PRINCE GEORGE'S COUNTY DEPARTMENT OF SOCIAL SERVICES CONTINUUM OF CARE HOMELESS INFORMATION MANAGEMENT TRACKING SYSTEM (HMIS)

Policies and Procedures Manual

ATTACHMENTS:

INTRODUCTION

The Prince George's County Department of Social Services Continuum of Care Homeless Information Management Tracking System (HMIS) is a project that utilizes Internet-based technology to assist homeless service organizations across the county to capture information about the clients that they serve. HMIS staff provides training and technical assistance to users of the system throughout the county.

A goal of HMIS is to collect critical information necessary to inform public policy about the extent and nature of homelessness in the county. This is accomplished through analysis and release of data that are grounded in the actual experiences of homeless persons and the service providers who assist them in shelters and homeless assistance programs throughout the state. Information that is gathered via interviews, conducted by service providers with consumers, is analyzed for an unduplicated count, aggregated and made available to policy makers, service providers, advocates, and consumer representatives.

HMIS is advised by a user committee 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 homeless men, women, and children 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 who are serving the same clients. If the client is unaware that information is shared (written consent form not completed), then information that is already in the system cannot be discussed with the client unless your agency entered the information.

Potential benefits for agency and program managers: When aggregated, information can be used to garner 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 Housing & Urban Development (HUD). The software has the capability to generate the 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.

This document provides the policies, procedures, guidelines, and standards that govern the HMIS project, as well as roles and responsibilities for HMIS and participating agency staff. Participating agencies will receive all relevant portions of the complete document. A copy of internal policies and procedures is available upon request.

GOVERNING PRINCIPLES

The following descriptions are the overall governing principles upon which all other decisions pertaining to the HMIS project are based.

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

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 working directly with clients or who have administrative responsibilities will receive authorization to look at, enter, or edit client records. Additional privacy protection policies include:

- Client has the right to not answer any question, unless entry into a service program requires it;
- Client has the right to know who has added to, deleted, or edited their client record in HMIS;
- Client information transferred from one authorized location to another over the web is transmitted through a secure, encrypted connection.

Application Software: Only tested and controlled software should be installed on networked systems. Use of unevaluated and untested software outside an application development environment is prohibited.

Computer Crime: Computer crimes violate state and federal law as well as the HMIS Data Security Policy and Standards. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs, or hardware; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, peripherals, data, or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly liable for their actions, or both. HMIS staff and authorized agencies must comply with license agreements for copyrighted software and documentation. Licensed software must not be copied unless the license agreement specifically provides for it. Copyrighted software must not be loaded or used on systems for which it is not licensed.

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 should not use HMIS computing resources for personal purposes. Users must not attempt to gain physical or logical access to data or systems for which they are not authorized. Users must not attempt to reverse-engineer commercial software. Users must not load unauthorized programs or data onto HMIS computer systems. Users should scan all personal computer programs and data for viruses before logging onto HMIS computer systems.

SECTION 1:

Contractual Requirements and Roles

SOP#: CRR-001	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: HMIS CONTRACT REQUIREMENTS

Policy: HMIS is committed to provide services to participating agencies.

Standard: HMIS will provide quality service to existing and new participating agencies.

Purpose: To outline the basic services for existing and new agencies

Scope: Participating agencies and HMIS Project

Basic Requirements:

A. **Purchase of Software Licensing and Technical Support:** All existing and new sites participating in the HMIS Project that are funded through the Prince George's County Department of Social Services Office of Housing and Homeless Services are covered under their current contracts. The costs covered by their contractors include user licenses for HMIS and technical assistance provided by HMIS staff. **Please note: participating agencies are responsible for all costs associated with hardware acquisition and maintenance, personnel, and Internet access.**

   Agencies that are not funded to participate in the HMIS Project must pay a yearly fee according to HMIS' cost document.

B. **Access:** Existing and new participating agencies covered under existing contracts will not be granted access to the HMIS software system until a contractual agreement has been signed with HMIS.

SOP#: CRR-002	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: HMIS USER COMMITTEE

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

Standard: The responsibilities of the User Committee will be apportioned according to the information provided below.

Purpose: To define the roles and responsibilities of the project User Committee.

Scope: All project stakeholders.

Responsibilities:

The User Committee meets monthly to advise and support HMIS' operations in the following programmatic areas: Resource Development; Consumer Involvement; and Quality Assurance/Accountability.

Membership of the User Committee will be established according to the following guidelines:

- Target will be 25 Active Users;
- There will be a concerted effort to find replacement representatives when participation has been inactive or inconsistent from the organizations involved in the project;
- There will be a pro-active effort to fill gaps in the membership of the Committee in terms of constituency representation, consumer representatives, shelters for families and individuals, advocacy organizations, government agencies that fund homeless assistance services, and statewide geographic distribution.

The User Committee is fundamentally an advisory committee to the HMIS project. However the HMIS delegates final decision making authority to the Committee on selected key issues that follow. These issues include:

- Determining the guiding principles that should underlie the implementation activities of HMIS and participating organizations and service programs;
- Selecting the minimal data elements to be collected by all programs participating in the HMIS project;
- Defining criteria, standards, and parameters for the release of aggregate data;
- Ensuring adequate privacy protection provisions in project implementation.

SOP#: CRR-003	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: HMIS MANAGEMENT

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

Standard: The responsibilities of the HMIS will be apportioned according to the information provided below.

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

Scope: System wide.

HMIS Roles and Responsibilities:

Management:

The HMIS management staff is responsible for oversight of all day-to-day operations including: technical infrastructure; planning, scheduling, and meeting project objectives; supervision of staff, including reasonable divisions of labor; hiring; and orientation of new staff to program operations, Guiding Principles and Policies and Procedures.

Technical Assistance:

The Technical Assistants are responsible for overseeing usage of the HMIS database application, and being available for phone support as needed.

Responsibilities and Duties of the TA Manager/Staff include:

- Provide training on a monthly basis to agency staff
- Provide technical assistance and troubleshooting as needed
- Provide technical assistance in generating funder-required reports

Data Analysis:

HMIS' data analysis manager/staff is responsible for the following:

- Provide data quality queries to sites on a regular basis.
- Provide detailed statewide reports on families and individuals accessing emergency shelter.
- Provide data analysis and reports for Continua that have contracts with HMIS.

Systems Administration/Security/User Accounts:

HMIS has a contract with Wellsky to host the central server. They will have overall responsibility for the security of the system.

The HMIS Technical Assistant Manager/Staff will review all network and security logs regularly.

All Site Technical Administrator user accounts are the responsibility of the Prince George's County Department of Social Services. All Participating Agency staff user accounts are the responsibility of the Site Technical Administrator.

SOP#: CRR-004	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: ROLE: PARTICIPATING AGENCY EXECUTIVE DIRECTOR & PROGRAM MANAGER

Policy: The Executive Director & Program Manager of each participating agency will be responsible for oversight of all agency staff who generate or have access to client-level data stored in the system software to ensure adherence to the HMIS standard operating procedures outlined in this document.

