

**VOLUSIA/FLAGLER COUNTY
COALITION FOR THE HOMELESS
HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)
POLICIES AND PROCEDURES
December 2004**

Introduction

The Volusia/Flagler County Coalition for the Homeless (Coalition) is the administrator responsible for the implementation of the Homeless Management Information System (HMIS) for the two-countywide area. The project utilizes Internet-based technology to assist service organizations to capture information about the clients that they serve. Originally, The Coalition entered into an agreement with the Homeless Services Network (HSN) to provide software technology. As the Coalition grew the Coalition added a full-time Administrator of its HMIS, ended its user agreement relationship with HSN and entered into an License and Support Agreement with Domus Systems, Inc. The Coalition System Administrator will provide training and technical assistance to users of the system throughout Volusia and Flagler county area.

A goal of the Coalition HMIS Project is to inform public policy makers about the extent and nature of the uninsured and homeless population in the Volusia and Flagler County area of Florida. This is to be accomplished through analysis and release of data that are grounded in the actual experiences of uninsured and homeless and the service providers who assist them. Information that is gathered will be analyzed for an unduplicated count, aggregated (void of any identifying client level information) and made available to Policy makers, service providers, advocates, and consumer representatives.

The Coalition HMIS project is advised by 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 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.

Potential benefits for Clients and case managers: Case managers can use the software as they assess their clients' needs to inform clients about services offered on site or available through referral. Case managers and clients can use on-line resource information to learn about resources that help clients find and keep permanent housing or meet other goals clients have for themselves. Service coordination can be improved when information is shared among case management staff within one agency or with staff in other agencies (with written client consent) who are serving the same clients.

Potential benefits for agency and program managers: When aggregated, information can be used to provide a more complete understanding of clients' needs and outcomes, and then used to advocate for additional resources, complete grant applications, conduct evaluations of program services, and report to funders such as HUD. The software has the capability of generating the revised HUD Annual Progress Report (APR).

Potential benefits for community-wide Continuums of Care and policy makers: Involvement in the project provides the capacity to programs within a Continuum to generate automated HUD APRs, to access aggregate reports that can assist in completion of the HUD-required gaps chart, and to utilize the aggregate data to inform Policy decisions aimed at addressing and ending homelessness at local, state and

federal levels. The HSN administers the COALITION HMIS limiting access to the database to programs participating in the project.

This document provides the policies, procedures, guidelines, and standards that govern as well as roles and responsibilities for COALITION HMIS and participating agency staff. Participating agencies will receive all relevant portions of the complete document, with the exception of those procedures that, if disseminated, would compromise the underlying security features of the COALITION HMIS and overall system.

Governing Principles

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

Data Integrity: Data is the most valuable asset of the COALITION HMIS Project. It is our Policy to protect this asset from accidental or intentional unauthorized modification, disclosure or destruction.

Our data security program must be a well-organized and cost-effective plan, which formulates the safeguards to protect client, agency, and Policy level interests. The COALITION HMIS System Administrator and trained agency administrative staff are responsible for controlling access to the system.

Access to Client Records: The Client Records Access Policy is designed to protect against the recording of information in unauthorized locations or systems. Only staff who work directly with clients or who have administrative responsibilities will receive authorization to look at, enter, or edit client records. Additional privacy protection policies include:

No client records will be shared electronically: No client records will be shared electronically with another agency without written client consent.

End User Ethics: Any deliberate action that adversely affects the resources of any participating organization or institution or employees is prohibited. Any deliberate action that adversely affects any individual is prohibited.

Users shall not use COALITION HMIS for personal purposes.

Users shall not attempt to gain physical or logical access to data or systems for which they are not authorized.

Users shall not attempt to reverse-engineer commercial software.

Users shall follow security guidelines of this policy.

