.** Review of security policies and procedures
   - **d.** Overview of system administrative functions
   - **e.** Setting up users and assigning access levels
   - **f.** Entering and updating information pertaining to the participating agency
   - **g.** Review of HMIS technical infrastructure

3. Advanced: Reporting with HMIS
   - **a.** Introduction to the report writing tool
   - **b.** Using existing reports
   - **c.** Creating new reports
   - **d.** Exporting information to other software applications

4. Approved Training
   - **a.** Only HMIS staff or individuals certified by HMIS staff, such as trained Site Technical Administrators will deliver training sessions.
   - **b.** Participating Agencies will receive information regarding training sessions based on their prioritization in the HMIS implementation plan.

c. Enrollment: All users must be registered with the designated HMIS Systems Administrator. Users not registered for a training session will be denied access to the session.

d. Cancellation: Participating Agencies must contact the HMIS 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. Program-specific information will not be released without the written consent of the Participating Agency Executive Director.

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 the CoC and the HMIS 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?**
        - HMIS is a web based information system that homeless services agencies across the nation are required to use to capture information about the clients they serve.

    b. **Why does this agency use HMIS?**
        - To understand client needs.
        - To help plan programs so there are appropriate resources for the people we serve.
        - 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.
        - To provide referral to services offered by participating agencies.
        - To access information to assist clients in obtaining resources that will help them.
        - 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. No information will be released to another agency without the client's written consent, except as allowed by law, including but not limited to properly executed subpoenas, and subject to notification of all Participating Agencies.

b. The client has the right to not answer any question, unless entry into a program 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 another Participating Agency must agree via a written client consent form to have their data shared.

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

c. Information Release: 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.

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 to 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 the HMIS System 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 C*) for use in 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 the HMIS System.

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 three 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 the HMIS System, 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 be forwarded to the HMIS Committee for review.

Appendix A - HMIS Project Documentation Checklist for Security Assessment Meeting

Program Name: _____ **Date:** _____

Meeting Attendees: _____

Check the following when paperwork is completed. Leave one copy with the program and return one copy to the HMIS office.

Participation Requirements

Initial Implementation Requirements

Agreement for Transfer of Data

Data Sharing Yes No

If yes, with what other agencies? _____

Interagency Data Sharing Agreement

Client Consent Form

Discussion of minimal data elements and interview protocol:

HMIS Interview Guide, with 25 customized questions

Minimal Data Elements – for families; for individuals

Discussion of Security and Privacy Protections:

HMIS User Access Form

Agency Procedures for Discipline

Appendix B

HMIS Participating Agency Agreement

This HMIS Participating Agency Agreement is between the Volusia/Flagler County Coalition for the Homeless (the "Coalition") and the Contributing HMIS Organization:

The Coalition is the HMIS Lead Agency for the FL 504 Continuum of Care (the "CoC"). This HMIS Participating Agency Agreement sets forth the roles and responsibilities of both parties with regard to the implementation and use of the Homeless Management Information System ("HMIS").

The Coalition will serve as the administrator for the HMIS provided by U.S. Department of Housing and Urban Development ("HUD") funds and will assume the responsibilities in association with federal, state and local laws and requirements. The Coalition will:

1. Ensure the operation of HMIS and participation by recipients of HUD funds and other funding sources that require participation in HMIS.

2. Develop a written Policies and Procedures Manual for the operation and maintenance of HMIS.

3. Monitor participation for consistency and adherence to the Data Quality Plan, the Security Plan, and Privacy Plan as outlined in the Policies and Procedures Manual.

4. Conduct data entry training and annual security and privacy training for all CHOs as required.

5. Conduct oversight of HMIS participation to ensure compliance with HUD regulations and take corrective action, if needed.

6. Report to the CoC on the state of HMIS with regard to participation, data quality, and compliance.

7. Submit HMIS reports to HUD as required.

As a Contributing HMIS Organization ("CHO"), _____ agrees to partner with the Coalition in support of HMIS for the CoC. The CHO will:

1. Contribute data to the HMIS in accordance with minimal requirements as outlined in the HMIS Policies and Procedures manual and the Homeless Management Information System Data Standards, released March 2010.