Standard: The Executive Director & Program Director holds final responsibility for the adherence of his/her agency's personnel to the HMIS Guiding Principles and Standard Operating Procedures outlined in this document.

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

Scope: Executive Director & Program Manager in each participating agency.

Responsibilities:

The participating agency's Executive Director or Program Manager is responsible for all activity associated with agency staff access and use of the HMIS data system. This person is responsible for 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. The Executive Director or Program Manager will be held liable for any misuse of the software system by his/her designated staff. The Executive Director or Program Director agrees to only allow access to the HMIS software system based upon need. Need exists only for those shelter staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.

The Executive Director & Program Manager also oversee the implementation of data security policies and standards and will:

1. Assume responsibility for integrity and protection of client-level data entered into the HMIS system;
2. Establish business controls and practices to ensure organizational adherence to the HMIS Policies and Procedures;
3. Communicate control and protection requirements to agency custodians and users;
4. Authorize data access to agency staff and assign responsibility for custody of the data;
5. Monitor compliance and periodically review control decisions.

SOP#: CRR-005	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: ROLE: PARTICIPATING AGENCY SITE TECHNICAL ADMINISTRATOR

Policy: Every participating agency must designate one person to be the Site Technical Administrator.

Standard: The designated Site Technical Administrator holds responsibility for the administration of the system software in his/her agency.

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

Scope: Participating Agencies.

Responsibilities:

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

- Editing and updating agency information;
- Granting technical access to the software system for persons authorized by the agency's Executive Director by creating usernames and passwords;
- Training new staff persons on the uses of HMIS software system, including review of the Policies and Procedures in this document and any agency policies that impact the security and integrity of client information;
- Ensuring that access to the HMIS system be granted to authorized staff members only 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;
- Notifying all users in their agency of interruptions in service.

The Site Technical Administrator is also responsible for implementation of data security policy and standards, including:

- Administering agency-specific business and data protection controls;
- Administering and monitoring access control;
- Providing assistance in the backup and recovery of data;
- Detecting and responding to violations of the Policies and Procedures or agency procedures.

SOP#: CRR-006	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: ROLE: USER

Policy: All individuals at the HMIS and at the Participating Agency levels who require legitimate access to the software system will be granted such access.

Standard: Individuals with specific authorization can access the system software application 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.

Scope: System wide

Responsibilities:

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 carrying out 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

SOP#: REQ-001	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: PARTICIPATION REQUIREMENTS

Policy: HMIS staff will communicate requirements for participation. All requirements for participation are outlined in this document.

Standard: HMIS staff and Participating Agencies will work to ensure that all sites receive the benefits of the system while complying with all stated policies.

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

Scope: System wide

Procedure:

Participation Agreement Requirements

- **High Speed Internet Connection Greater than 56k / v90:** DSL, Cable, etc.

- **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 Service Point system.

- **Security Assessment:** Meeting of Agency Executive Director (or designee), Program Manager/Administrator and Site Technical Administrator with DSS staff member to assess and complete Agency Information Security Protocols. See attached Initial Implementation Requirements.

- **Training:** Commitment of Site Technical Administrator and designated staff persons to attend training(s) at Prince George's County Department of Social Services prior to accessing the system online. **Note:** Staff will **NOT** be allowed to attend training until **ALL** Information Security paperwork is complete and signed by Executive Director (or designee).

- **Interagency Data Sharing Agreements:** Interagency Data Sharing Agreements must be established between any shelter/service program where sharing of client level information is to take place. See attached Interagency Data Sharing Agreement.

- **Client Authorization 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 Authorization Form as an example.

- **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 HMIS. See attached Initial Implementation Requirements.

- **Minimal Data Elements:** Agencies will be required to enter minimal data elements as defined by the HMIS Project and its Steering Committee.

SOP#: REQ-002	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**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.

Standard: All implementation requirements must be complete and on file prior to using the system.

Purpose: To indicate documentation requirements prior to implementation.

Scope: Participating Agencies

Procedure: HMIS staff will assist Participating Agencies in the completion of all required documentation.

On Site Security Assessment Meeting: Meeting of Agency Executive Director or authorized designee, Program Manager/Administrator and Site Technical Administrator with HMIS staff member to assist in completion of the Agencies' Information Security Protocols.

Participation Agreement
The Participation Agreement refers to the document agreement made between the participating agency and the HMIS Project. This agreement includes commitment to minimal data as defined by the HMIS Project and its HMIS User Committee on all clients. This document is the legally binding document that refers to all laws relating to privacy protections and information sharing of client specific information. See Attachment A: Initial Implementation Requirements.

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 HMIS Security Manual. The Executive Director of designee will be responsible for signing this form. See Attachment A: Initial Implementation Requirements.

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

SOP#: REQ-003	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**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.

Standard: For participating agencies to engage in data sharing arrangements, a written, formal document must be signed by the Executive Director of each of the Participating Agencies involved in the data sharing.

Purpose: To explain the vehicle through which agencies can enter into an agreement allowing them to share client records.

Scope: Participating Agencies wishing to share client records.

Responsibilities:

Interagency Sharing Agreements

A. **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 Participating Agencies. See Attachment A: Interagency Sharing Agreement.

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

Procedure:

A. Executive Directors wishing to participate in a data sharing agreement contact HMIS staff to initiate the process.

B. Executive Directors complete the Interagency Sharing Agreement. Each participating agency retains a copy of the agreement and a master is filed with the HMIS Organization.

C. Site Technical Administrators receive training on the technical configuration to allow data sharing.

D. Each Client whose record is being shared must agree via a written client authorization form to have their data shared. A client must be informed of what information is being shared and with whom it is being shared.

SOP#: REQ-004	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: WRITTEN CLIENT AUTHORIZATION PROCEDURE FOR ELECTRONIC DATA SHARING

Policy: As part of the implementation strategy of the system software, a Participating Agency must have client authorization procedures and completed forms in place when electronic data sharing is to take place.

Standard: Client authorization procedures must be on file prior to the assignment of user accounts to the site by Prince George's County Department of Social Services.

Purpose: To indicate the type of client consent procedures that Participating Agencies must implement prior to actual implementation.

Scope: Participating Agencies wishing to share client records

Procedure:

Client Authorization Procedures
See attached Client Authorization Form.

SOP#: REQ-005	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: CONFIDENTIALITY AND INFORMED CONSENT

Policy: All Participating Agencies agree to abide by all privacy protection standards and agree to uphold all standards of privacy as established by Prince George's County Department of Social Services Technicians.

Standard: It is suggested that Participating Agencies develop procedures for providing oral explanations to clients about the usage of a computerized Homeless Management Information System. Participating Agencies are required to use written client authorization forms when information is to be shared with another agency.

Purpose: To ensure protection of clients' privacy.