Introduction	1
SECTION 1: Contractual Requirements and Roles.....	5
Title: COALITION HMIS CONTRACT REQUIREMENTS	6
Title: COALITION HMIS NEW SITES REQUIREMENTS	7
Title: STEERING COMMITTEE	8
Title: COALITION HMIS MANAGEMENT	9
Title: ROLE: PARTICIPATING AGENCY EXECUTIVE DIRECTOR.....	10
Title: PARTICIPATING AGENCY SITE TECHNICAL ADMINISTRATOR.....	11
Title: SYSTEM USERS.....	12
SECTION 2: Participation Requirements	13
Title: PARTICIPATION REQUIREMENTS.....	14
Title: IMPLEMENTATION REQUIREMENTS	15
Title: INTERAGENCY DATA SHARING AGREEMENTS	16
Title: CONFIDENTIALITY AND INFORMED CONSENT	17
Title: INTERVIEW PROTOCOL AND COMMON DATA ELEMENTS	20
Title: INFORMATION SECURITY PROTOCOLS	21
Title: RIGHT TO DENY USER AND PARTICIPATING AGENCIES' ACCESS	27
Title: MAINTENANCE OF ONSITE COMPUTER EQUIPMENT	28
SECTION 3: Training	29
Title: TRAINING.....	30
Title: AUDITING: MONITORING, VIOLATIONS AND EXCEPTIONS.....	33
Title: DATA INTEGRITY CONTROLS	34
SECTION 4: Stages of Implementation.....	35
Title: IMPLEMENTATION STAGE 1: START-UP AND INITIAL TRAINING	36
Title: IMPLEMENTATION STAGE 2: DATA ENTRY BEGINS	37
Title: IMPLEMENTATION STAGE 3: BASIC INFORMATION ON 90% OF CURRENT CLIENTS	38
Title: IMPLEMENTATION STAGE 4: SYSTEM FULLY INTEGRATED IN DAILY OPERATION	39
SECTION 5: Data Release Protocols.....	40
Title: DATA RELEASE AUTHORIZATION AND DISTRIBUTION.....	41
Title: CLIENT RIGHT TO ACCESS and RIGHT TO DENY ACCESS TO CLIENT IDENTIFIED INFORMATION.....	42
SECTION 6: Internal Operating Procedures	43
Title: COMPUTER VIRUS: PREVENTION	44
Appendix: Sample Forms	45

SECTION 1: Contractual Requirements and Roles

HMIS-001 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: COALITION HMIS CONTRACT REQUIREMENTS

Policy: COALITION HMIS is committed to providing services to social service agencies providing direct services to homeless clients in Volusia and Flagler Counties.

Purpose: To delineate the responsibilities of the Coalition in initiating and maintaining a Continuum-wide HMIS and to set forth basic requirements for participating Agencies.

Basic Requirements:

1. **Purchase of Software Licensing and Technical Support:** All existing and new sites participating in the COALITION HMIS Project that enter into a Memorandum of Understanding with the Coalition (MOU) shall be authorized to purchase licenses and shall receive technical support for the HMIS system from the Coalition's System Administrator. In 2004, the Coalition has received HUD Supportive Housing Program funds to initiate a Continuum-wide HMIS project. The following agencies shall be entitled PHASE 1 HMIS Users, and shall each receive one complete computer package that will include a printer/scanner and shall receive one software license at no cost. All participating Agencies are responsible for all costs associated with hardware maintenance, technical support for non-HMIS software, personnel, and Internet access.
2. **Access:** No Agency will be granted access to the HMIS software system until a Memorandum of Understanding has been signed with COALITION HMIS and Agency staff that will be provided access to the system have completed Ethics and Confidentiality Training.
3. **Phase I HMIS Agencies:** The following agencies are designated Phase I, for initiation of the HMIS Project which is to take place in the year July 1, 2004 – June 30, 2005:
 - a. ACT Corporation
 - b. AIDS Coalition of Volusia/Flagler
 - c. Domestic Abuse Council
 - d. Family Life Center
 - e. Family Renew Community
 - f. Flagler County Community Services Dept.
 - g. Halifax Urban Ministries
 - h. Mental Health Association
 - i. Mid-Florida Housing Partnership
 - j. Neighborhood Center of West Volusia
 - k. Saint Barnabas
 - l. Salvation Army
 - m. Serenity House
 - n. Stewart Marchman
 - o. Volusia County Community Services Dept.
 - p. Volusia/Flagler County Coalition for the Homeless, HAC
 - q. United Way of Volusia/Flagler County

