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

Policies and Procedures Manual

Contents

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 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 county. 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.

The 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 gather 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 CoC APR, ESG CAPER, RHYMIS Export, PIT, HIC, System Performance Measures (SPM), and LSA Export.

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 reports, 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 System Administrators are responsible for overseeing usage of the application HMIS and being available for phone support as needed.

Responsibilities and Duties of the System Administrators/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 System Administrators/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 System Administrators/Staff will review all network and security logs regularly.

All Agency 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 Agency 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 AGENCY ADMINISTRATOR

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

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

Purpose: To outline the role of the Agency Administrator.

Scope: Participating Agencies.

Responsibilities:

The participating agency agrees to appoint one person as the Agency 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 System Administrator is 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.
- If the Executive Director/Program Manager has HMIS Policies or Procedures that they want implemented in addition to the above, please notify System Administrators.

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 Lead 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 plan 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**.

- **Identification of Agency Administrator:** Designation of one key staff person to serve as Agency 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.

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

- **Training:** Commitment of Agency 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 **HMIS Participation Agreement** 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 Information Authorization Forms (ROI)** 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 HMIS Participation Agreement

- **Minimal Data Elements:** Agencies will be required to enter HUD Universal data elements as defined by the HMIS Project and its HMIS 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 Agency 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 Lead. 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: HMIS Participation Agreement and
Interagency 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 Plan. 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 the Resource module.

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 Lead.

C. Agency 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 Information 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 with an oral explanation and 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 HMIS 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 managers and clients 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 collect all data contained within the Profile Screen, Entry/Exit, Residential Assessment.

Standard: All agencies will collect universal data elements.

Purpose: To ensure that agencies are collecting quality data.

Scope: All Participating Agencies

Procedure: **Agency Staff completes the following based on Client interviews:**
Name
Social Security Number
Date of Birth
Race and Ethnicity
Gender
Veteran Status
Relationship to Head of Household
Client Location
Prior Living Situation
Housing Move-In Date (only required for PH, PSH, and RRH)
Disabling Condition
Creates a Project Start Date (Entry Date)
Creates an Exit (once Client exits project)
Destination (once Client exits)
Income
Non-Cash Benefits
Place in shelter Bed (if appropriate)

Commitment to Utilization of Interview Protocol

Universal Data Elements: The Participating Agency is responsible for ensuring that all clients are asked the questions contained within the Profile Screen, Entry/Exit, and Residential Assessment. Data will be used in aggregate analysis.

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
- Access to a secure VPN (remote/telework)
- 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 12 Mbps) whether through a wired connection, wireless connection, or wireless hotspot.

Standard: Any Internet connection greater than 12 Mbps 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 12 Mbps 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 of user equipment.

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

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 the 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 external devices (such as thumb drive or 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 System News in HMIS. Users will register for training there. They will receive their link. The training is virtual. After attending HMIS Training the staff will receive an HMIS and Evaluation Assignments. The staff person must complete. Once the assignments have been completed and they receive a passing score. They will receive the User Agreement to complete and return. In order to gain access to HMIS live site.

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

Title: USER and Agency ADMINISTRATOR

Policy: All users will undergo security training is done during the User Training. . 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 are 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. Agency Administrators must also attend an Administrator training and a Report Writer training in addition to a user training. Agencies will be notified of scheduled training sessions.

Training:
The Participating Agencies Agency 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 System or Agency Administrator. The System or Agency Administrator will generate username and passwords within the administrative function of HMIS.

B. User name format: The System or Agency 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. System or Agency 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 8 to 50 characters long with a mix of numbers, special characters, and upper and lower case letters.

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

4. If a user forgets their password, they can use the Forget Password feature to re-set their password. Please check spam or junk mail to see if a link appears, if that doesn't work, contact System or Agency Administrator(s) . The Agency Administrator is responsible for making sure the User Contract has not expired. If the User contract has expired the Agency or System Administrators must have the User sign a new User Contract on a yearly basis.

5. **Termination or Extended Leave from Employment:** The System or Agency 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 User account should be inactivated within 5 business days of the start of their leave. The System Administrator is responsible for removing users from the system.

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 Agency Administrator under authorization of the Participating Agency's Program Manager.

Designation of HMIS Users

User Levels: There are 4 levels of access to the HMIS system that are used in the Prince George's County HMIS. 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.

Case Manager	Case Managers have access to all features excluding administrative functions. They have access to all screens within the Clients module, 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 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-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 becomes 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 this 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 have 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 USB port or thumb drives 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 Agency 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 Prince George's County HMIS. Authorized employees, using methods deemed appropriate by the participating agency, may transport HMIS data that meets the above standard. Reasonable care should be used, and media should be secured when left unattended.
- Internal or External 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 internal or external 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 log on 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 8 to 50 characters long with a mix of numbers, special characters, and upper and lower case letters.
- 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.
- Any password written down should be securely stored and inaccessible to other people. Users should **not** store passwords on a personal computer for easier log-in.

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 Agency Administrator. Passwords will be communicated in written or verbal form. The first time a temporary password can be communicated via email. *Forced Password Change (FPC)*
  FPC will occur every forty-five days once a user account is issued. Passwords will expire and the 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 log-in 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.
  Forget Password

If a User has forgotten their password, they can use the Forget Password functionality to reset their password. The Reset Password link will be sent via email. It may appear in Junk Mail or Spam folder. If the Reset Password link does not work, the user will need to contact the System or Agency Administrator.

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 violations 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-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 Agency 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 is 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:

WellSky understands the significance of keeping our clients information confidential. They are committed to protecting that information pursuant to the legal standards created by the Federal and State requirements.

The "Solution Security Posture – Community Services" document in the appendix outlines the measures taken by WellSky to secure all client data on our HMIS. This document provides an overview of WellSky's approach to information security and its practices to secure data systems and services aligned around the five functions of the National Institute of Standards and Technology Cybersecurity Framework for network security. In addition, it outlines the specific privacy and security practices to make sure to adhere to the HIPAA requirements. Here are some of the features:

Identification & Authentication

- Dual factor, unique user name and password controls
- Restrictive password requirements
- Randomly generated, one-time temporary passwords
- Grant access only to customer authorized networks

Restricted Access

- Customer configurable
- Restrict access as to time and scope, down to file level
- Access rights can be restricted at system of user level
- Ability to mask logon credentials
- Integration and Active Directory

Audit Controls

- Real time monitoring
- High definition audit reports
- Details log files
- Unilateral ability to terminate session at any time

Secure Data Transfer

- Customer configurable levels of encryption

Finally, three levels of security: System, Operational, and Data Center.

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 regarding the use of the system software. In addition, System Administrative staff will use a Help Desk ticketing system to provide technical assistance to track user support requests.

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

Scope: System Wide

Procedure: System & Agency Administrative Staff

For the System Administrative Staff, technical support is initiated when the user creates and submits a ticket to the Help Desk system by email or on a form. One of the System Administrative Staff will assign themselves to the support request and work on it. The Help Desk System is accessible through the internet. If needed, the System Administrative Staff will use a virtual face-to-face option to research the issue further with the user.

The System & Agency Administrative Staff provide the following:

- New user training
- Refresher training
- Report writing training
- On-going technical assistance

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 Agency Administrator. If no Agency Administrator exists, requests can come from users directly to System 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 Agency Administrator) or the Agency Staff contacts a System Administrator for service using the Help Desk system.

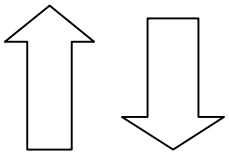
B. The assigned System Administrator determines resources needed for the service.

C. The System Administrator contacts the Agency Management Staff or Agency Staff through the Help Desk system to work out a mutually convenient service schedule and obtains the resolution.

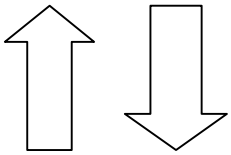
D. See Chain of communication on the following page.

Chain of communication

System Administrator



Agency Management staff – Executive Director or Agency Administrator



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 user's 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 24 hours a day, 7 days a week except when the System is down for maintenance or updates.

SOP#: TSS-004 **Revision:** **Prepared by: HMIS**

Effective date: 07/05 **Revision date:** **Revised by:**

Title: AVAILABILITY: System Administrator 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

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

Title: AVAILABILITY: INTERRUPTION TO SERVICE

Policy: System Administrator will inform participating agencies of any planned interruption to service. Participating Agencies may or may not be notified in advance of unplanned interruption to service.