Scope: Participating Agencies

Procedure:

Confidentiality / Client Consent

Informed Consent: Oral Explanation (non-shared records): All clients should be provided an oral explanation that their information will be entered into a computerized record keeping system. The Participating Agency should provide an oral explanation of the HMIS Project and the terms of consent. The agency may want to develop a fact sheet to post within the agency. HMIS suggests including the following information in the fact sheet:

1. What HMIS is
   - Web-based information system that homeless services agencies across the state use to capture information about the persons they serve
2. Why the agency uses it
   - To understand their clients' needs
   - Help the programs plan to have appropriate resources for the people they serve
   - To inform public policy
3. Security
   - Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records
4. Privacy Protection
   - No information will be released to another agency without written authorization
   - Client has the right to not answer any question, unless entry into a program requires it
   - Client has the right to know who has added to, deleted, or edited their Service Point record

- Information that is transferred over the web is through a secure connection

5. Benefits for clients
   - Case manager tells client what services are offered on site or by referral through the assessment process
   - Case manager and client can use information to assist clients in obtaining resources that will help them meet their needs.

Written Client Consent

Each client whose record is being shared electronically with another Participating Agency must agree via a written client authorization form to have his or her data shared. A client must be informed of what information is being shared and with whom it is being shared.

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 Authorization Form.

Federal/State Confidentiality Regulations

The Participating Agency will uphold Federal and State Confidentiality regulations to protect client records and privacy. In addition, the Participating Agency will only release client records with written consent by the client, unless otherwise provided for in the regulations.

1) 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.
2) The Participating Agency will abide specifically by Maryland general laws. 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.

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.

SOP#: REQ-006	**Revision:**	**Prepared by: HMIS**
Effective date: 7/04	**Revision date:**	**Revised by:**

Title: MINIMAL DATA ELEMENTS

Policy: Participating Agencies that collect client data through the Homeless Management Information System collects all data contained within the Profile Screen.

Standard: All agencies will collect minimal data elements.

Purpose: To ensure that agencies are collecting quality data.

Scope: All Participating Agencies

Procedure:

Commitment to Utilization of Interview Protocol

Minimal Data Elements: The Participating Agency is responsible for ensuring that all clients are asked the questions contained within the Profile Screen. Data will be used in aggregate analysis. These questions are contained within the Profile Screen.

SOP#: REQ-007	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: INFORMATION SECURITY PROTOCOLS

Policy: Participating Agencies must develop and have in place minimum information security protocols.

Standard: Participating Agencies must develop rules, protocols and procedures to address each of the following:

- Assignment of user accounts
- Unattended workstations
- Physical access to workstations
- Policy on user account sharing
- Client record disclosure
- Report generation, disclosure and storage

Purpose: To protect the confidentiality of the data and to ensure its integrity at the site.

Scope: Participating Agencies.

Procedures: To develop internal protocols, please reference Section 4.

SOP#: REQ-008	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: IMPLEMENTATION: CONNECTIVITY

Policy: Participating Agencies are required to obtain an adequate Internet connection (greater than 56K/v90)

Standard: Any Internet connection greater than 56K/v90 is acceptable.

Purpose: To ensure proper response time and efficient system operation of the Internet application.

Scope: Participating Agencies

Procedure: Prince George's County Department of Social Services staff informs all participating agencies about availability of Internet providers. Obtaining and maintaining an Internet connection greater than 56K/v90 is the responsibility of the participating agency.

SOP#: REQ-009	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**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.

Standard: Participating Agencies must meet technical standards for minimum computer equipment configuration, Internet connectivity, data storage and data back up.

Purpose: To ensure that participating agencies adopt equipment and data maintenance program.

Scope: Participating Agencies

Responsibilities:

The Executive Director 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:

A. **Computer Equipment:** The Participating Agency is 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.
B. **Backup:** The Participating Agency is responsible for supporting a back-up procedure for each computer connecting to the HMIS Project.
C. **Internet Connection:** HMIS staff members are not responsible for troubleshooting problems with Internet Connections.
D. **Virus Protection:** As a matter of course, each agency should install virus protection software on all computers.
E. **Data Storage:** The Participating Agency agrees to only download and store data in a secure format.
F. **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. HMIS staff can be contacted for advice on appropriate processes for disposal of electronic client level data.

SECTION 3:

Training

SOP#: TRA-001	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: TRAINING SCHEDULE

Policy: Prince George’s County Department of Social Services staff will maintain an ongoing training schedule for Participating Agencies.

Standard: Prince George’s County Department of Social Services staff publishes a training schedule and will offer them regularly.

Purpose: To make participating agencies aware of on going training.

Scope: System wide

Procedure:

A training schedule will be published monthly on the Prince George’s County Department of Social Services HMIS website. Agencies will RSVP for all trainings. Trainings will be offered at Prince George’s County Department of Social Services unless otherwise noted.

SOP#: TRA-002	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: USER, ADMINISTRATOR AND SECURITY TRAINING

Policy: All users will undergo security training before gaining access to the system. This training includes a review of Prince George's County Department of Social Services security Policies and Procedures.

Standard: Prince George's County Department of Social Services staff will provide data security training.

Purpose: To ensure that staff is properly trained and knowledgeable of Prince George's County Department of Social Services' security Policies and Procedures.

Scope: System wide

Procedure: Agency staff must attend user training. Site Technical Administrators must also attend an administrator training and a Report Writer I training in addition to a user training. Agencies will be notified of scheduled training sessions.

Training:
The Participating Agencies Site Technical Administrator is responsible for training new users. Users must receive HMIS training prior to being granted user privileges for the system.

SECTION 4:

User, Location, Physical and Data Access

SOP#: ULPD-001	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: ACCESS PRIVILEGES TO SYSTEM SOFTWARE

Policy: Participating Agencies will apply the user access privilege conventions set forth in this procedure.

Standard: Allocation of user access accounts and privileges will be made according to the format specified in this procedure.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

Procedure:

User Access Privileges to HMIS

A. **User access:** User access and user access levels will be deemed by the Program Manager of the participating agency in consultation with the Site Technical Administrator. The Site Technical Administrator will generate username and passwords within the administrative function of HMIS.

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, then the middle initial should be used. If someone has the same first name and middle initial and last name, the sequential number should be placed at the end of the above format. Example: JDoe2, JDoe3.

C. **Passwords:**

1. **Creation:** Passwords are automatically generated from the system when a user is created. Site Technical Administrators will communicate the system-generated password to the user.

2. **Use of:** The user will be required to change the password the first time they log onto the system. The password must be between 8 and 16 characters and contain 2 numbers.

3. **Expiration:** Passwords expire every 45 days.

4. **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 5 business days 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 yearly basis.

SOP#: ULPD-002	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: ACCESS LEVELS FOR SYSTEM USERS

Policy: participating agencies will manage the proper designation of user accounts and will monitor account usage.

Standard: Participating agency agrees to apply the proper designation of user accounts and manage the use of these accounts by agency staff.

Purpose: To enforce information security protocols

Scope: Participating Agencies

Procedure: User accounts will be created and deleted by the Site Technical Administrator under authorization of the Participating Agency's Program Manager.

<u>Designation of HMIS Users</u>

User Levels: There are 9 levels of access to the HMIS system. These levels should be reflective of the access a user has to client level paper records, and access levels should be need-based. Need exists only for those shelter staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.