HMIS-002 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: COALITION HMIS NEW SITES REQUIREMENTS

Policy: COALITION HMIS is committed to provide HMIS service to social service agencies who deliver services to the homeless, and who may wish to join the system after June 30, 2005.

Purpose: To outline the Basic Requirements for new agencies that wish to use COALITION HMIS services after June 30, 2005.

Basic Requirements:

1. **Purchase of Software Licensing and Technical Support:** All new sites participating in the COALITION HMIS Project who are not funded by HUD SHP will be required to purchase user licenses for HMIS and, and pay for Technical Assistance from COALITION HMIS.
2. **Access:** New Participating Agencies will be granted access to the HMIS software system when a contract including software licensing fees and technical support has been executed, a Memorandum of Understanding has been signed with COALITION HMIS and Agency staff that will be provided access to the system have completed Ethics and Confidentiality Training.
3. No Agency will be granted access to the HMIS software system until a Memorandum of Understanding has been signed with COALITION HMIS and Agency staff that will be provided access to the system have completed Ethics and Confidentiality Training.

HMIS- 003 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: STEERING COMMITTEE

Policy: An HMIS Project Committee, representing all stakeholders to this project will advise all project activities.

Purpose: To define the roles and responsibilities of the HMIS Project Committee.

Responsibilities:

The HMIS Project Committee advises and supports the COALITION HMIS operations in the following programmatic areas: Security, resource development; consumer involvement; and quality assurance/accountability. The committee shall meet not less than quarterly.

1. Membership of the HMIS Project Committee will be established according to the following guidelines:
2. Target for membership will be 17 persons – one from each of the Phase I agencies;
3. There will be a concerted effort to find replacement representatives when participation has been inactive or inconsistent from the organizations involved in the project;
4. The HMIS Project Committee is fundamentally an advisory committee to the COALITION Board of Directors.
5. 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 COALITION HMIS and participating organizations and service programs;
 - b. Selecting the minimal data elements to be collected by all programs participating in the COALITION HMIS project;
 - c. Defining criteria, standards, and parameters for the release of aggregate data and ensuring adequate privacy protection provisions in project implementation.

HMIS- 004 Effective date: Prepared by: COALITION HMIS Policy Group
Revision: Revision date: Revised by:

Title: COALITION HMIS MANAGEMENT

Policy: A COALITION HMIS management structure will be put into place that can adequately support the operations of the COALITION HMIS according to the Guiding Principles described in the Introduction.

Purpose: To define the roles and Responsibilities of the COALITION HMIS organization and staff.

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 Guiding Principles, as determined by the HMIS Project Committee.

2. The COALITION 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 HMIS software provider; security; initial orientation of new agency staff.
 - b. Monitoring functionality, speed, database backup procedures
 - c. Auditing usage and access of the database
 - d. Developing reports to present the data
 - e. Working closely with data analysts to develop queries
 - f. Documenting work on the database and in development of reports/queries
 - g. Provision of technical assistance to HMIS sites including on-site training
 - h. Technical support on a planned schedule with each participating agency as follows:
 - i. Assist Participating Agencies in initial set up of computer.
 - 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 Systems Administrator by the Agency's Executive Director or the Site Technical Administrator. System Administrator will respond by phone within one business day

HMIS- 005 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: ROLE: 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 system software to ensure adherence to the COALITION HMIS Standard operating procedures outlined in this document.

Purpose: To outline the role of the agency Executive Director with respect to oversight of agency personnel in the protection of client data within the system software application.