Standard: Participating Agencies will be notified of planned interruption to service prior to the interruption. Participating Agencies will be notified of unforeseen interruptions to service that are expected to exceed two hours.

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

Scope: System-wide

Procedure:

Planned Interruption to Service

System Administrator will notify Participating Agencies via HMIS Newsflash, e-mail 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 service has resumed.

SECTION 6:

Data Release Protocols

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 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 is 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 the 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 PERSONALLY IDENTIFIED INFORMATION

Policy: PGCDSSCOC retains authority to deny access to all clients personally 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 <u>every</u> 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

HOMELESS SERVICES MANAGEMENT INFORMATION SYSTEM (HMIS)
PARTICIPATION AGREEMENT

Project Name: _____

The providers of the numerous services offered to the Department's Homeless Customer base will be required to manage and operate a HMIS web-based information management system that provides client tracking and case management, service and referral management, bed availability for shelters and food banks, resource indexing and reporting.

HMIS has been subdivided into several different functional modules. The modules' designs make the software easier to use and understand. Most of the modules can be used independently of one another, allowing staff members to learn only the parts of the software needed for their job. On-site training provided by the Contractor and the Department's Homeless/Housing Service Unit Project Coordinator will clarify end-user operation of the system.

The modules for the system will capture all services that may be available to a client. The system operator will be able to see all the services a client has received in the past, but it also indicates any needs the client has that have not yet been met.

HMIS Management Structure - The Prince George's County Department of Social Services (PGCDSS), who provided the system, will hire all system administration staff as direct employees of the organization. The Department of Social Services will be responsible for the central server functions, management of accounts, data storage and analysis, system security, site technical assistance and training. Even with this model, project consultation is often used to supplement staff, e.g. system assessment and set-up, security testing and legal advice.

For the purposes of this *Attachment* document, the **Department of Social Services** is herein referred to as the **HMIS Lead**, the **Contractor** will be referred to as the **Participating Agencies** (P/A) and **System Operators** will be referred to as **Users**.

IT IS HEREBY AGREED THAT THE PARTICPATING AGENCY RESPONSIBILITIES WILL INCLUDE:

I. **PARTICIPATION REQUIREMENTS/ROLES AND RESPONSIBILITIES:**

A. Provide High Speed Internet Connectivity
B. Identify Agency Administrator to serve as primary contact.
C. Complete security assessments and signed contract for the user.
D. **LICENSES –** Each P/A has been allocated a previously agreed upon number of licenses. If additional licenses are desired, it is the P/A

responsibility to purchase additional licenses for their agency. The cost is about $185 per user.

II. **IMPLEMENTATION REQUIREMENTS:**

A. **INTERAGENCY DATA SHARING AGREEMENTS** – Agencies that will be sharing client specific records must agree in writing to uphold the same standards of privacy protection.

B. **WRITTEN CLIENT CONSENT PROCEDURE FOR ELECTRONIC DATA SHARING (ROI) -** Agencies that will be sharing client specific records must have documented releases of information from each client.

C. **DATA COLLECTION COMMITMENT** – Participation in the HMIS project requires that all participating programs collect certain data elements on all consenting clients (as detailed in the HMIS Policies and Procedures Manual)

E. **INFORMATION SECURITY PROTOCOLS –** Internal policies must be developed at each site to establish a process for the violation of any of HMIS's information security protocols.

F. **IMPLEMENTATION: CONNECTIVITY –** Once implementation has begun each site agrees to maintain connectivity in order to continue project participation (as detailed in the HMIS Policies and Procedures Manual).

G. **MAINTENANCE OF ONSITE COMPUTER EQUIPMENT –** Each agency agrees to maintain computer equipment in order to continue project participation (as detailed in the HMIS Policies and Procedures Manual).

H. **CONVERSION OF LEGACY DATA -** Agencies that are using legacy systems that request data conversion must provide resources and processes to enable conversion unless specific contracts have been established to provide the conversion at no cost.

III. **TRAINING :**

A. **TRAINING SCHEDULE –** HMIS Lead provides ongoing training on all relevant aspects of system operation for the duration of the project. Training modules are developed based on skill level and type of access to the system. Each user of the system is required to complete basic user training in order to begin using the system.

B. **PHYSICAL ACCESS CONTROL -** All equipment or media containing HMIS data must be physically controlled at the central site. Protections and destruction policies vary depending on the type of data and media.

C. **LOGICAL ACCESS -** Access to system resources must be limited to authorized users for authorized transactions.

D. **UNIQUE USER ID AND PASSWORD -** Each user of the system must be individually and uniquely identified. Identification will be verified through a password.

E. **AUDITING: MONITORING, VIOLATIONS AND EXCEPTIONS -** HMIS considers any exception to stated security policies a violation of those policies that must be investigated.

F. **LOCAL DATA STORAGE –** If agencies choose to store local copies of data they are encouraged to develop policies and procedures on how data is generated, stored, and destroyed.

G. **PARTICIPATING AGENCY SERVICE REQUEST -** Service requests from participating agencies must originate from either the Executive Director or Agency Administrator or Users if Agency Admin does not exist.

H. **RAPID RESPONSE TECHNICAL SUPPORT -** Requests for service during a business day that requires a rapid response will be responded to within (1) business day.

I. **PROVIDE TECHNICAL AND USER SUPPORT -** For HMIS software including agency account set-up, system monitoring problem diagnosis and resolution, routine software and data maintenance.

J. **PROVIDE/COORDINATE ON-GOING TRAINING** - Technical support for the system. Support the end user in the use of the software, troubleshooting software problems by phone and virtual.

GENERAL INFORMATION - SYSTEM AVAILABILITY:

A. **AVAILABILITY: HOURS OF SYSTEM OPERATION –** The system is available to users everyday, 24 hours a day. The system is periodically scheduled for two 2-hour time blocks of potential downtime and the System Administrator will provide notice to users when the system is unavailable and users can resume

B. **AVAILABILITY: SYSTEM ADMINISTRATOR(S) AVAILABILITY -** System administrator(s) are available during normal business hours to respond to service requests.

C. **AVAILABILITY: PLANNED INTERRUPTION TO SERVICE –** Participating agencies will be notified of planned interruptions to service prior to the interruption. **AVAILABILITY: UNPLANNED INTERRUPTION TO SERVICE -** In the event of an unplanned interruption to service System Administrator(s) will make a determination if the cause can be repaired. The System Administrator(s) will let the users know when they can expect the system to be available.

IV. CONFIDENTIALITY REQUIREMENTS:

A. Responding to client information requests

B. Maintaining record for requests and responses

C. Training other employees

D. Maintaining library of confidential information

E. Maintaining Confidentiality Commitments signed by all employees

F. Reviewing Computer Security

G. Securely storing thumb drives and any other external devices

H. Limiting access to computers

I. Protecting online information protected by passwords

J. Protecting information that is too sensitive by not storing it on computer.

K. Identifying clients only by Client ID

L. Interagency agreements should require other agencies to take the same measures

Right to Deny Access To Personally Identifiable Information – All users of the HMIS cannot release personally identifiable information to any third party. Court orders for information will be forwarded to DSS for review. No release will occur unless the party obtains the written release of every client within the database prior to receiving the database.

IT IS HEREBY AGREED THAT THE DEPARTMENT OF SOCIAL SERVICES (HMIS LEAD) RESPONSIBILITIES WILL INCLUDE:

I. **PARTICIPATION REQUIREMENTS/ROLES AND RESPONSIBILITIES:**

A. Provide the software that is required to manage and operate this Internet based system.

B. During program implementation, PGCDSS will provide:

1. Software licensing
2. Custom programming
3. Interface design
4. Project management
5. Data conversion (Will be done by WellSky at the P/A's expense)
6. Training and ongoing support

C. Assure that only trained, designated staffs have access to the data.

D. Assign log-on and user licenses to end-users.

E. Monitor security and confidentiality requirements for participating agencies.

F. Monitor integrity of agency input of data into HMIS.

II. **IMPLEMENTATION REQUIREMENTS:**

A. **Implementation: Stage 1. Start-up and Initial Training – Implementation begins with Stage 1. To enter Stage 1 an agency must complete all requisite paperwork and create user accounts on the system.**

B. **Implementation: Stage 2. Data Entry Begins -** To enter Stage 2 an agency must begin entering data on their client population. To move to Stage 3 an agency must be entering information on at least 25% of their clients or entering information for 2 continuous months.