Access Level	Description
Resource Specialist I	Access is limited to the ResourcePoint module. 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 Resource Specialist cannot modify or delete data.
Resource Specialist II	The same access rights as Resource Specialist I, however, this person is considered an agency-level I&R Specialist who updates their own agency and program information.
Resource Specialist III	The same access rights as Resource Specialist II, however, this person is a system-wide I&R Specialist who can update any agency or program information. This access level can also edit the system-wide news.
Volunteer	Access to ResourcePoint module is limited access to ClientPoint, and limited access to service records. A volunteer can 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 the intake

	and then refer the client to agency staff or a case manager.
Agency Staff	Agency staff has access to ResourcePoint, limited access to ClientPoint, full access to service records and access to most functions in HMIS. However, Agency Staff can only access basic demographic data on clients (profile screen). All other screens are restricted, including assessments and case plan records. They have full access to service records. Agency Staff can also add news items to the newswire feature. There is no reporting access.
Case Manager	Case Managers have access to all features excluding administrative functions. They have access to all screens within ClientPoint, including the assessments and full access to service records. There is full reporting access.
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. They cannot access the following administrative functions: Assessment Administration, Picklist Data, Licenses, Shadow Mode, or System Preferences.
Executive Director	Same access rights as Agency Administrator, but ranked above Agency Administrator.
System Operators	System Operators have no access to ClientPoint or ShelterPoint. They have no access to reporting functions, but do have access to administrative functions. The System Operator can setup new agencies, add new users, reset passwords, and access other system-level options. The system operator helps to maintain the system, but does not have access to any client or service records. The system operator can order additional user licenses and modify the allocations of licenses.
System Administrator I	Same access rights to **client** information (full access) as **Agency Administrator.** However, this user has full access to administrative functions.
System Administrator II	System Administrator IIs have full and complete access to the system. However, this user does not have the option of choosing a Provider other than the default provider assigned to their ID.

SOP#: ULPD-003	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: ACCESS PRIVILEGES TO SYSTEM SERVER

Policy: Participating agencies agree to enforce the location access privileges to the system server.

Standard: Only authorized computers will be able to access the system from authorized locations.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

Procedure:

Location Access: Access to the software system will only be allowed for computers identified by the Executive Director and Site Technical Administrator of the participating agency. Those designated computers will be registered electronically with the central server by HMIS. Laptops and off-site installations will require an additional security form stating that use will not be for unauthorized purposes from unauthorized locations. See attached Laptop and Off-Site Installation Access Privileges to System Server Commitment Form.

SOP#: ULPD-004	**Revision:**	**Prepared by HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: ACCESS TO DATA

Policy: Participating agencies must agree to enforce the user access privileges to system data server as stated below.

Standard: **A. User Access:** Users will be able to view the data entered by other users of HMIS. Security measures exist within the HMIS software system that restricts agencies from viewing each other's data.

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, the data 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 must 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 Countywide HMIS Data: Access will be granted based upon policies developed by the Access to Data Subcommittee of the HMIS User Committee.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

SOP#: ULPD-005 **Revision:** **Prepared by: HMIS**

Effective date: 7/04 **Revision date:** **Revised by:**

Title: ACCESS TO CLIENT PAPER RECORDS

Policy: Participating Agencies will establish procedures to handle access to client paper records.

Standard: The Participating Agencies agree to establish procedures regarding which staff have access to client paper records.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

Procedures:

- 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.
- Identify how and where client paper records are stored.
- Develop policy regarding length of storage and disposal procedure of paper records.
- Develop policy on disclosure of information contained in client paper records.

SOP#: ULPD-006	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: PHYSICAL ACCESS CONTROL

Policy: 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.

Standard: 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.

Purpose: To delineate standards for physical access.

Scope: System wide

Guidelines:

Access to computing facilities and equipment

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

Media and hardcopy protection and transportation

- Printed versions of confidential data should not be copied or left unattended and open to unauthorized access.
- Media containing client-identified data will not be shared with any agency that does not participate in the Prince George's County HMIS system. Authorized employees, using methods deemed appropriate by the participating agency, may transport HMIS data that meet the above standard. Reasonable care should be used, and media should be secured when left unattended.
- Magnetic media containing HMIS data, which is released and/or disposed of from the Participating Agency and Central Server, should first be processed to destroy any data residing on that media.
- Degaussing and overwriting are acceptable methods of destroying data.
- Responsible personnel must authorize the shipping and receiving of magnetic media, and appropriate records must be maintained.
- HMIS information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

SOP#: ULPD-007	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: UNIQUE USER ID AND PASSWORD

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

Standard:

- Each user will be required to enter a User ID with a Password in order to logon to the system.
- User ID and Passwords are to be assigned to individuals.
- 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, middle initial, and last name. If someone has the same first and middle initial and last name, then the number 1 should follow, i.e., JBDoe1, JBDoe2.
- The Password must be no less than eight and no more than 16 characters in length, and must contain two numbers.
- The password must be alphanumeric

Purpose: In order to ensure that only authorized users will be able to access, modify or read data, a unique User ID will be issued to every user.

Scope: System wide

Procedures:

- *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 a temporary password can be communicated via email. HMIS staff is not available to agency staff to reset passwords. Only a Site Technical Administrator can reset a password.
- *Forced Password Change (FPC)*
  FPC will occur every forty-five days once a user account is issued. Passwords will expire and user 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.
- *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.

SOP#: ULPD-008	**Revision:**	**Prepared by: HMIS**
Effective date: 7/04	**Revision date:**	**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.

Standard: Serious or repeated violation by users of the system may result in the suspension or revocation of an agency's access.

Purpose: To outline consequences for failing to adhere to information security protocols.

Scope: Participating Agency

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. Sanctions may include but are not limited to: a formal letter of reprimand; suspension of system privileges; revocation of system privileges; termination of employment and criminal prosecution.
3. Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.
4. The Continuum of Care Steering Committee imposes all sanctions.

SOP#: ULPD-009	**Revision:**	**Prepared by: HMIS**
Effective date: 7/04	**Revision date:**	**Revised by:**

Title: DATA ACCESS CONTROL

Policy: Site Technical Administrators at Participating Agencies and HMIS staff must regularly review user access privileges and remove identification codes and passwords from their systems when users no longer require access.

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

Participating Agencies and HMIS staff must audit all unauthorized accesses and attempts to access HMIS information. Participating Agencies and HMIS staff also must audit all off-site accesses and attempts to access HMIS systems. Audit records shall be kept at least six months, and Site Technical Administrators and HMIS staff will regularly review the audit records for evidence of violations or system misuse.

Purpose: To indicate the standards and guidelines for data access control for the participating agency.