Responsibilities:

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 software data system;
2. Establishing and monitoring agency procedures that meet the criteria for access to the HMIS software system, as detailed in the Policies and Procedures outlined in this document;
3. Any misuse of the software system by his/her designated staff;
4. Allowing access to the HMIS Software system based solely upon on need, and 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.
5. Overseeing the implementation of data security policies and standards;
6. Integrity and protection of client-level data entered into the HMIS system;
7. Establishing business controls and practices to ensure organizational adherence to the COALITION HMIS Policies and Procedures;
8. Communication of control and protection requirements to agency custodians and users;
9. Authorizing data access to agency staff and assigning responsibility for custody of the data;
10. Monitoring compliance and periodically reviewing control decisions;
11. Immediately informing the Coalition Executive Director 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.

HMIS-006 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: 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 system software in his/her agency.

Purpose: To outline the role of the Site Technical Administrator

The Participating Agency agrees to appoint one person as the Site Technical Administrator. This person will be responsible for:

1. Editing and updating agency information;
2. Granting technical access to the software 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 software 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 System Administrator will assist the agency's Executive Director as needed.

HMIS-007 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: SYSTEM USERS

Policy: All individuals at the COALITION HMIS and at the Participating Agency levels who require legitimate access to the software system will be granted such access for the purpose of conducting data management tasks associated with their area of responsibility.

Purpose: To outline the role and responsibilities of the system user.

The COALITION HMIS agrees to authorize use of the HMIS Software system only to users who need access to the system for technical administration of the system, report writing, data analysis and report generation, back-up administration or other essential activity associated with COALITION HMIS.

Responsibilities:

The Participating Agency agrees to authorize use of the HMIS Software system only to users who need access to the system for data entry, editing of client records, viewing of client records, report writing, administration or other essential activity associated with carrying out participating agency responsibilities.

Users are any persons who use the HMIS software for data processing services. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure.

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. They are accountable for their actions and for any actions undertaken with their usernames and passwords.

SECTION 2: Participation Requirements

HMIS-008 Effective date: Prepared by: COALITION HMIS Policy Group
Revision: Revision date: Revised by:

Title: PARTICIPATION REQUIREMENTS

Policy: COALITION HMIS staff will communicate requirements for participation to ensure that all sites receive the benefits of the system while complying with all stated policies. All requirements for participation are outlined in this document.

Purpose: To provide the structure of on-site support and compliance expectations.

Participation Agreement Requirements:

1. Internet Connection 56k/v90, DSL, Cable, etc.
2. Identification of Site Technical Administrator: Designation of 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 system.
3. Security Assessment: Meeting of Agency Executive Director (or designee), Site Technical Administrator with COALITION HMIS staff member to assess and complete Agency Information Security Protocols. See attached Initial Implementation Requirements.
4. Training: Commitment of Site Technical Administrator and designated staff persons to attend training. Note: Staff will NOT be allowed to attend training until ALL Information Security paperwork is complete and signed by Executive Director (or designee).
5. Conversion: Any conversion or bridging of client data by any Agency to the Coalition's HMIS must be pre-arranged through the Coalition System Administrator and must be cleaned and updated prior to conversion.
6. Interagency Data Sharing Agreements: Interagency Data Sharing Agreements must be established between any service program where sharing of client level information is to take place. See attached Interagency Data Sharing Agreement.
7. 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.
8. Interview Protocols: Agencies must identify which data elements they wish to collect in addition to the minimally required data elements established by the COALITION HMIS Steering Committee. These data elements will be available in an Interview Protocol format for use with clients during the intake/assessment process. See attached Interview Guide.
9. Participation Agreement: Agencies are required to sign a participation agreement stating their commitment to develop the policies and procedures for effective use of the system and proper collaboration with COALITION HMIS. See attached Initial Implementation Requirements.