C. **Implementation: Stage 3. Universal Data Elements On Most Clients -** Stage 3 lasts for 6 months. Agencies must move out of Stage 3 within six months. In order to move out of Stage 3 an agency must be entering universal data elements on at least 60% of their client population.

D. **Implementation: Stage 4. System Fully Integrated In Daily Operation –** Stage 4 is the final stage of implementation. To classify as Stage 4 an agency must be entering information on 100% of their

client population or be continuously entering information for at least 12 continuous months.

III. **TRAINING TOPICS:**

A. Why client information should be kept confidential

B. Specific information the agency needs

C. Why this information is needed

D. The types of information the agency will share

E. Why this information will be shared

F. Protocol for fielding client information requests

G. Applicable confidentiality laws

H. Requirements for informed consent

I. How to interact with the client to be sure consent is informed

J. Sensitivity to language and culture

K. Role and scope of interagency agreements and court orders

L. Scheduled Training Delivery – Agrees to provide a regional basis as needed.

M. On-Site Training – HMIS Lead is available to deliver virtual training in the event that an agency has a large number of staff to train. Department of Social Services will not deliver one to one training on-site. If Agency trainer is not able to provide training then Department of Social Services will provide the necessary training.

N. Planned Technical Support – HMIS Lead offers a standard technical support package to all participating agencies. Support services include training, implementation support, report writing support, and process troubleshooting.

O. Right To Deny User And Participating Agencies' Access – HMIS Lead retains the right to suspend or revoke the access of any agency or individual to the system for consistent or egregious violation of HMIS policies.

P. Data Access Control – Access to the system must be audited. All audits must be reviewed regularly.

HANDWRITTEN SIGNATURE OF AUTHORIZED PRINCIPAL(S):

Operating Agencies: _____

Print Name: _____

Title: _____

Signature: _____

Date: _____

PRINCE GEORGE'S COUNTY DEPARTMENT OF SOCIAL SERVICES

HMIS STATEMENT OF CONFIDENTIALITY AND REQUEST OF COC USER

Please complete the following:

Employee Name: _____
(Print)

Agency Name: _____

Employee E-Mail Address: _____
(Print Clearly)

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 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 Community Services Division (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 Management Information 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, Homeless Management Information System.

Employee Signature: _____ **Date**: _____

Executive Director's or
Authorized Personnel Signature: _____Date: _____

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 Department of Social Services Continuum of Care tracking systems (PGCDSSCOC)

User ID (Assigned by PGCDSSCOC): _____

_____

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 Homeless Management Information 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 PGCDSSCOC 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 PGCDSSCOC Tracking information must be kept in a secure file.

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

_____ I understand that once the hard copies of PGCDSSCOC 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 PGCDSS 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
Community Service Division
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 system, HMIS, allows programs the ability to share information electronically about clients who have been entered into the software. Client level information can only be shared between agencies that have established an Interagency Sharing Agreement with PGCDSSCOC 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 HMIS.

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 PGCDSSCOC 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
Client Demographics
Household Composition
Entry/Exits into Participating Programs
Required Data Elements (HUD Universal Data Elements and Program Specific Data Elements)
HUD Data Elements For Children
HUD Assessments
Shelter Stays
Income/Benefits
Disabilities
Case Notes
Federal Partner Program Specific Assessments (PATH, RHY, SSVF)
File Attachments
Services
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
Homeless Management 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 Homeless Management 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 at the Prince George's County Department of Social Services, Community Services Division, has personnel authorized to view my personal information.

Information entered into the HMIS Client Profile, Entry and services, will be shared with all agencies that participate in the HMIS 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 HMIS
IN PRINCE GEORGE'S COUNTY

ACIS
Aid of Humanity
Bowman Internet Systems
Center for Therapeutic Concepts
Community Crisis Services (CCSI)
Covenant House Washington
DCVET
Department of Corrections
Department of Family Services
Department of Housing and Community Development (Prince George's County Offices)
Department of Human Resources/Community Services Administration/ Office of Transitional Services
Family Preservation
FES Oxon Hill
Friendship Place
Homeless Hotline
Housing Initiative Partnership
House of Ruth
JHP (Jobs Have Priority)
Kristin's Place
Laurel Advocacy & Referral Services (LARS)
Maryland Department of Housing and Community Development
Maryland Department of Juvenile Services – Metro Region
Maryland Mental Hygiene Administration
Maryland Multicultural Youth Center (MMYC) /Latin American Youth Center (LAYC)
Maryland University- Fostering Terps
MCVET
Mission of Love
People Encouraging People (PEP)
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
Promise Place
Quality Care, Inc
Salvation Army Rehab
Sasha Bruce Youthwork
Shepherd's Cove
St. Ann's Infant and Maternity Home
DSS Transitional Housing Programs
U.S. Department of Veterans Affairs
United Communities Against Poverty (UCAP)
US Army 310 ESC
US Vets
VESTA Inc.
Volunteers of America Chesapeake VOA)
Youth Connection- Outreach

Revised 8/18/2023

CLIENT YOUTH INFORMATION AUTHORIZATION
Homeless Management Information System (HMIS)
Prince George's County, Maryland

Youth Name: _____Date of Birth: _____

Your personal information is kept in an electronic case record which is secure but can be viewed by the organization listed above as well as those listed on the back of this form. It is important that we are able to share the information that you have given us during our work with you for any of the following reasons:

- To share necessary information with other workers in the shelters, schools or county agencies to avoid asking you the same question more than once
- To gather information needed to help you access appropriate shelter and service
- To share basic information with other service providers in order to coordinate services and referrals for you and your family
- To gain a better understanding of how many homeless/runaway youth there are in our County and what services are needed for their success.

By signing this form, you are stating that you understand the following:

1. I understand that the information I provide about myself may be seen by the agencies listed above, below and on the back of this form for the purposes listed above;
2. I understand that the sources listed above, below and on the back of this form may share information about me for the purposes listed above;
3. I understand that the System Administrators (the persons responsible for working on the HMIS) may view my personal information;
4. I understand that my information may be used in order to gain a better understanding of how many homeless/runaway youth there are in our County and what services are needed for their success.

Shelter/Program Name: _____

School District: _____

_____ _____
Youth Signature Date (good for one year from date)

_____ _____
Parent/Guardian signature (if available) Date (good for one year from date)

Established 9/9/2022

PROVIDER CONFIGURATION WORKSHEET

DISCLAIMER:

THIS DOCUMENT IS NOT MEANT TO BE ALL INCLUSIVE. IT IS INTENDED TO BE A STARTING POINT FOR PROVIDER SET UP AND WILL REQUIRE ADMINS MEETING WITH AGENCIES FOR FULL COMMUNITY SERVICES SET UP.

IF YOU HAVE ANY QUESTIONS WHILE FILLING OUT THIS DOCUMENT, PLEASE CONSULT YOUR SYSTEM ADMINISTRATOR.

