PromisSE Policies and Procedures

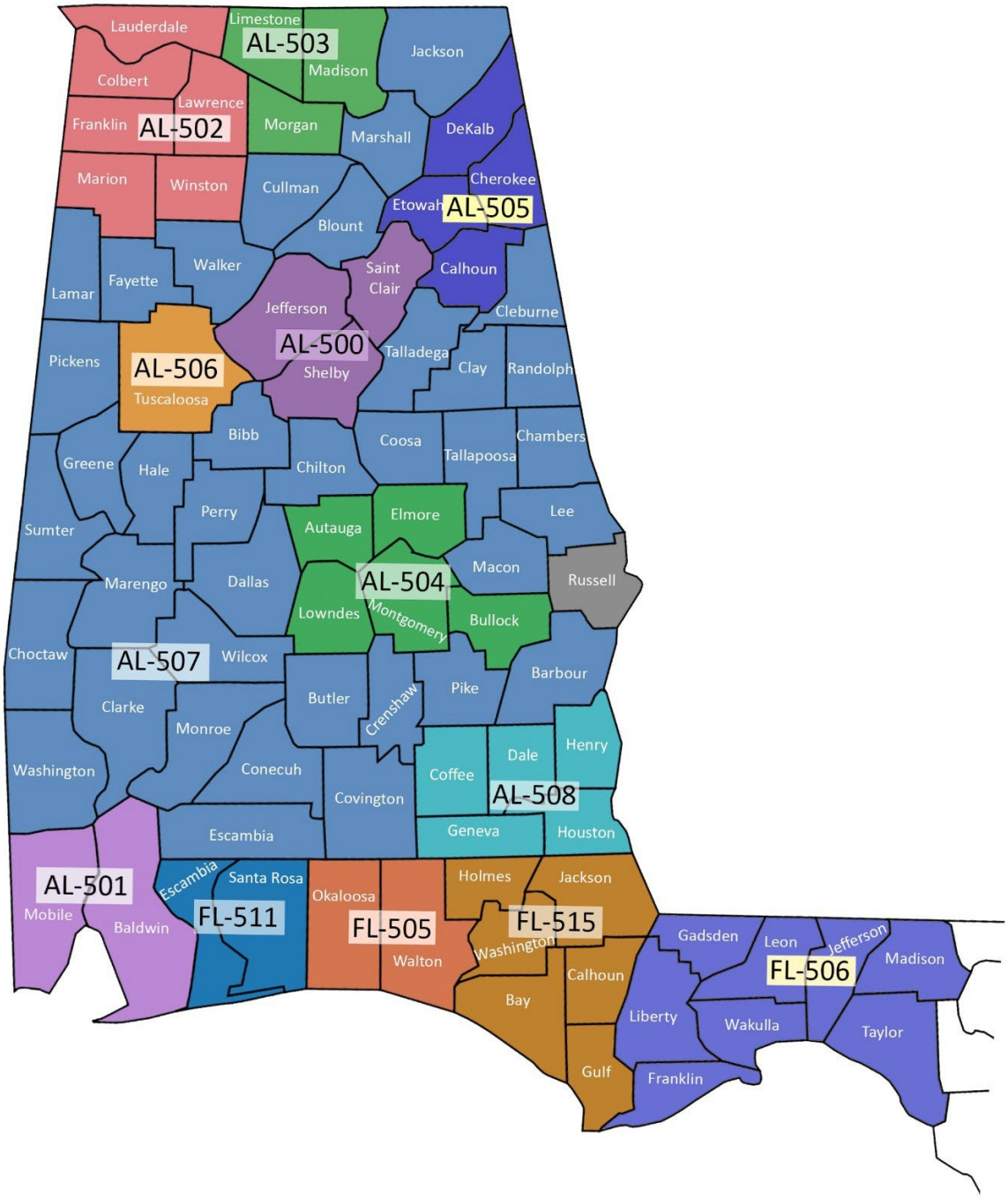


Table of Contents

Introduction..... 3
PromisSE Continuums of Care..... 3
PromisSE Steering Committee..... 4
Key Terms and Acronyms..... 5
Policy Disclaimers and Updates..... 7
Privacy Statement..... 8
Agreements, Certifications, Licenses, and Disclaimers..... 9
Privacy and Security Plan..... 11
Privacy Standards..... 13
Data Security Standards..... 15
System Administration and Data Quality Plan..... 17
Appendix A – CoC and Agency Participation Agreement..... 20
Appendix B – CoC Agency Administrator Agreement..... 29
Appendix C – Agency Security Officer Agreement..... 30
Appendix D – CoC Policies and Procedures Compliance Checklist..... 31
Appendix E – Privacy and Security Checklist..... 30
Appendix F – License Agreement and Statement of Confidentiality..... 31
Appendix G – PromisSE Release of Information (ROI)..... 33
Appendix H – Public Notice..... 37
Appendix I – Privacy Notice to Clients..... 38
Appendix J – Partner Agency Privacy Policy..... 40
Appendix K - HUD Data Elements..... 47
Appendix L – PromisSE and CoC Participation Agreement..... 48
Appendix M – CoC System Administrator Agreement..... 52
Appendix N – CoC System Security Officer Agreement..... 53
Appendix O – Sample CoC Agency Audit Checklist..... 53
Appendix P – HMIS Data Sharing, Security & Usage Agreement..... 56
Appendix Q – Sample HMIS Criminal Background Check Certification..... 58
Appendix R – Flowchart of HUD's Definition of Chronic Homelessness..... 59
Appendix S – HUD Program Types..... 60