HMIS- 009 Effective date: Prepared by: COALTION HMIS Policy Group
Revision: Revision date: Revised by:

Title: IMPLEMENTATION REQUIREMENTS

Policy: All Participating Agencies must read and understand all participation requirements and complete all required documentation prior to implementation of the system.

Purpose: To indicate documentation requirements prior to implementation.

1. **On Site Security Assessment Meeting:** To assist in completion of Agencies Information Security Protocols, an on-site security assessment meeting shall be held prior to implementation of HMIS at any agency. Participants shall include Agency Executive Director or authorized designee, and Site Technical Administrator and COALITION HMIS staff member.
2. **Participating Agreement:** Refers to the document agreement made between the participating agency and the COALITION. This agreement includes commitment to enter information on a representative portion of clients served within the agencies' participating programs. This document is the legally binding document that refers to all laws relating to privacy protections and information sharing of client specific information. See attached Initial Implementation Requirements.
3. **Agency Participation/Data Sharing Agreements:** Upon completion of the Security Assessment, each agency must agree to abide by all policies and procedures laid out in the COALITION HMIS Security Matrix. The Executive Director or designee will be responsible for signing this form. See attached Initial Implementation Requirements.
4. **Agency Specific Information:** Each participating Agency shall complete specific questions prior to the use of the system.
5. **Definition of Agency Specific Questions:** HMIS software provides the flexibility for each agency to define a limited number of questions that are not included in the software. The agency is responsible for defining these questions and the Site Technical Administrator is responsible for entering them into and administering them within HMIS. 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.
6. **Identification of Referral Agencies:** HMIS software 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 software by the System Administrator.

HMIS-010 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: INTERAGENCY DATA SHARING AGREEMENTS

Policy: Data sharing among agencies will be supported upon completion of Interagency Sharing Agreements by Participating Agencies wishing to share client identified data.

Purpose: To explain the means through which agencies can enter into an agreement allowing the sharing of client records.

Responsibilities:

1. 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.
2. 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 COALITION HMIS staff to initiate the process.
2. 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.
3. Site Technical Administrators receive training on the technical configuration to allow data sharing.
4. 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.

HMIS-011 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: CONFIDENTIALITY AND INFORMED CONSENT

Policy: To ensure protection of clients' privacy, all Participating Agencies agree to abide by all privacy protection Standards and agree to uphold all Standards of privacy as established by the COALITION HMIS organization.

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 their information will be entered into a computerized record keeping system. The Participating Agency will provide an oral explanation of the COALITION 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 Counties 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 encrypted at HMIS.
- d. The client has the right to know which agency has accessed, added to, deleted, or edited their HMIS record.
- e. Information that is transferred over the web is through 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. In addition, the Participating Agency will only release client records with written consent by the client, unless otherwise provided for in the regulations.
- c. 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. 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 Participating Agency understands that the COALITION HMIS Project will maintain the server, which will contain all client information in an encrypted state. All client identifiable data is inaccessible to unauthorized users who have not been authorized by the owner/creator of that information.

HMIS-012 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: INTERVIEW PROTOCOL AND COMMON DATA ELEMENTS

Policy: Participating Agencies that collect client data through this Management Information system will do so according to an approved Interview Protocol.

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

Procedure:

Commitment to Utilization of the Interview Protocol

- a) Common Data Elements: The Participating Agency is responsible for ensuring that all clients are asked the set of questions entitled Common Data Elements for use in case management. These questions are available in an Interview Protocol format.
- b) Customization: Participating Agencies may customize Interview Protocol format to meet case management needs. Participating Agencies shall work with the COALITION HMIS staff to develop a customized agency Interview Protocol or like format that contains the required Common Data Elements.
- c) Data Entry and Data Maintenance: Participating Agencies also agree to enter Common Data Elements into the HMIS software system.