Scope: System wide

Guidelines:

- Access to computer terminals within restricted areas should be controlled through a password or through physical security measures.
- Each user should have a unique identification code.
- Each user's identity should be authenticated though an acceptable verification process.
- Passwords are the individual's responsibility, and users cannot share passwords.
- Users should be able to select and change their own passwords, and must do so at least every forty-five days. A password cannot be re-used until 1 password selection has expired.
- Passwords should not be able to be easily guessed or found in a dictionary. The password format is alphanumeric.
- Any password written down should be securely stored and inaccessible to other persons. Users should **not** store passwords on a personal computer for easier log on.

SOP#: ULPD-010	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: AUDITING: MONITORING, VIOLATIONS AND EXCEPTIONS

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

Standard: **Monitoring**
HMIS staff will monitor compliance with data security standards.

Violations
Any exception to the data security policies and standards not approved by the Continuum of Care Steering Committee is a violation, and will be reviewed for appropriate disciplinary action that could include termination of employment or criminal prosecution.

Exceptions
All exceptions to these standards are to be requested in writing by the Program Manager or Executive Director of the Participating Agency and approved by the Continuum of Care Steering Committee as appropriate, as well as the HMIS Management Team.

Purpose: To outline the standards and procedures on compliance with information security protocols and the process by which HMIS staff will monitor compliance with such policies.

Scope: System wide

Monitoring

- Monitoring compliance is the responsibility of HMIS.
- All users and custodians are obligated to report suspected instances of noncompliance.

Violations

- HMIS staff will review standards violations and recommend corrective and disciplinary actions.
- Users should report security violations to the Site Technical Administrator, or HMIS staff person as appropriate.

Exceptions

- Any authorized exception to this policy must be issued from the Continuum of Care Steering Committee and the Participating Agency's Executive Director or Program Manager.

SOP#: ULPD-011	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: LOCAL DATA STORAGE

Policy: Client records containing identifying information that are stored within the Participating Agency's local computers are the responsibility of the Participating Agency.

Standard: Participating Agencies should develop policies for the manipulation, custody and transmission of client-identified data sets.

Purpose: To delineate the responsibility that Participating Agencies have for client-identified data.

Scope: Participating Agencies

Procedure: A Participating Agency develops policies consistent with Information Security Policies outlined in this document regarding client-identifying information stored on local computers.

SOP#: ULPD-012	**Revision:**	**Prepared by: HMIS**
Effective date: 7/05	**Revision date:**	**Revised by:**

Title: TRANSMISSION OF CLIENT LEVEL DATA

Policy: Client data will be transmitted considering the utmost security method to protect client privacy and confidentiality.

Standards: Administrators of the Central Server data must be aware of access-control vulnerabilities for that data while they are in transmission within the network.

Purpose: To provide guidelines regarding security of client level data during transmission.

Scope: System wide

Guidelines: Transmission will be secured by 128-bit encryption provided by SSL Certificate protection, which is loaded at the HMIS server.

SECTION 5:

Technical Support and System Availability

SOP#: TSS-001	**Revision:**	**Prepared by: HMIS**
Effective date: 07/05	**Revision date:**	**Revised by:**

Title: PLANNED TECHNICAL SUPPORT

Policy: System & Agency Administrative staff will offer standard technical support to all participating agencies.

Standards: System & Agency Administrative staff will provide technical assistance to participating agencies on use of the system software.

Purpose: To describe the elements of the technical support package offered by HMIS.

Scope: System Wide

Procedure: **System & Agency Administrative**

- Start-up and implementation
- On-going technical assistance
- Training
- Technical assistance with report writing

SOP#: TSS-002 **Revision:** **Prepared by: HMIS**

Effective date: 7/05 **Revision date:** **Revised by:**

Title: PARTICIPATING AGENCY SERVICE REQUEST

Policy: System Administrator will respond to requests for service that arrive from the Agency's Executive Director or the site Technical Administrator.

Standards: To effectively respond to service requests, System Administrators will require that proper communication channels be established and used at all times.

Purpose: To outline the proper methods of communicating a service request from a Participating agency to a System Administrator.

Scope: Participating Agencies

Procedure:

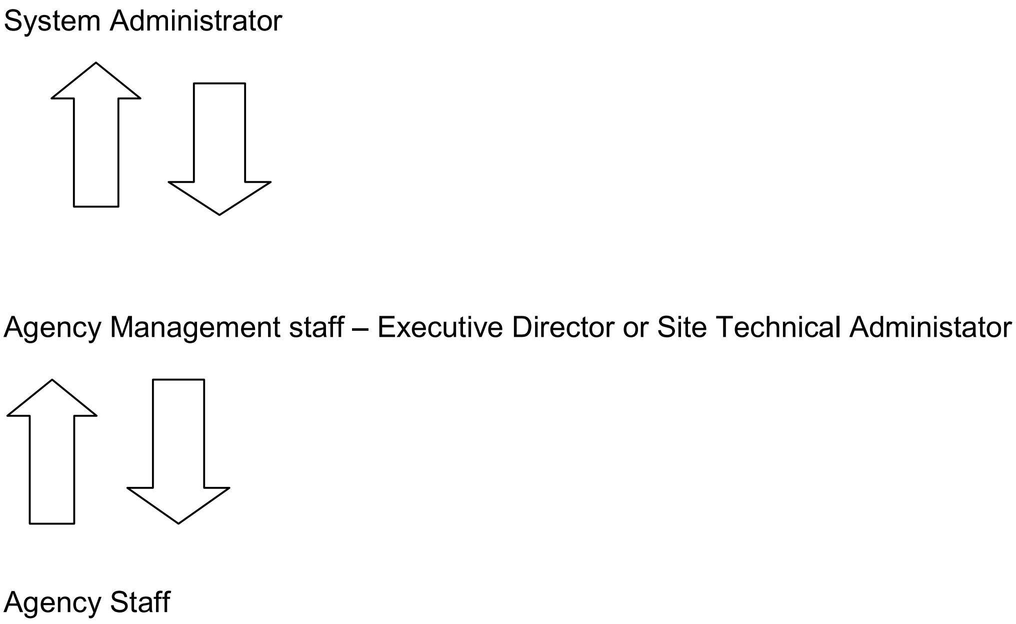
Service Request from Participating Agency

A. Agency Management Staff (Executive Director or site Technical Administrator) contact assigned system administrator for service

B. System Administrator assigned to the participating Agency determines resources needed for service.

C. System Administrator contacts agency management staff to work out a mutually convenient service schedule

Chain of communication



System Administrator

Agency Management staff – Executive Director or Site Technical Administator

Agency Staff

SOP#: TSS-003	**Revision:**	**Prepared by: HMIS**
Effective date: 07/05	**Revision date:**	**Revised by:**

Title: AVAILABILITY: HOURS OF SYSTEM OPERATION

Policy: The system will be available to the community of users in a manner consistent with the users reasonable usage requirements**.**

Standard: Members of the HMIS agree to minimally operate the System website twenty hours a day/ seven days a week. Some time is required each day to back-up the server and database.

Purpose: To delineate the schedule that Prince George's County Department of Social Services will make the system available to the network of users throughout Prince George's County.

Scope: System Wide

Schedule: The system will be available from 6:00 A.M – 12:00PM and 2:00PM-4:00AM, seven days a week, excluding acts of god, or federal or state declared emergency situations.