PROVIDER INFORMATION

Provider Name: _____

Agency/Program (AKA): _____

Parent Provider: _____

Provider Profile Image: **Yes** ☐ **No** ☐

NOTE: If yes, please provide an electronic file to upload)

HUD/HMIS Provider:	☐
AIRS Compliant:	☐
Uses Community Services:	☐
Operational:	☐

PROFILE – PROVIDER PROFILE

Description:

Module Access Settings

☐	Provider Uses ActivityPoint	☐	Provider Uses CallPoint
☐	Provider Uses ClientPoint	☐	Provider Uses Eligibility
☐	Provider Uses Measurement Tools	☐	Provider Uses Medicaid Billing Module
☐	Provider Uses SkanPoint	☐	Provider Uses FundManager
☐	Provider Uses ShelterPoint	☐	Other:

Location Information

PRIMARY ADDRESS

Address Type:			
Street Address:			
Additional:			
Zip:	**City:**	**State:**	**County/Parish:**
Area:		**Landmarks:**	

ADDITIONAL ADDRESS

Address Type:			
Street Address:			
Additional:			
Zip:	**City:**	**State:**	**County/Parish:**
Area:		**Landmarks:**	

ADDITIONAL ADDRESS

Address Type:			
Street Address:			
Additional:			
Zip:	**City:**	**State:**	**County/Parish:**
Area:		**Landmarks:**	

Contact Information

CONTACT NUMBERS

Primary Number:	**Description:**
Number:	**Description:**
Number:	**Description:**

CONTACT PERSONAL

Primary Contact Name:		**Description:**	
Title:		**Email:**	
Phone Number (Ext):		**Website Address:**	
Note:			
☐ **Hide from Provider Profile**		☐ **Receives Email**	

Additional Contact Name:		**Description:**	
Title:		**Email:**	
Phone Number (Ext):		**Website Address:**	
Note:			
☐ **Hide from Provider Profile**		☐ **Receives Email**	

Additional Contact Name:		**Description:**	
Title:		**Email:**	
Phone Number (Ext):		**Website Address:**	
Note:			
☐ **Hide from Provider Profile**		☐ **Receives Email**	

Additional Information

Website Address:	**Hours:**
Program Fees:	**Intake/ Application Process:**
Eligibility:	**Languages:**
Volunteer Opportunities:	**Wishlist:**
Accessibility:	**Other:**

☐	**Handicap Access**	☐	**Brochures**	☐	**Show On Public Site**
☐	**Printed Directory**	☐	**Is Shelter**		

Shelter Requirements:

PROFILE – PROVIDER PROFILE

HMIS Participation Status

Status: (Participating, Non-Participating, or Comparable Database Participation)	Participation Start Date:	Participation End Date:

AIRS Standards Information

AIRS Designation:	Agency: ◯ Site: ◯	Federal Employer ID Number:
Type of Facility or Organization:		
Year of Incorporation:	Legal Status:	
Capacity Type:	Service Capacity:	
Provider Maintaining:		
Type of License / Accrediting Bodies:		

Payment Methods Accepted:	☐ Cash/Checks	☐ Medicaid
	☐ Credit Card	☐ Medicare
	☐ Insurance	☐ No fees/charges

HUD Standards Information

Organization Identifier:	Project Type:
If PH-Rapid Re-housing, Identify sub type (RRH: Housing with or without Services, RRH: Services Only):	
If Services Only for "Project Type" or *RRH: Services Only* subtype, is it affiliated with a residential project?	
If yes for "Affiliated with a residential project" Please list the project ID(s) of residential project(s) affiliated with SSO or RRH: Services Only project:	

Principal Site:		Target Population:
Geocode:		Method for Tracking Emergency Shelter Utilization:
Continuum Project:	Provider Grant Type:	Service Transaction Workflow (Program does not use Entry/Exits)

Coordinated Entry Participation Status

Project is a Coordinated Entry Access Point?	
Project Receives CE Referrals?	Provided by CE Project ☐ Homeless Prevention Assessment, Screening, and/or Referral ☐ Crisis Housing Assessment, Screening, and/or Referral ☐ Housing Assessment, Screening, and/or Referral ☐ Direct Services (search and/or placement support)
CE Participation Status Start Date:	CE Participation Status End Date:

Bed and Unit Inventory

Bedlist Name:		Bed Inventory:
Household Type:	Bed Type:	Availability:

Of the total inventory what number of beds are dedicated to:

Chronic Homeless Bed Inventory (PSH Only):	Veteran Bed Inventory:	Youth Beds Inventory:

Of the youth beds, what number are restricted to:

Only under age 18:	Only Ages 18 to 24:	Only under age 24:
Unit Inventory	Inventory Start Date	Inventory End Date
HMIS Participation Beds:	HMIS Participation Start Date:	HMIS Participation End Date:
Target Population A:	Target Population B:	
McKinney Vento Funding		

Bed and Unit Inventory

Bedlist Name:		Bed Inventory:
Household Type:	Bed Type:	Availability:

Of the total inventory what number of beds are dedicated to:

Chronic Homeless Bed Inventory (PSH Only):	Veteran Bed Inventory:	Youth Beds Inventory:

Of the youth beds, what number are restricted to:

Only under age 18:	Only Ages 18 to 24:	Only under age 24:
Unit Inventory	Inventory Start Date	Inventory End Date
HMIS Participation Beds:	HMIS Participation Start Date:	HMIS Participation End Date:
Target Population A:	Target Population B:	
McKinney Vento Funding		

Bed and Unit Inventory

Bedlist Name:		Bed Inventory:
Household Type:	Bed Type:	Availability:

Of the total inventory what number of beds are dedicated to:

Chronic Homeless Bed Inventory (PSH Only):	Veteran Bed Inventory:	Youth Beds Inventory:

Of the youth beds, what number are restricted to:

Only under age 18:	Only Ages 18 to 24:	Only under age 24:
Unit Inventory	Inventory Start Date	Inventory End Date
HMIS Participation Beds:	HMIS Participation Start Date:	HMIS Participation End Date:
Target Population A:	Target Population B:	
McKinney Vento Funding		

Funding Partner Program

Federal Partner Program:		**Grant Identifier:**	
Grant Start Date:		**Grant End Date:**	
Federal Partner Program:		**Grant Identifier:**	
Grant Start Date:		**Grant End Date:**	
Federal Partner Program:		**Grant Identifier:**	
Grant Start Date:		**Grant End Date:**	

SERVICES

Search Terms Information

Areas (CoC) Served (I.E. North, Central, South-Central etc.)			
Geography Served:			
State:	**County/Parish:**	**City:**	**Zip Code:**
Does this project serve all geographies (NOTE: Includes all US geographies): ☐ **Yes** ☐ **No**			

Services Provided

Primary Services *(AIRS Taxonomy Codes)*	**Secondary Services** *(AIRS Taxonomy Codes)*	**Occasional Services** *(AIRS Taxonomy Codes)*	

			NOTE: Service Details, Target Populations, Modalities and Eligibility requirements are not included in this document. Please refer to the Provider Admin Services Document.
Emergency Support Functions (ESF):			
Service Quick List:			
Eligibility Service Quick List:			
Referral Quick List:			

Provider-Specific Locations:						
Provider-Specific Staff:						
Provider-Specific Services:						
Service History Display (Select up to seven in the order to be displayed from left to right)						
Need History Display (Select up to seven in the order to be displayed from left to right)						
Provider Service Unit Types: (I.E. Month Arrears, Nights of Stay, Tokens, Hours, Minutes, etc.)						

WellSky Community Services
Systems and Solutions Security Posture

Version 2

Release Date: November 2022

Contents

Scope

The intent of this document is to supply healthcare providers with important information about how WellSky protects personal and confidential data, including protected health information (PHI), that WellSky may receive on behalf of its clients. This document should:

- Help our clients understand how we address security and compliance
- Include solution-specific information addressing the technical privacy and security related attributes of the individual solution model
- Provide a simple, flexible way of collecting administrative, physical, and technical solution and service-specific elements of the common information needed by healthcare providers during information requests and risk management activities

Information provided in this document is intended to help our clients and potential clients understand our commitment to security and evaluate our overall security program. The information within this document is not intended for other purposes.

WellSky

Privacy Practices

WellSky understands that certain information about our clients' and individuals whom our clients serve, or service users is personal and confidential. We are committed to protecting that information pursuant to the legal standards created by Federal and State requirements. Therefore, WellSky has implemented reasonable and appropriate privacy practices with the intention of helping to ensure that Individually Identifiable Health Information (IIHI) about the past, present, or future health condition of any teammate, or any of our clients' patients' Protected Health Information (PHI) as defined by HIPAA, and any Personally Identifiable Information (PII) as defined by applicable law, is treated appropriately by WellSky.

WellSky maintains reasonable and appropriate safeguards to help protect the confidentiality and integrity of personal and confidential information that is collected, received, maintained, and/or disseminated by WellSky pursuant to services provided for clients under the applicable agreement(s). The implemented Privacy Practices establishes WellSky's commitment to fully complying with applicable State and Federal regulations.

WellSky teammates will only have access to personal and confidential information in connection with the provision of services, as agreed upon, under the terms of the Contract, Business Associate Agreement (BAA), or Data Use Agreement (DUA), as applicable. It is expected that such access to personal and confidential information will be limited to the determined need for access. WellSky will implements role-based access to personal and confidential information per job description. For any type of use or disclosure, WellSky asks that our clients provide us with access only to the minimum amount of information necessary to complete the intended use, and WellSky will limit our use or disclosure to the minimum necessary to achieve the purpose of the use or disclosure.