HMIS-013 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: INFORMATION SECURITY PROTOCOLS

Policy: Participating Agencies shall comply with minimum information security protocols to protect the confidentiality of the data and ensure its integrity at the site. The COALITION is responsible for ensuring that updated security measures are in place for all data stored on the server. 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. The COALITION HMIS and each participating agency will employ a variety of technical and procedural methods to ensure that only authorized individuals have access to individual client data.

Procedure:

No re-assignment shall be made of user accounts except with authorization from the Coalition HMIS staff.

1. No unsecured workstation where HMIS is being used shall be left unattended.
2. Physical access to workstations shall be restricted such that clients and staff not authorized to access HMIS cannot gain access to workstations or view records showing on screens.
3. User accounts shall not be shared, except as authorized by Coalition HMIS staff.
4. Client record disclosure shall be made only with written consent of the client.
5. Reports generated by HMIS staff shall be subject to the same security protocols as HMIS data. Each agency is responsible for developing a secure method for storing reports.
6. Data Storage: The Participating Agency agrees to only download and store data in a secure format.
7. Data Disposal: The Participating Agency agrees to dispose of documents that contain identifiable client level data 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. COALITION HMIS staff is available to consult on appropriate processes for disposal of electronic client level data.
8. User Access:
 - a. User access: User access and user access levels will be deemed by the Executive Director of the Participating Agency in consultation with the Site Technical Administrator. The Site Technical Administrator will assign username and passwords
 - b. User name format: The Site Technical Administrator will create all usernames using the first initial of first name and last name. Example John Doe's username 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.

9. User ID and Passwords:

- 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 ID 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. COALITION 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 logon 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.

10. Access Levels

An HMIS system should have many levels of access. These levels should be reflective of the access a user has to client-level paper records and 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: This role 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: A 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: 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: Case Managers have 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: Agency Administrators have access to all features, including agency level administrative functions. This level can add/remove users for his/her agency and edit their 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: A System Operator helps to maintain the system, but does not have access to any Client or Service Records. They have no access to reporting functions, but do have access to administrative functions. The System Operator would setup new agencies, add new users, reset passwords, and access other system-level options. The System Operator would order additional User Licenses and modify the allocations of Licenses.

- h. System Administrator: System Administrators have the same access rights to client information (full access) as Agency Administrator. However, this user would have full access to administrative functions.

11. Location Access:

Access to the system software 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 user rights.

12. Access To Data:

- a. User Access: Users will only be able to view the data entered by users of their own agency. Security measures exist within the HMIS software system that restricts agencies from viewing each other's data unless data sharing agreements are in place.
- 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 onto their local computer. Once this information has been downloaded from the HMIS server in raw format to an agency's computer, these data then become the responsibility of the agency. A participating Agency should develop protocol regarding the handling of data downloaded from the Report Writer.
- 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 HMIS Data: Access will be granted based upon policies developed by HMIS Project Committee.

13. 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.

14. Data Classification:

All data will be handled according to the following classifications to ensure that data are handled according to the following procedures and establish controls required for enforcing and maintaining security.

- 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.

15. Physical Access Control

- a. Physical access to the system data processing areas, equipment and media must be controlled. 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 proportionate with the threat and exposure to loss. Available precautions include equipment enclosures, lockable power switches, equipment identification and fasteners to secure the equipment.
- c. The COALITION HMIS staff and the Site Technical Administrators within Participating Agencies will determine the physical access controls appropriate for their organizational setting based on COALITION 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.
 1. Public Data: Security controls are not required.
 2. 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.

3. 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.
 4. 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 Systems Administrator. These data can only be delivered by hand to data owner.
- h. All data must be handled according to their classification. Failure to handle data properly is a violation of this Policy.
 - i. Magnetic media containing COALITION HMIS data which is released and/or disposed of by the Participating Agency and COALITION HMIS should first be processed to destroy any data residing on that media.

16. Logical Access

- a. To prevent unauthorized access, all of COALITION HMIS computing, data communications and sensitive data resources will be controlled based on the user's needs. 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 System Administrator.
- d. A member of the COALITION HMIS COALITION HMIS Staff will authorize all database accounts.