SOP#: TSS-004	**Revision:**	**Prepared by: HMIS**
Effective date: 07/05	**Revision date:**	**Revised by:**

Title: AVAILABILITY: CSPTECH STAFF AVAILABILITY

Policy: System or Agency Administrator will be available to the community of users in a manner consistent with the user's reasonable service request requirements.

Standard: System Agency Administrator are available for Technical Assistance, questions and troubleshooting between the hours of 8:30am and 5:00pm Monday to Friday, excluding city, state, and federal holidays

Purpose: To delineate the range of technical issues that System and Agency Administrators will be able to resolve**.**

Scope: County

Procedure:

SOP#: TSS-005	**Revision:**	**Prepared by: HMIS**
Effective date: 07/05	**Revision date:**	**Revised by:**

Title: AVAILABILITY: PLANNED INTERRUPTION TO SERVICE

Policy: System Administrator will inform participating agencies of any planned interruption to service.

Standard: Participating Agencies will be notified of planned interruption to service one week prior to the interruption.

Purpose: To indicate procedures for communicating interruption to service. To indicate procedures for communicating when services resume.

Scope: County

Procedure:

Planned Interruption to service

System Administrator will notify Participating Agencies via HMIS Newsflash, e-mail and/ or fax the schedule for the interruption to service. An explanation of the need for the interruption will be provided and expected benefits or consequences articulated.

Service Restoration

System Administrator will notify via e-mail and / or fax service has resumed.

SOP#: TSS-006	**Revision:**	**Prepared by: HMIS**
Effective date: 07/05	**Revision date:**	**Revised by:**

Title: AVAILIBILITY: UNPLANNED INTERRRUPTION TO SERVICE

Policy: Participating Agencies may or may not be notified in advance of unplanned interruption to service.

Standard: Participating Agencies will be notified of unforeseen interruption to service that are expected to exceed two hours**.**

Purpose: To indicate procedures for communicating unforeseen interruption to service

Scope: System Wide

SECTION 6:

Data Release Protocols

SO SOP#: DRP-001	**Revision:**	**Prepared by: HMIS**
Effective date: 07/05	**Revision date:**	**Revised by:**

Title: DATA RELEASE AUTHORIZATION AND DISTRIBUTION

Policy: HMIS staff will follow User Committee procedures to release of all data as needed.

Standard: HMIS staff will abide by Access to Data Policies as established by the User Committee.

Purpose: To outline the procedures for the release of data from the HMIS Training System.

Scope: User Committee and HMIS Staff will decide based on procedure how to release all data.

Procedure: All data that are to be released in aggregate format must represent at least sixty percent (60%) of the clients in that region.

Release of data principals (Participating Agency)

- 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
- There will be full access to aggregate data for the inner circle (all participating agencies).
- Aggregate data will be available in the form of an aggregate report or as a raw data set.
- Aggregate data will be made directly available to the public in the future.
- 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.
- An executive committee shall be put in place when approval is required for release of data that does not meet the 60% release rate.

SOP#: DRP-002	**Revision:**	**Prepared by: HMIS**
Effective date: 07/05	**Revision date:**	**Revised by:**

Title: RIGHT TO DENY ACCESS TO CLIENT IDENTIFIED INFORMATION

Policy: PGCDSS retains authority to deny access to all client identified information contained within the system.

Standard: No data will be released to any person, agency, or organization that is not the owner of said data.

Purpose: To protect client confidentiality.

Scope: Countywide.

Procedure:

1. Any request for client identified data from any person, agency, or organization other than the owner will be forwarded to the PGCDSSCoC Board for review.

2. Pursuant to PGCDSSCoC Review Board Policy any outside entity must obtain the written consent of every client contained within the database prior to the release of the data.

SOP#: DRP-003	**Revision:**	**Prepared by: HMIS**
Effective date: 0705	**Revision date:**	**Revised by:**

Title: RIGHT TO DENY ACCESS TO AGGREGATE INFORMATION

Policy: HMIS staff retains authority to deny access to all aggregate data contained within the system.

Standard: No data will be released without proper authorization.

Purpose: To prevent the unauthorized distribution of aggregated reports.

Scope: County Wide.

Procedure: When a person or organization requests data, the request will be reviewed by PGCDSSCoC.

ATTACHMENTS

CONFIDENTIAL
DO NOT SHARE, CITE, QUOTE, OR DUPLICATE WITHOUT AUTHORS' PERMISSION

Attachment A

HMIS Tracking System

Initial Implementation Requirements

This contractual agreement is entered into on ___/_____/_____ between the **HMIS**.

Agency Name ____

Executive Director ____

Name of person completing questionnaire ________________________

Address _________________________ Phone ( ) -_______
_________________________ Fax ____________________
__________________________ Email __________________

This document contains the specific obligations that each agency and PGCDSSCoC must follow in order to participate in the HMIS. The signatory for the document shall be the agency Executive Director or designee.

I. Contractual Requirements and Rules ___________________________
Signature

I agree to abide by the following policies as contained in SECTION 1 of the HMIS Procedures as described below.

A. **Steering Committee:** Advises the project on all activities.
B. **Participating Agency Executive Director:** Assumes responsibility for the entire implementation and administration of the system.
C. **Participating Agency Site Technical Administrator:** The Executive Director's designees to manage operations.
D. **Participating Agency User:** Agency Staff who serve clients who are authorized by the Executive Director to access the system.

II. Participation Requirements ___________________________
Signature

I agree to abide by the following policies as contained in SECTION 2 of the PDCDSSCoCHMITS procedures.

A. ***Participation Requirements of Participating Agency and HMIS***: Layouts responsibilities of all parties involved in implementation.
B. ***Implementation Documentation***: Delineates all written documentation required for implementation including data sharing agreements, clients consent forms, data collection commitment and participating agency security protocols.

C. ***Minimal Data Elements*: ** Participating agencies must make every effort to enter information on all clients served in participating programs. Agencies agree to enter at a minimum, all data contained within the Profile Screen.

D. ***Confidentiality*: ** The Participating Agency will uphold federal and state confidentiality regulations that protect client records and privacy as referenced in 42 CFR Part 2, Health Insurance Portability and Accountability Act (HIPPA) and Maryland general law chapter 66A

E. ***Maintenance of Internet Connection and Onsite Computer Equipment*: ** Outlines responsibility of agency in maintaining connectivity and equipment.

III. Training ____
Signature

I agree to abide by the following polocies as contained in SECTION 3 of the PGCDSSCOC Policies and Procedures as described below.

A. ***Training Schedule: System Admin*** staff will provide schedule and on site training as documented.

B. ***User, Administration and Security Training***: Prior to being granted access to the system, all staff will be trained on relevant information security issues.

IV. User, Location, Physical, and Data Access ____________________________
Signature

I agree to abide by the following policies as contained in SECTION 4 of the PGCDSSCOC procedures as described below.