Security Practices

The need for effective cybersecurity to ensure solution functionality and safety has become more important with increasing use of wireless, Internet-and network-connected devices, portable media, and the frequent exchange of solution related health information. In addition, cybersecurity threats to the healthcare sector have become more frequent, more sever, and more clinically impactful. Such cyberattacks, and exploits can delay diagnosis and/or treatment and may lead to patient harm.

As a leader in Health Information Technology Solutions, WellSky has an ethical, legal, and professional duty to ensure that the information it holds conforms to the principles of confidentiality, integrity, and availability. We must ensure that the information we hold or are

responsible for is safeguarded against inappropriate disclosure; is accurate, timely, and attributable; and is available to those who should be able to access it.

WellSky places great importance on information security, including cybersecurity, to protect against internal and external threats. WellSky's cybersecurity strategy prioritizes detection, analysis, and response to known, anticipated or unexpected cyber threats, effective management of risk, and resilience against security incidents. WellSky continuously strives to meet or exceed the industry's information security best practices and applies reasonable and appropriate controls to protect our clients and WellSky. WellSky maintains a formal information security program structured around the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and related industry standards.

This document provides an overview of WellSky's approach to information security and its practices to secure data systems and services, similarly, aligned around the five functions of the NIST CSF:

Identify

- Risk Governance and Oversight
- Information Security and Cybersecurity Policies and Standards
- Asset Management

Protect

- Training and Awareness
- Identity and Access Management
- Application and Software Security
- Infrastructure Security
- End User Device Security
- Data Protection and Data Privacy
- Physical Security
- Vendor Security

Detect

- Continuous Monitoring
- Anomaly Detection
- Enforcing Protective Measures

Respond

- Security Incident Management
- Response Planning

Recover

- Business Continuity Planning and Disaster Recover Planning

While information security measures will evolve over time and may differ across WellSky's business lines, this document provides an overview of our security practices. WellSky does not represent that this document will be appropriate or adequate for your intended purposes. Please contact your WellSky representative if you have any additional questions.

WellSky

Service Organizations Controls (SOC) 1 Type 2, SOC 2 Type 2 and SOC 3

As part of WellSky's ongoing efforts to maintain the highest standard of information security for our clients, WellSky has contracted with independent, third-party providers to routinely assess the compliance, security, and risk of our information systems. This is evident through routine vulnerability and penetration testing and the successful completion of the SSAE 18 / Service Organization Controls (SOC) 1 Type II, SOC 2 type II and SOC 3 examinations, which included detailed testing of WellSky's design, implementation, operation, and maintenance of effective controls within WellSky's Healthcare Solutions, Value Based Care Suite, Community Care Solutions, and Advisory Services Systems throughout the current reporting period. This commitment to excellence further demonstrates that WellSky's policies, procedures, and infrastructure for data security, confidentiality, processing integrity, availability, and privacy met or exceeded the most stringent criteria.

WellSky maintains an appropriate internal control environment and reports upon its effectiveness as well as material changes to its internal controls. As of this date, WellSky is not aware of any material changes in our control environment that would adversely affect the auditor's opinion reached in current SOC 1 Type II, SOC 2 Type II and SOC 3 reports.

To obtain the current reports, please contact your WellSky representative.

6

WellSky

Setting the Standard: Overview of WellSky's Privacy and Security Practices

Under the Department of Health and Human Services (HHS) HIPAA Final Omnibus Rule, organizations (business associates) that work with healthcare providers, insurers, or other services that process PHI must meet HIPAA privacy and security rule requirements. Unfortunately, many business associates are falling short and not doing everything they need to do in order to comply with the rule. As part of WellSky's founding principles to protect confidentiality and earn the trust of the industry we serve, we have invested heavily in data integrity, confidentiality, and security.

The security and integrity of information that moves through WellSky's systems and servers are of critical importance for our clients. WellSky is committed to providing strong, industry-standard security systems to help ensure the availability, confidentiality, and integrity of data, including intellectual property and personal and confidential personal information. Well-established information security policies, processes, and standards are in place within WellSky, with development and production systems that are maintained at a secured site to ensure around-the-clock protection.

To ensure comprehensive and effective network security, WellSky employs a defensive framework based on the National Institutes of Standards and Technologies (NIST) Cybersecurity Framework. The use of packet filtering, firewalls, and control devices limits access to WellSky's environments. Intrusion detection and prevention devices are deployed to filter out specific types of unwanted traffic. WellSky's network is monitored constantly by automated and manual means, with support provided around the clock. Redundancy and fault tolerance are guiding principles in WellSky's information system architecture. WellSky's network design utilizes redundant components and connections to ensure high availability.

WellSky

Remote Access Policy

WellSky Corporation requires that all our solutions be installed as outlined by WellSky's approved installation procedure. WellSky also requires remote access be established to the Windows servers. This access is to include, but is not limited to, direct console access and the ability to transfer files to and from the servers. The preferred method is via ***SecureLink*** product.

WellSky, like many other vendors trying to provide a fast and secure means of support for our clients needed, needed to find a better way to provide this. Because many VPN, dial-up, and third-party software solutions cannot reside on the same machine, it became very difficult to manage all of these on computers and laptops used to support or implement our clients.

With HIPAA and other security and confidentiality laws came the need to deliver a better and more secure way to support our clients. In 2005 WellSky chose to use the SecureLink product to provide a more secure and fast form of support for our clients.

The SecureLink product allows us to decrease our overhead by eliminating the need to manage multiple types of connectivity. SecureLink provides a single HIPAA-compliant, dual-authenticated, and fast-manageable means to provide the best support to our clients.

This solution provides many benefits to both WellSky and our Clients:

- Auditing – SecureLink VSNs offer a very detailed audit report to monitor all vendor activity, which is increasingly important in security-conscious industries and particularly important for HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley compliance. With a SecureLink VSN, the client has a detailed audit report of who accessed the system, what ports and hosts were accessed, what services were performed, when the connection was made, and, for FTP and Telnet services, which specific commands were used.
- Encryption strength – SecureLink VSNs are FIPS compliant and offer several choices for maximum encryption strength and security. By default, SecureLink VSNs offer 128-bit AES level encryption, but clients have the option of dynamically setting encryption strength to 3DES, 192-bit AES, or 256-bit AES encryption, depending on their encryption preferences.
- Real-time reporting – All session information is available in real-time and can be archived for later retrieval and inspection.
- Unique logins – Some vendors are given one or two generic vendor VPN logins when supporting a client. In this case, connections can only be audited based on these generic logins, rather than actual users. In these scenarios, a support engineer can potentially access a client network even when no longer employed by the vendor. SecureLink VSNs require each support engineer to have a valid, unique login, so that all connection information is associated with a specific individual.
- Dedicated server – Some remote support solutions rely on a centrally hosted, shared server. SecureLink VSNs provide each vendor with a dedicated server, hosted inside the vendor's network, so clients can be confident their personal and confidential information will remain private.

8

- Desktop sharing optional – Screen scraping, and remote-control solutions only enable desktop sharing and give no alternatives for supporting server-based software. This is limiting in multi-platform environments, inherently insecure, and forces the client to give up his or her desktop in some situations. In many instances, a vendor can potentially take over a desktop and gain all the access privileges of the user, including the ability to delete files or read email. SecureLink VSNs allow the option of desktop sharing and desktop-based support but allow the client to disable it if appropriate.
- No Additional Outside Exposure - Using a VPN requires the client to leave a hole open to the outside, awaiting the connection. Any additional remote logins create additional security risks. Even with a login disabled, the remote user still has the client configuration information that could be used to access the client's network at a later date. SecureLink' s sessions are initiated and controlled by the client from within their network, eliminating the threat of an outside attack.

In addition, WellSky can now offer support at the client's workstation without any additional software or security issues. This allows us to expand our support to where the user is having the issue while still maintaining a secure connection.

From a technical aspect, SecureLink provides a single means of direct access to the Windows server or workstation with no other software needed to assist the user.