HMIS-014 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: RIGHT TO DENY USER AND PARTICIPATING AGENCIES' ACCESS

Policy: Participating Agency or a user 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 their access privileges suspended or revoked, and funding sources may be notified.
4. All sanctions are imposed by the Executive Director of the Coalition.
5. All sanctions can be appealed to the HMIS Project Committee.

HMIS-015 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: MAINTENANCE OF ONSITE 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.

Procedure:

1. 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 COALITION HMIS Project including the following:
2. Computer Equipment: The Participating Agency is solely responsible for maintenance of onsite computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for utilization in the COALITION HMIS Project.
3. Backup: The Participating Agency is not responsible for supporting a HMIS backup procedure for each computer connecting to the COALITION HMIS Project. A HMIS backup procedure is provided by the HMIS Vendor for HMIS data. All other backup up is the sole responsibility of the Participating Agency.
4. Internet Connection: COALITION HMIS staff members are not responsible for troubleshooting problems with Internet Connections.
5. Software: The COALITION HMIS staff members are not responsible for troubleshooting problems with software other than HMIS software.

SECTION 3: Training

HMIS-016 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: TRAINING

Policy: COALITION 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: COALITION 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

1. Basic: Introduction to HMIS
 - a. Introduction to the COALITION 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 COALITION 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 COALITION 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 COALITION HMIS staff or individuals certified by COALITION 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 COALITION HMIS implementation plan.
 - c. Enrollment: All users must be registered with the designated COALITION HMIS Systems Administrator. Users not registered for a training session will be denied access to the session.

- d. Cancellation: Participating Agencies must contact the COALITION HMIS training coordinator within 24 hours if they are unable to attend.

HMIS-017 Effective date: Prepared by: COALITION HMIS Policy Group
Revision: Revision date: Revised by:

Title: DATA ACCESS CONTROL

Policy: Site Technical Administrators at Participating Agencies and COALITION HMIS staff must monitor access to system software.

1. Site Technical Administrators at Participating Agencies and COALITION HMIS staff 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 COALITION HMIS staff must implement discretionary access controls to limit access to COALITION HMIS information when available and technically feasible.
3. Participating Agencies and COALITION HMIS must audit all unauthorized accesses and attempts to access COALITION HMIS information. Participating Agencies and COALITION HMIS also must audit all off-site accesses and attempts to access COALITION HMIS systems.
4. Audit records shall be kept at least six months, and Site Technical Administrators and COALITION HMIS Database Administrator shall 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. Each user's identity shall be authenticated through an acceptable verification process.
4. Passwords are the individual's responsibility, and users shall not share passwords.
5. 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.
6. 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.
7. Any passwords written down shall be securely stored and inaccessible to other persons.
8. Users shall not store passwords on a personal computer for easier log on.

HMIS-018 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: AUDITING: MONITORING, VIOLATIONS AND EXCEPTIONS

Policy: COALITION HMIS staff will monitor access to all systems that could potentially reveal a violation of information security protocols.

Violations

Any exception to the data security policies and Standards not approved by COALITION HMIS 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 shall be requested in writing by the Executive Director of the Participating Agency and approved by the COALITION HMIS Director as appropriate as well as COALITION HMIS Management Team and Applications Administrator.

Procedure:

1. Monitoring compliance is the responsibility of the 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 COALITION HMIS System Administrator as appropriate
3. The COALITION HMIS Project Group and System Administrator will review violations and recommend corrective and disciplinary actions.
4. COALITION 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. System Administrator shall have access to those logs.

HMIS-019 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: DATA INTEGRITY CONTROLS

Policy: Controls must exist to ensure data remain consistent with their source.

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 system will enforce referential integrity rules and restraints.
3. Only authorized personnel are permitted access to authorized records.
4. Only COALITION HMIS staff has access to the back-end of the system.
5. COALITION HMIS staff will not change data in the back-end of the system.