A. ***User Access***: Identifies process for user access including authorization of user names and passwords.

B. ***Location Access***: Participating agencies must identify the locations from which system software can be accessed.

C. ***Physical Access***: All agencies must develop internal access policies to all systems.

D. ***Data Storage and Transmission***: All agencies will develop internal protocols for the transmission and storage of client level information, System Agency Admin to provide recommendations for policy development.

V. Technical Support And System Availability ___________________________
Signature

I agree to abide by the following policies as contained in SECTION 5 of the PGCDSS policies and procedures as described below.

A. ***Planned Technical Support***: Participating agencies will receive planned technical support as requested.

B. ***Availability***: System software will be made available for set periods of time with time for updates and protocols for unplanned interruption to service.

VI. Data Release Protocols. ____________________________
Signature

I agree to abide by the following policies as contained in SECTION 6 of the PGCDSS policies and procedures as described below.

A. ***Data release Authorization***: Outlines specific policies regarding release of aggregate data.

By Signing this document, I agree to abide by all policies as stated in the PGCDSS policies and procedures Document. I also agree to educate all staff members in my agency as to the policies that directly affect their work.

____
Name of Program

____ ________________
Name/Title of person Completing Questionnaire Date

____
Name of Sponsoring Agency / Signature of Person Completing Questionnaire / Date

_________________________ __________________________________
Executive Director Signature of Executive Director / Date

______________________ ___________________________________
PGCDSSCoC Signature PGCDSSCoC / Date

(HMIS TRACKING SYSTEM)

Program Information

Please complete for each program in the agency which will be linking data to HMIS

Agency Name: ____

Program Name: __________________________________Date ________

Address: ____

City: _______________________ State________________Zip_________

Completed By: ____________________________ Phone: ____________

Type Of Program:
□ Emergency Shelter
□ Transitional Housing
□ Permanent Supportive Housing
□ Supportive Services Only
□ Outreach
□ Other: Specify ________________________

Population Served: □ Individuals □ Families □ Both

Target Population (ex. Youth, Elders, Families with Children, Singles, etc.)
____

Capacity Information: Please use the following categories to identify the number of beds / slots in your program. Select only one category per bed (s) / Slot (s).

	# Individual Beds:	*# Beds entered intoyour database:*
Regular:	_________________	____________________
Winter:	_________________	____________________
Overflow:	_________________	____________________
Hud Funded:	_________________	____________________

Operating Year: From ____/______/____ To _____/_____/___

Additional: _________________________
Explain: ____

# Family Units:

DTA Funded: _________________ _____________________

Community Beds: _________________ _____________________

Additional: _________________ _____________________

Explain: ____

Service Programs

# Slots: __________________ ____________________

HUD Funded: __________________ ____________________

Operating Year: From ____/____/___ To ____/_____/___

Other: ___________________ ____________________

Explain: ____

HMIS

HMIS User Access Form

Program Name: ____
Agency Administrator: ____
Executive Director: ____

Staff Name	Access Level (See Below)	Status (active / inactive)	Authorized By	Date
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

	Resource Specialist I	Resource specialist II	Resource Specialist III	Volunteer	Agency Staff	Case Manager	Agency Admin	Exec Direct	System Oper	Syst Admin I	System Admin II
Client Point											
Profile				X	X	X	X	X		X	X
Employment						X	X	X		X	X
Residential History						**X**	X	X		X	X
Medical Addict							X	X		X	X
Legal						X	X	X		X	X
Military						X	X	X		X	X
Case Notes						X	X	X		X	X
Worksheets					X	X	X	X	X	X	X
HMIS											
Referrals				X	X	X	X	X		X	X
Check in / out				X	X	X	X	X		X	X
Other Services					X	X	X	X		X	X
ResourcePoint	**X**	X	X	X	X	X	X	X	X	X	X
ShelterPoint				X	X	X	X	X		X	X
Reports						**X**	X	**X**		**X**	**X**

Administration											
Add Users							X	X	X	X	X
Remove Users							X	X	X	X	X
Reset Password							X	X	X	X	X
Add Agency									X	X	X
Edit Agency		X	X				**X**	**X**	X	X	X
Remove Agency									X	X	X
Picklist options									X	X	X
Licenses									X	X	X
Other Options									X	X	X

HMIS

Location Access Authorization

Please List the locations and users of each computer that should be registered with HMIS server that can access the Service Point software system.

Location	Computer Description	Users of Computer	Registered With Server PGCDSS

Laptop and Off Site Installation Access Privileges to System Server Commitment Form.

Security Agreement

This agreement is made between PGCDSSCoC and (Agency Name) ____

By signing this security agreement, I agree that I will not allow persons other than Agency authorized staff to use the laptop. I understand that I will only use the Service Point software from locations authorized by the agency as appropriate for entering data. I realize if I access the HMIS software from an unauthorized agency location that I am putting the confidentiality of all of the clients served in this agency at risk.

By signing this document, I agree to abide by the above policies.

______________________________ ____________________
Staff Name Date

______________________________ ____________________
Agency Name Date

PGCDSS Staff Commitment Form Part I

Staff Security Agreement

PRINCE GEORGE'S COUNTY DEPARTMENT OF SOCIAL SERVICES

HMIS STATEMENT OF CONFIDENTIALITY AND REQUIEST OF COC USER

Please complete the following:

Employee Name: ______________________________
(Print)
Agency Name: ________________________________

Important – Please note
New Users and Existing Users must complete this form annually.
If you have any questions regarding the completion of this request, please contact the Prince George's County Department of Social Services Housing and Homeless Services Unit at (301) 909-6346.
After filling out this form, mail it to Prince George's County Department of Social Services at 805 Brightseat Road, Landover, MD 20785. Do not fax this form due to confidentiality issues.

SERVICE AGREEMENT

________________________ ("Agency") agrees to provide resources to persons referred to this service provider for the purpose of facilitating the necessary established goals and outcomes for the individual within the Homeless Services Partnership and on the Service Point Information System (HMIS).

STATEMENT OF CONFIDENTIALITY

I AGREE TO MAINTAIN THE STRICT CONFIDENTIALITY OF INFORMATION OBTAINED THROUGH THE Prince George's County Department of Social Services CoC Homeless Information Management Tracking System. This information will be used only for the legitimate client services and administration of the above named agency. Any breach of confidentiality will result in immediate termination of participation in the Prince George's County Department of Social Services, Office of Homeless Services Continuum of Care Client Tracking Systems.

Employee Signature: ________________________ Date: ___________________

Executive Director
Or Authorized Personnel Signature:____Date:_____________

Part II

REQUEST FOR ACCOUNT

Each user requires a unique username and password (to be kept private). Use of another user’s username (account) is grounds for immediate termination from the Prince George’s County Continuum of Care Homeless Management Information Systems, Office of Housing & Homeless Services Department of Social Services tracking systems (PGCCoCHMISOHHSDSS)

User ID (Assigned by PGCDSS): ___________________________

USER’S RESPONSIBILITY STATEMENT

Your username and password give you access to the Department of Social Services Information Services Center network system. Initial each item below to indicate your understanding of the proper use of your username and password, and sign where indicated. Any failure to uphold the confidentiality standards set forth below is grounds for immediate termination from the Prince George’s County Information Services Center Network system.