The solution provides a secure desktop management at the server's console as well as a secure transfer capability. This is all encrypted using SSH/SSL connectivity initiated by the Gatekeeper, small solution service running on the server, which communicates to the SecureLink server via an outbound internet connection. Once a request for connection is made by a support person the SecureLink server confirms the user and the encrypted key to make the connection to the server.

Unlike VPN there are no additional holes that need to be opened in the firewall to allow desktop sharing, etc.

Benefits to both WellSky and our clients:

- Reduces time to resolution
- Improves technician efficiency and effectiveness
- Improves client satisfaction
- Eliminates risks & liabilities associated with insecure remote access
- Eliminates direct costs of desktop sharing services, modems, travel, etc.
- Peace of mind with e-mail connection notifications
- Removes the use of extra third-party solutions to access the remote servers or workstations, which may require extra licensing and opening of ports in the firewall.
- Vendor accountability and industry compliance ensured with high-definition audit

HIPAA Requirement	SecureLink Feature
Identification & Authentication	Dual factor, unique user name and password controls Restrictive password requirements Randomly generated, one time use keys Grant access only to customer authorized networks
Restricted Access	Customer configurable Restrict access as to time and scope, down to file level Access rights can be restricted at system or user level Ability to mask logon credentials Integration with Active Directory
Audit Controls	Real time monitoring High definition audit reports Detailed log files, video capture of screen sharing/RDP sessions Unilateral ability to terminate session at any time
Secure Data Transfer	Customer configurable levels of encryption, up to and including, 3DES, Blowfish, and 256 AES

We currently use this product to access several states DOH accounts as well as a host of acute care hospitals, behavioral institutions, and jail systems.

SecureLink is our primary method.

WellSky understands that many sites may already have specific solutions for access in place, which may not be listed above. However, the solutions listed have been tested to allow WellSky to provide 24/7 support from any location without delay.

Reference information:

SecureLink

10

WellSky

Information Security

System security

- Dedicated information technology department ensures high availability and service quality
- Routine vulnerability and penetration tests
- Annual risk assessments, compliance reviews, and management reviews
- Documented information security and privacy procedure training for all teammates
- Systems access logged and tracked for auditing purposes
- Proactive solution code scanning
- Required privacy and security training at time of hire and annually thereafter

Operational security

- Industry-leading data protection and security policies combined with full 256-bit SSL encryption and 2048-bit private keys and AES multilayered encryption for all documents and data, both at rest and in transit
- SSAE 18 SOC 1Type II SOC 2 Type II and SOC 3 reports.
- Access controls configurable by master account administrator
- All passwords encrypted during storage and never transmitted
- Configurable account and password security settings, including role-based permissions
- Account access can be restricted to specific IP addresses
- Intelligent encryption with access controls to ensure data is only decrypted for authorized requests
- Encrypted session IDs uniquely identify each user
- Automated session time-outs
- System installation using hardened OS with ongoing protection from exploits
- Dedicated firewall and intrusion detection system
- Data protection with managed backup solutions
- Distributed Denial of Service (DDoS) mitigation

11

WellSky

Data center security

- Redundant state-of-the-art secured facilities, with redundant hardware, power, and internet connectivity
- Physical access limited to our own data center technicians
- 24 x 7 x 365 on-site security.
- Physical security independently audited

12

WellSky

Company Profile

Company Name	Address	Contact information
WellSky Corporation	11300 Switzer Rd Overland Park, KS 66210	Phone: 913.307.1000 Toll Free: 888.633.4927 Fax: 913.307.1111
Contacts / Title	**Address**	**Contact information**
Jon Moeckel – Sr. Regulatory Compliance Manager Privacy Official	11300 Switzer Rd Overland Park, KS 66210	Jon.Moeckel@WellSky.com Phone: 913.307.1051 Fax: 913.307.1111
Jim Burkholder – Director, Information Technology	11300 Switzer Rd Overland Park, KS 66210	Jim.Burkholder@WellSky.com Phone: 913.307.1021 Fax: 913.307.1111
Jami Albro-Fisher - VP, Engineering Information Security	11300 Switzer Rd Overland Park, KS 66210	Jami.albro-fisher@WellSky.com Phone: 413.584.5300 Fax: 913.307.1111
Andrew Blasiman - Director, Infrastructure Operations	11300 Switzer Rd Overland Park, KS 66210	Andrew.blasiman@wellsky.com Phone: 614.543.8801x13005 Fax: 913.307.1111

13

WellSky

Privacy and Security – General Information

Risk Assessment and Treatment	Response	Additional Information
Is there a risk assessment program that has been approved by management and communicated to appropriate constituents, and is there an owner to maintain and review the program?	Yes	WellSky documented a management-approved risk assessment program that has been appropriately communicated to teammates. The program is managed by the Privacy/Security Official.
Security Policy	**Response**	**Additional Information**
Is there an information security policy that has been approved by management and communicated to appropriate constituents, and is there an owner to maintain and review the policy?	Yes	Quality Management System Section 10 is WellSky's documented information security policy that has been approved by management and communicated to WellSky teammates.
Have the policies been reviewed in the last 12 months?	Yes	Policies and procedures are routinely reviewed, at a minimum annually, by the Privacy/Security Official.
Is there a vendor management program?	Yes	The vendor management program is part of our Quality Management System Section 5, Purchasing Control and Vendor Management.
Organizational Security	**Response**	**Additional Information**
Is there a respondent information security function responsible for security initiatives?	Yes	Security initiatives are the function and responsibility of the Director, Information Technology, and the Privacy/Security Official.
Do external parties have access to systems and data or processing facilities?	Yes	The data centers (Iron Mountain, TierPoint, Data Foundry, FNTS, AWS, Azure, Zayo) have physical access to the systems and data. However, they do not have technical access.
Asset Management	**Response**	**Additional Information**
Is there an asset management policy or program that has been approved by management and communicated to appropriate constituents, and is there an owner to maintain and review the policy?	Yes	Device and Media Controls has been approved by management and communicated to appropriate teammates.
Are information assets classified?	Yes	Information and information assets are classified per the data classification (Low Risk, Medium Risk-Restricted, High Risk- Confidential)
Human Resource Security	**Response**	**Additional Information**
Are security roles and responsibilities of constituents defined and documented in accordance with the respondent's information security policy?	Yes	WellSky maintains adequate job descriptions that outline the roles and responsibilities of the security personnel.

14

Is a background screening performed prior to allowing constituent access to systems and data?	Yes	Background screening is conducted as part of the hiring process.
Are new hires required to sign any agreements upon hire?	Yes	Confidentiality agreements are provided, reviewed, and signed by new hires.
Is there a security awareness training program?	Yes	A security awareness program has been formally documented within Quality Management System Section 2.; Quality System Requirements. WellSky teammates are trained at the time of hire and annually thereafter. Quarterly awareness trainings are provided.
Is there a disciplinarily process for noncompliance with information security policies?	Yes	WellSky's Sanctions Policy has been formally documented, implemented, and provided to WellSky teammates.
Is there a constituent termination or change of status process?	Yes	WellSky Security Policy and Procedures has been formally documented, implemented, and provided to WellSky teammates.
Physical and Environmental Security	**Response**	**Additional Information**
Is there a physical security program?	Yes	Facility, System and Information Access Management policy and procedure has been formally documented, implemented, and provided to WellSky teammates. The policy provides information related to the physical security program.
Are reasonable physical security and environmental controls present in the building/data center that contains systems and data?	Yes	The data centers manage all physical security and environmental controls.
Are visitors permitted in the facilities?	Yes	Visitors are permitted into facilities following authorization activities and approved visitor list.

Communications and Operations Management	Response	Additional Information
Are management-approved operating procedures utilized?	Yes	The information system has been documented and implemented, and management has approved operating procedures.
Is there an operational change management / change control policy or program that has been approved by management and communicated to appropriate constituents, and is there an owner to maintain and review the policy?	Yes	The change control process has been approved by management, formally documented, and communicated to appropriate WellSky teammates.