SECTION 4: Stages of Implementation

HMIS- 020 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: IMPLEMENTATION STAGE 1: START-UP AND INITIAL TRAINING

Policy: All Participating Agencies must complete Stage 1 implementation prior to receipt of computer equipment and software. After this period if the agency has not progressed to the next level, the participation agreement will be revisited with all parties involved to assess where obstacles for progress exist.

Procedure:

Each agency will:

1. Commit to participate and acquisition of Internet connection of at least 56K.
2. Sign user agreement, including data sharing agreement.
3. Commit to follow the security protocols and all policies and procedures adopted for the HMIS system.
4. Commit to inform all clients of their rights, both verbally and by providing printed materials, and to obtaining a release for sharing of data.
5. Designate a Site Technical Administrator.
6. Create User IDs and passwords for the COALITION HMIS.
7. Require all those who will be using the HMIS system to attend training.
8. COALITION Systems Administrator will visit each site to set up computer and do initial training.

HMIS-021 Effective date: Prepared by: COALITION HMIS Policy Group
Revision: Revision date: Revised by:

Title: IMPLEMENTATION STAGE 2: DATA ENTRY BEGINS

Policy: Participating Agencies must complete Stage 2 implementation with 90 days of receipt of software from the Coalition. After this period if the agency has not progressed to the next level, the participation agreement will be revisited with all parties involved to assess where obstacles for progress exist.

Procedure:

Each Agency will:

1. Develop agency specific interview protocols as necessary.
2. Use standard demographic interview protocols for intake.
3. Systematic data entry of records for all existing clients and all new homeless clients.

HMIS-022 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: IMPLEMENTATION STAGE 3: BASIC INFORMATION ON 90% OF CURRENT CLIENTS

Policy: Participating Agencies must complete Stage 3 implementation within 180 days of receipt of software. After this period if the agency has not progressed to the next level, the participation agreement will be revisited with all parties involved to assess where obstacles for progress exist.

HMIS-023 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: IMPLEMENTATION STAGE 4: SYSTEM FULLY INTEGRATED IN DAILY OPERATION

Policy: Participating Agencies include in-depth interviewing of clients on 100% of reportable clients served and, maintain all appropriate records on the system and fulfill all reporting requirements using the system within 12 months of receipt of software. If the agency has not progressed to this level within the 12 month period, the participation agreement will be revisited with all parties involved to assess where obstacles for progress exist.

SECTION 5: Data Release Protocols

HMIS-024 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: DATA RELEASE AUTHORIZATION AND DISTRIBUTION

Policy: The only data that will be released publicly shall be data in aggregate format. Only de-identified aggregate data will be 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 will be made directly available to the public in the future.
4. Parameters of the aggregate data, that is, where the data comes from, what it includes and what it does not include will be presented with each report.

HMIS- 025 Effective date: Prepared by: COALITION HMIS Policy Group
Revision: Revision date: Revised by:

Title: CLIENT RIGHT TO ACCESS and RIGHT TO DENY ACCESS TO CLIENT IDENTIFIED INFORMATION

Policy: COALITION HMIS retains authority to deny access to all personally identifying information contained within the system, except to the client for his/her own data. Any client will have access within three business days, to obtain 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.

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. 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, 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.

Procedure: Any request for personally identifying data from any person, agency, or organization other than the client himself/herself will be forwarded to the COALITION's HMIS Project Group for review.

SECTION 6: Internal Operating Procedures

HMIS- 026 Effective date:
Revision: Revision date:

Prepared by: COALITION HMIS Policy Group
Revised by:

Title: COMPUTER VIRUS: PREVENTION

Policy: COALITION HMIS staff and each participating agency will take all necessary precautions to prevent any destructive or malicious program (virus or worm) from being introduced to the system

Procedure:

1. No unscanned media will be introduced to the system.
2. Virus definitions will be updated weekly.

Appendix: Sample Forms

COALITION 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 COALITION 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