2. Designate a CHO staff member to serve as Site Technical Administrator and provide contact information to the HMIS Lead Agency.

3. Ensure that all CHO staff members who contribute data to the HMIS receive training as outlined in the Policies ands Procedures Manual.

4. Implement the standard intake form developed by the CoC or develop an agency-specific intake form that captures all required data elements as outlined in the HMIS Data Standards and submit the form to the CoC to verify compliance.

5. Comply with all data entry, security and privacy policies as outlined in the HMIS Policies and Procedures Manual.

6. Ensure that the HMIS processing capabilities used by the CHO remain consistent with the privacy obligations of the CHO and collaborate with the HMIS Lead Agency to adjust HMIS processes as needed.

7. Ensure that all HMIS users within the CHO have received unique HMIS User IDs and passwords.

8. Report any staff changes that impact HMIS to the HMIS Lead Agency immediately.

9. Comply with the roles and responsibilities set forth in this HMIS Participating Agency Agreement.

Neither the CHO nor the HMIS Lead Agency may transfer the rights and responsibilities outlined in this agreement without the written consent of the other party. This Participating Agency Agreement will be in force until revoked in writing by either party and then will be terminated within 30 days of written notice by the CHO or the HMIS Lead Agency.

This agreement will be reviewed and renewed annually, in accordance with federal regulations.

By signing this document, I agree to abide by all policies as stated in the Coalition HMIS Policies and Procedures. I also agree to educate all staff members in my agency as to the policies that directly affect their work.

Agency Executive Director Printed Name _____ Date _____

Signature _____

HMIS Lead Agency Executive Director Printed Name _____ Date _____

Signature _____

Appendix C

Universal Data Elements

1. Name
2. Social Security Number
3. Date of Birth
4. Race
5. Ethnicity
6. Gender
7. Veteran Status
8. Disabling Condition
9. Residence Prior to Project Entry
10. Project Entry Date
11. Project Exit Date
12. Destination
13. Personal Identification Number
14. Household Identification Number
15. Head of Household
16. Length of Time Homeless

Appendix D – Client Informed Consent and Release of Information Form

Volusia/Flagler County Coalition for the Homeless
HMIS Client Consent Form
Authorization for Release of Information

Agency Name _____

Client Name _____

Dependent children, if any (first and last names and date of birth)

_____

_____

_____

I know that this agency is a Partner Agency in the Homeless Management Information System (HMIS). The HMIS is a shared homeless and housing information system administered by the Volusia/Flagler County Coalition for the Homeless. It can improve the services and programs for homeless and low income households by allowing authorized staff at Partner Agencies to share client information and to follow trends and service patterns over time. The HMIS operates over the internet and uses many security protections to ensure confidentiality.

Participation in the HMIS program is important to our community's ability to provide you with the best services and housing possible. As you receive services, information will be collected about you, the services provided to you, and the outcomes these services help you to achieve.

- Your name and other identifying information will not be shared with any agency not participating in the system (unless required to do so by law.)
- Your name, gender, race, social security number and date of birth may be shared with Partner Agencies for Identification purposes even if you elect not to share other relevant information.
- Sensitive information such as diagnosis or treatment or mental health disorders, drug or alcohol disorders, HIV/AIDS, or domestic violence concerns, will not be shared between Partner Agencies without specific written consent.
- A list of Partner Agencies is available upon request.
- Authorizing your information to be entered into the HMIS is voluntary. Refusing to do so will not limit your access to shelter or services.

I understand that:

- I may cancel this authorization at any time by written request, but the cancellation will not be retroactive.
- I have the right to see my HMIS record, ask for changes, and to have a copy of my record from this agency upon written request.
- Participation in data collection is optional and will not limit my access to shelter and housing services if I choose not to participate in data collection. *This does not override this agency's active policies or intake procedures.*
- This release is valid for 5 years from the date of my signature.

Please initial one of the following levels of consent:

____(1) I give authorization for my basic and relevant information to be entered into the HMIS and shared among Partner Agencies.

____(2) I give authorization for my basic and relevant information to be entered into the HMIS, but not shared among Partner Agencies.

_____		_____	
Client Signature	Date	Agency Witness	Date