Do third-party vendors have access to systems and data (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc.)?	Yes	At times, third-party vendors may have access to systems, such as data centers. Access to data is not provided unless specifically authorized and applicable agreements / BAAs have been executed.
Is there an antivirus / malware policy or program (workstations, servers, mobile devices) that has been approved by management and communicated to appropriate constituents, and is there an owner to maintain and review the policy?	Yes	An antivirus/malware policy has been approved by management and implemented throughout the organization.
Are system backups performed?	Yes	Backups are performed at defined intervals. Restoration tests are conducted periodically and documented appropriately.
Are firewalls in use for both internal and external connections?	Yes	Firewalls have been implemented.
Are vulnerability assessments, scans, or penetration tests performed on internal or external networks?	Yes	WellSky conducts annual third-party vulnerability assessments and penetration tests on the internal and external networks. Refer to the SMP Auditors Letter.
Are there external network connections (Internet, intranet, extranet, etc.)?	Yes	WellSky has employed external network connections (Internet and intranet).
Is wireless networking technology used?	Yes	WellSky utilizes wireless technologies within its development facilities.
Is there a removable media policy or program (CDs, DVDs, tapes, disk drives) that has been approved by management and communicated to appropriate constituents, and is there an owner to maintain and review the policy?	Yes	A removable media policy and procedures have been approved by management, formally documented, and provided to WellSky teammates.
Is data sent or received electronically or via physical media?	Yes	Data can be sent or received through secure electronic transmission or encrypted physical devices.
Access Control	Response	Additional Information
Are electronic systems used to transmit, process, or store data?	Yes	WellSky utilizes approved electronic systems to transmit, process, or store data.
Are unique user IDs used for access?	Yes	Unique user IDs and passwords are required for access.
Are passwords required to access systems transmitting, processing, or storing data?	Yes	Unique user IDs and passwords are required for access.
Is remote access permitted?	Yes	WellSky does allow remote access for teammates through VPN, utilizing unique user IDs and passwords.

WellSky Acquisition Development and Maintenance	Response	Additional Information
Are business information systems used to transmit, process, or store data?	Yes	WellSky uses owned business information systems to transmit, process, and store data.
Is solution development performed?	Yes	WellSky is a software manufacturer.
Is there a formal software development life cycle (SDLC) process?	Yes	Configuration Management Process_ Software Development Life Cycle has been developed, formally documented, approved by management, and provided to applicable teammates.
Are systems and solutions patched?	Yes	Systems and solutions are patched following appropriate change control practices to ensure successful implementation of patches.
Are vulnerability tests (internal/external) performed on all solutions at least annually?	Yes	Internal vulnerability tests are performed no less than annually. The vulnerability consists of a complete scan of the solution code through use of the Checkmarx tool.
Are encryption tools managed and maintained for data?	Yes	WellSky implements industry-recommended encryption for data at rest and during transmission. AES 256, BitLocker, SSL, TLS 1.2, HTTPS, Accellion, and Secure Link.
Incident Event and Communications Management	Response	Additional Information
Is there an incident management program?	Yes	Quality Management System 10.8; Security Incident Response has been formally documented, management-approved, and provided to WellSky teammates.
Business Continuity and Disaster Recovery	Response	Additional Information
Is there a documented policy for business continuity and disaster recovery that has been approved by management and communicated to appropriate constituents, and is there an owner to maintain and review the policy?	Yes	Information System Contingency Plan policy and procedure has been formally documented, approved by management, and provided to WellSky teammates.
Is there an annual schedule of required tests?	Yes	The contingency plan is tested on a regular basis, no less than annually.
Are BC/DR tests conducted at least annually?	Yes	The Business Continuity and Disaster Recovery tests are conducted as part of the Information System Contingency Plan Testing.
Compliance	Response	Additional Information

17

Is there an internal audit, risk management, or compliance department with responsibility for identifying and tracking resolution of outstanding regulatory issues?	Yes	WellSky has a designated Privacy and Security Official who is responsible for internal audits, risk management, tracking, and regulatory issues. Privacy Official: Jon Moeckel Sr. Regulatory Compliance Manager Jon.moeckel@wellsky.com Regulatory.compliance@wellsky.com 913.307.1000 Security Official: Jami Albro-Fisher VP, Engineering – Information Security Jami.albro-fisher@wellsky.com 913.307.1000
Is there an internal compliance and ethics reporting mechanism and training program for teammates to report compliance issues?	Yes	Compliance and ethics personnel report directly to executive management. Teammates are trained on the Corporate Compliance Manual at time of hire.
Mobile	Response	Additional Information
Are mobile devices used to access systems and data?	Yes	Upon authorization, mobile devices may be used to access systems and data. The mobile devices must be configured to WellSky's IT standards and encrypted if utilized to access or maintain PHI or confidential information.
Privacy	Response	Additional Information
Is data transmitted, processed, or stored that can be classified as non-public information (NPI), personally identifiable information (PII), or personal and confidential client financial information? If yes, describe and list types of data.	Yes	Name, address, DOB, SSN, health information, and insurance information.
Is data transmitted, processed, or stored that can be classified as protected health information, electronic health records, or personal health records? If yes, identify the classifications.	Yes	Protected health information (PHI) Personally Identifiable Information (PII)
For data, is personal information about individuals transmitted to or received from countries outside the United States? If yes, identify the countries.	No	Client data is not transmitted or received outside of the United States.
For data, is there a dedicated person (or group) responsible for privacy compliance. If yes, describe. If no, explain reason.	Yes	The Privacy/Security Official: Jon Moeckel - Regulatory Compliance Specialist

For data, is there a documented privacy policy or procedures to protect confidential information?	Yes	Quality Management System Section 9; WellSky Privacy Practices.
For data, are regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain reason.	Yes	Risk assessments are conducted both internally and externally by third parties. The assessments are conducted no less than annually. Assessment reports are presented to executive management for privacy program review.
Is there formal privacy awareness training for teammates, contractors, and third-party users to ensure confidentiality and privacy of data?	Yes	Training is provided to all WellSky teammates to ensure confidentiality and privacy of data.
Is there a formal process for reporting and responding to privacy complaints or privacy incidents for data? If yes, describe. If no, explain reason.	Yes	WellSky has formally documented, implemented, and provided a complaint policy and procedure to WellSky teammates.
Is there a data classification and retention program for data that identifies the data types that require additional management and governance?	Yes	Data classification has been implemented and enforced through Information Technology. A data retention policy has been formally documented, implemented, and provided to applicable WellSky teammates.
Is there a documented response program to address privacy incidents, unauthorized disclosure, unauthorized access, or breach of data?	Yes	Quality Management System Section 10.8: Security Incident Response has been formally documented, management approved, and provided to WellSky teammates.
Is data disclosed to third parties? If yes, describe.	No	
Is data disclosed to third parties outside of the U.S.? If yes, describe.	No	Production data is not disclosed to offshore entities. WellSky does utilize offshore development resources. However, these resources do not have access to or are disclosed production data.
Are there contractual controls to ensure that data shared with third parties is limited to defined parameters for access, use, and disclosure? If yes, describe the controls. If no, explain reason.	Yes	WellSky enters agreements, including business associate agreements, with all vendors to identify and limit the defined parameters for access, use, and disclosure.
Is there a business associate contract in place to address obligations for the privacy and security requirements of the services provided?	Yes	WellSky executes business associate agreements to address obligations for the privacy and security requirements of the services provided.
Is there a documented privacy program with administrative, technical, and physical safeguards for the protection of data?	Yes	WellSky has a documented privacy and security program that includes reasonable and appropriate administrative, physical, and technical safeguards for the protection of data.

Is there a process to ensure that the personal information provided by an individual is limited for the purposes described in the respondent's privacy notice? If yes, describe. If no, explain reason.	Yes	WellSky has implemented a Minimum Necessary procedure to ensure only the minimum amount of data necessary to complete the required task is accessed or disclosed.
Are there documented policies, procedures, and controls to limit access based on need to know or minimum necessary for constituents? If yes, describe.	Yes	WellSky has formally documented, implemented, and provided information to WellSky teammates that control the access based off a need to know and user role within the organization.
Are enforcement mechanisms applied to constituents who violate privacy policies or confidentiality requirements?	Yes	WellSky teammates are subject to corrective actions and sanctions outlined within WellSky policy.