Initial Only

_____ I understand that my username and password are for my use only.

_____ I understand that I must take all reasonable means to keep my password physically secure.

_____ I understand that the only individuals who can view PGCCoCHMISOHHSDSS Tracking information are authorized users and the clients to whom the information pertains.

_____ I understand that I may only view, obtain disclose, or use the database information that is necessary in performing my job.

_____ I understand those hard copies of PGCCoCHMISOHHSDSS Tracking information must be kept in a secure file.

_____ I understand that these rules apply to all users of the PGCCoCHMISOHHSDSS Tracking Systems whatever their work role of position.

_____ I understand that once the hard copies of PGCCoCHMISOHHSDSS Tracking information are no longer needed, they must be properly destroyed to maintain Confidentiality.

_____ I understand that if I notice or suspect a security breach, I must immediately notify PGCCoCHMISOHHSDSS at (301) 909-6346.

I understand and agree to the above statements.

Employee Signature: ________________________ Date: _______________

Please mail this form back to:

Prince George’s County Department of Social Services
Office of Housing and Homeless Services
805 Brightseat Road
Landover, MD 20785

Interagency Data Sharing Agreement

The PGCDSSCOC administers a computerized record-keeping system that captures information about people experiencing homelessness, including their service needs. The HMIS system, allows programs the ability to share information electronically about clients who have been entered into software. Client level information can only be shared between agencies that have established an Interagency Sharing Agreement with PGCDSS and have received written consent from particular clients agreeing to share their personal information with other agencies participating with HMIS. The agency receiving the written consent has the ability to "share" that client's information electronically through the HMIS system with a collaborating agency.

This process benefits clients by eliminating duplicate intakes. Intake and exit interviews can be shared, with written consent, between PGCDSSCOC.

By establishing this agreement the PGCDSSCOC agree that within the confines of the HMITS.

1.) HMIS information in either paper or electronic form will never be shared outside of Prince George's County without client written consent.
2.) Client level information will only be shared electronically through HMIS System Agencies that were authorized by the client.
3.) Information that is shared with written consent will not be used to harm or deny any services to a client.
4.) A violation of the above will result in immediate disciplinary action.
5.) Information will be deleted from the system upon client request.
6.) Clients have the right to request information about who has viewed or updated their HMIS record.

We at PGCDSSCOC establish this interagency sharing agreement so that our agencies will have the ability to share client level information electronically through the HMIS System. This agreement does not pertain to client level information that has not been entered into the HMIS system. This electronic sharing capability only provides us with a tool to share client level information. This tool will only be used when a client provides written consent to have an agreement with PGCDSSCOC and have completed security procedures regarding the protection and sharing of client data.

By signing this form, on behalf of our agencies, I authorize the PGCDSS to allow us to share information between our agencies. We agree to follow all of the above policies to share information between our collaborating agencies.

We agree to share the following information (please check all that apply)

□ Basic Client Information
□ Required Data Elements (HUD Universal Data Elements)
□ Children's Required Data Assessment (HUD Data Elements For Children)
□ COC APR
□ ESG CAPER
□ Other (Please Specify)_______________________________________

______________________________ Agency 1	______________________________ Agency 2
______________________________ Printed Name of Executive Director	______________________________ Printed Name of Executive Director
______________________________ Signature of Executive Director	______________________________ Signature of Executive Director
______________________________ Date	______________________________ Date

CLIENT INFORMATION AUTHORIZATION

Service Point Information System
Prince George's County, Maryland

I, ______________________________, hereby authorize _____________________ to exchange any information concerning my history, and/or that of my immediate family, care, treatment, household demographic, housing issues, income, assets or benefits between directors, agencies, and staff of the Service Point Information System listed herein. The purpose of this release is to protect my privacy, help staff make referrals and to help me or my family receive better planning and delivery of services.

I understand that the aforementioned information will be communicated to other agencies using this computer system in several ways, one of which will include communication through a computer-based system that uses telephone lines to send and receive information. The highest level of security measures will be used to protect the information sent and received by telephone. Only authorized personnel will be able to view my personal information.

I understand that the System Administrator, the Prince George's County Department of Social Services, Office of Housing and Homeless Services, has personnel authorized to view my personal information.

Information entered into the Service Point Client Profile, which is basic demographic and services, will be shared with all agencies that participate in the Service Point System in Prince George's County.

This release authorizes a free exchange of information between agencies for one year in order to give the most complete and thorough services available. I understand that I may revoke this authorization at anytime.

______________________________ ______________________________
Print Name Social Security Number

______________________________ ______________________________
Signature Date

______________________________ ______________________________
Signature of parent, guardian, or authorized representative when required Date

______________________________ ______________________________
Witness Date

I understand that my records are protected under federal regulations and cannot be disclosed without my written consent or as otherwise permitted by such regulations, and that in any event this consent expires one year from the date of entry or upon my departure from further service provider participation.

[CURRENT HMIS MEMBER LIST TO BE ATTACHED]

AGENCIES AND PROGRAMS WITH ACCESS TO SERVICE POINT IN PRINCE GEORGE'S COUNTY

Aid of Humanity
Bethel House
Bowie Interfaith Pantry and Emergency Aid Fund
Wellsky
Center for Therapeutic Concepts
Community Crisis Services
Community Ministry
Covenant House Washington
DCVET
Department of Corrections
Department of Family Services
Department of Housing and Community Development
Department of Human Resources/Community Services Administration/ Office of Transitional Services
DLLR One Stop
Easter Seals
Family Crisis Center
Family Preservation
FES Oxon Hill
FES Oxon Hill
Friendship Place
Homeless Hotline
Housing Initiative Partnership
iMind
Jobs Have Priority
Kristin's Place
Laurel Advocacy & Referral Services
Maryland Department of Housing and Community Development (TBD)
Maryland Department of Juvenile Services – Metro Region
Maryland Mental Hygiene Administration
Maryland Multicultural Youth Center (MMYC) /Latin American Youth Center (LAYC)
MCVET
New Vision House of Hope
People Encouraging People (PEP)
Prince George's Community College
Prince George's Community College Upward Bound
Prince George's County Department of Social Services
Prince George's County Economic Development Corporation
Prince George's County Health Department
Prince George's County Public Schools
Prince George's House
Prince George's Vet Center
Quality Care, Inc.
Rehabilitation Systems, Inc.
Salvation Army Rehab
Sasha Bruce Youthwork
Sexual Minority Youth Assistance League (SMYAL)
St. Ann's Infant and Maternity Home
The Believers Worship Center/See the Other Side Re-Entry Program
Transitional Housing Programs
U.S. Department of Veterans Affairs
United Communities Against Poverty (UCAP)
United Way of Central America (TBD)
US Army 310 ESC
VESTA Inc.
VA Benefits/Readjustment
VA Health Suite
VA Mobile Vet Center
VA Outreach
Veterans Forever Inc.
Volunteers of America Chesapeake VOA)