WellSky

Solution Information

Solution Manager	Address	Contact information
Gabriel Cate, Vice President Solutions Management	WellSky Corporation 11300 Switzer Rd Overland Park, KS 66210	Gabe.Cate@wellsky.com

Solution Profile

Solution Name	Solution Version	Solution Release Date
Community Services (fka "ServicePoint")	5.14.11	September 22, 2022

Intended Use

WellSky (SOLUTION) is intended to:

21

WellSky

Solution Security Posture

Management of Personal and confidential Data, including ePHI	Response	Additional Information
Can the solution display, transmit, or maintain personal or confidential data? Describe the data displayed, transmitted, or maintained.	Yes	Protected health information (PHI) Personally, identifiable information (PII) Payment Cared Information (PCI)
Types of personal and confidential data, including ePHI, that can be maintained by this solution:		
Demographic (e.g., name, address, location)?	Yes	
Medical record (e.g., MRN#, account#, test, or treatment date)?	Yes	Administrators can configure the system to collect this data through custom fields, as needed.
Diagnostic/therapeutic (e.g., photo/radiograph, test results, physiologic data)?	Yes	Administrators can configure the system to collect this data through custom fields, as needed.
Open, unstructured text entered by solution user?	Yes	
Biometric data?	No	
Personal financial information?	Yes	Administrators can configure the system to collect this data through custom fields, as needed.
Maintaining personal and confidential data, including ePHI – Can this solution:		
Maintain personal and confidential data, including ePHI, temporarily in volatile memory?	N/A	
Store personal and confidential data, including ePHI, persistently on local media?	No	
Import/export personal and confidential data, including ePHI, with other systems?	Yes	
Maintain personal and confidential data, including ePHI, during power service interruptions?	Yes	Stored in database.
Mechanisms used for the transmitting importing/exporting of personal and confidential data, including ePHI – Can the solution:		
Generate hard copy reports or images containing personal and confidential data, including ePHI?	Yes	
Display personal and confidential data, including ePHI (e.g., video display, etc.)?	Yes	

22

Retrieve personal and confidential data, including ePHI, from or record this data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	Yes	
Transmit/receive or import/export personal and confidential data, including ePHI, via dedicated cable connections (e.g., serial port, USB, FireWire, etc.)?	Yes	
Transmit/receive personal and confidential information, including ePHI, via a wired network connection (e.g., LAN, WAN, VPN, intranet, internet, etc.)?	Yes	
Transmit/receive personal and confidential data, including ePHI, via an integrated wireless network connection (e.g., Wi-Fi, Bluetooth, infrared, etc.)?	Yes	
Import personal and confidential data, including ePHI, via scanning?	Yes	
Other?	N/A	
Does the solution transmit, process, store or maintain Payment Card Information (PCI)?	No	
Security Capabilities	**Response**	**Additional Information**
Automatic Logoff – Can the solution be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	Yes	
Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? *(Indicate time {fixed or configurable range} in notes)*	Yes	Configurable by WellSky staff.
Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the user?	No	
Is the solution a multi-tenant system?	No	
Audit Controls – Can the solution create an audit trail?	Yes	
Indicate which of the following events are recorded in the audit log:		
Login/logout	Yes	
Display/presentation of data	Yes	
Creation/modification/deletion of data	Yes	
Import/export of data from removable device	Yes	File uploads are audited

Receipt/transmission of data from/to external (e.g., network) connection	Yes	
Remove service activity	Yes	
Other events? (Describe)		All CRUD actions performed by solution users are audited.
Indicate what information is used to identify individual events recorded in the audit log:		
User ID	Yes	
Date/time	Yes	
Other? (Describe)	Yes	User action performed and the Provider the user is associated with.
Authorization		
Can the solution prevent access to unauthorized users through user login requirements or other mechanisms?	Yes	Role-based access and administrator-configured data sharing rules govern what information each solution user is able to access.
Can users be assigned different privilege levels within a solution based on "roles" (e.g., guests, regular users, power users, administrators, etc.)?	Yes	
Can the solution owner/operator obtain unrestricted administrative privileges (e.g., access operating system or solution via local root or admin account)?	No	
Configuration of Security Controls		
Can the solution owner/operator reconfigure product security capabilities?	Yes	The application administrator can configure role-based security and other system security settings.
Cyber Security Product Upgrades		
Can relevant OS and solution security patches be applied to the solution as they become available?	Yes	Performed by WellSky staff.
Can security patches or other software be installed remotely?	Yes	
Health Data De-Identification		
Does the solution provide an integral capability to de-identify personal and confidential information, including ePHI?	Yes	This can be accommodated via custom scripting, as needed, by WellSky staff before data is exported.
Data Backup and Disaster Recovery		

Does the solution have an integral data backup capability, (i.e., backup to remote storage or removable media such as tape, disk)?	Yes	
Emergency Access		
Does the solution incorporate an emergency access ("break-glass") feature?	No	SaaS based application.
Health Data Integrity and Authenticity		
Does the solution ensure the integrity of stored data with implicit or explicit error detection/correction technology?	Yes	
Malware Detection/Protection		
Does the device support the use of anti-malware software or other anti-malware mechanism?	Yes	
Can the user independently reconfigure anti-malware settings?	No	
Does notification of malware detection occur in the solution user interface?	No	
Can only authorized persons repair systems when malware has been detected?	Yes	SaaS based application.
Can the solution owner install or update antivirus software?	No	SaaS based application.
Can the solution owner/operator (technically/physically) update virus definitions on installed antivirus software?	No	SaaS based application.
Node Authentication		
Does the solution provide/support any means of node authentication that assures that both the sender and the recipient of data are known to each other and are authorized to receive transferred information?	Yes	All transmissions must be authenticated and authorized.
Person Authentication		
Does the solution support user/operator specific username(s) and password(s) for at least one user?	Yes	
Does the solution support unique user/operator specific IDs and passwords for multiple users?	Yes	
Can the solution be configured to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	No	The system is designed to be used by multiple, independent organizations which will not share a single authentication service.
Can the solution be configured to lock out a user after a certain number of unsuccessful logon attempts?	Yes	

25

Can default passwords be changed at/prior to installation?	Yes	
Are any shared user IDs used in the system?	No	
Can the solution be configured to enforce creation of user account passwords that meet established complexity rules?	Yes	
Can the solution be configured so that account passwords expire periodically?	Yes	
Road Map for Third-Party Components in Device Life Cycle		
In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) – including versioning number(s)	N/A	SaaS based application.
Is a list of other third-party solutions available?	N/A	
System and Solution Hardening		
Does the solution employ any hardening measures? Please indicate the level of conformance to any industry recognized hardening standards.	Yes	The SaaS environment machines are hardened using CIS standards as a baseline.
Does the solution employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the authorized program or software update?	N/A	SaaS based application.
Does the file system allow the implementation of file-level access controls (e.g., New Technology File System for MS Windows platforms)?	N/A	
Are all accounts that are not required for the intended use of the solution disabled or deleted, for both users and solutions?	Yes	
Can the solution boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	N/A	SaaS based application.
Security Guidance		
Are security-related features documented for the solution user?	Yes	
Are instructions available for solution/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal and confidential data, including ePHI)?	N/A	SaaS based application.
Health Data Storage Confidentiality		
Can the solution encrypt data at rest?	Yes	

Transmission Confidentiality		
Can personal and confidential data, including ePHI, be transmitted only via a point-to-point dedicated cable?	N/A	SaaS based application.
Is personal and confidential data, including ePHI, encrypted prior to transmission via a network or removable media? (If yes, indicate which encryption standard is implemented.)	Yes	Data is encrypted in transport using a third-party SSL/TLS certificate (TLS 1.2, employing 2048-bit key for digital signatures, and County with Cipher block chaining mode (CCM), with AES-256 for message authentication and a SHA2-256-bit hash for secure hashing.
Is personal and confidential data, including ePHI transmission, restricted to a fixed list of network destinations?	No	SaaS based application.
Transmission Integrity		
Does the solution support any mechanisms intended to ensure data is not modified during transmission? (If yes, describe how this is achieved.)	Yes	Data is encrypted in transport using a third-party SSL/TLS certificate (TLS 1.2, employing 2048-bit key for digital signatures, and County with Cipher block chaining mode (CCM), with AES-256 for message authentication and a SHA2-256-bit hash for secure hashing.
Other Security Considerations		
Can the solution be serviced remotely?	Yes	
Can the solution restrict remote access to/from specified devices or users or network locations (e.g., specific IP addresses)?	No	
Can the solution be configured to require local user to accept or initiate remote access?	N/A	SaaS based application.