Introduction

The purpose of the HMIS (Homeless Management Information System) is to record and store client-level information about the numbers, characteristics, and needs of persons who use homeless housing and supportive services, to produce an unduplicated count of homeless persons for each Continuum of Care; to understand the extent and nature of homelessness locally, regionally and nationally; and to understand patterns of service usage and measure the effectiveness of programs and systems of care. The following operating policies and procedures apply to all designated HMIS participating CoCs and Agencies (Contributing HMIS Organizations – CHOs).

PromisSE Continuums of Care

PromisSE is a multi-CoC HMIS implementation comprising the following CoCs:

COC Code	Lead Organization	General Area
AL-500	One Roof	Birmingham, AL
AL-501	Housing First	Mobile, AL
AL-502	Homeless Care Council of Northwest Alabama	Florence, AL
AL-503	City of Huntsville	Huntsville, AL
AL-504	Montgomery Area Coalition for the Homeless (MACH)	Montgomery, AL
AL-505	Homeless Coalition of Northeast Alabama (HCNEA)	Gadsden, AL
AL-506	CHALENG of Tuscaloosa	Tuscaloosa, AL
AL-507	Alabama Rural Coalition for the Homeless (ARCH)	Montgomery, AL
AL-508	Southeast Alabama Coalition for the Homeless	Dothan/Coffee, AL
FL-505	Homelessness And Housing Alliance (HHA)	Fort Walton Beach, FL
FL-506	Big Bend Continuum of Care	Tallahassee, FL
FL-511	Opening Doors Northwest Florida	Pensacola, FL
FL-515	Doorways of Northwest Florida	Panama City, FL

PromisSE Steering Committee

The PromisSE Steering Committee serves as the governing agency of the PromisSE implementation, and is responsible for developing policies and procedures to support the objectives of the implementation and the efforts of its members.

Purpose

The purpose of the PromisSE Steering Committee is to serve as the decision-making body for the PromisSE implementation.

Activities of the Committee

The responsibilities of the committee include but are not limited to the following:

Developing and maintaining PromisSE Policies and Procedures.
Expansion of the implementation.
Selecting and approving the HMIS software vendor.
Determining the CoC who will hold the HMIS software vendor contract.
Selecting the minimal data elements to be collected by all HMIS-contributing projects in the implementation.
Conduct an annual review of all required privacy and security plans, privacy standards, data security standards, and HMIS data quality standards, and update when necessary.

Composition

The PromisSE Steering Committee is a partnership of representatives from each of the participating Continuums of Care and Continuum-designated HMIS lead agencies.

Voting

- One voting seat will be provided to each participating CoC. The Steering Committee can add non-voting advisory seats as needed for additional partners and subject matter experts.
- Membership will comprise no less than one duly authorized representative appointed by each participating CoC, with each CoC designating an equally authorized alternate representative in the event the primary is unavailable.
- Appointment of a primary voting member and an alternate voting representative is required of each CoC, with appointment to the secondary non-voting seat at the discretion of each CoC.
- The committee may elect to add additional non-voting seats as needed in order to incorporate more partners and subject matter experts.
- Two thirds of the total CoCs represented on the PromisSE Steering Committee will constitute a quorum.

Meetings and Attendance

The Steering Committee will participate in quarterly calls and will hold meetings twice per year. All meetings will open with a roll call of PromisSE CoCs.

Officers

- The Steering Committee will identify three officers to serve a one-year term and they will be as follows:

- The Steering Committee Chair will be responsible for calling and facilitating meetings, designating committees, and assigning committee duties.
- The Steering Committee Vice-Chair will be responsible for assuming the duties of the Chair in the event the Chair is unable to fulfill them.
- The Steering Committee Secretary will be responsible for maintaining minutes and documentation relating to the Steering Committee.

- PromisSE Steering Committee Officers will be elected annually.

HMIS Vendor Contract

The HMIS vendor contract-holding CoC will:

- Invoice PromisSE-participating CoCs for HMIS software use, in addition to requested vendor upgrades or training.
- Order licenses as requested by local HMIS lead agencies.

Each CoC will add that determining the HMIS software is done in a collaborative manner to their own governance charters.

Key Terms and Acronyms

Term	Acronym (if used)	Brief Definition or Link
Balance of State CoC	BOS	A large area within a state that is often rural in nature, which is not covered by regional, county, or city continuums.
Chronic Homeless Definition		See Appendix S
Community Partner		A Community Partner is an agency that is not a PromisSE Member Agency or a Contributing HMIS Organizations. A Community Partner is unable to participate as a PromisSE Member Agency due to internal or external restrictions. Community Partners are often state and local government agencies. HMIS information may be released to a Community Partner in a life-threatening situation or upon a client's death. A Community Partner must sign non-participating agency and confidentiality agreement (Appendix Q).
Continuum-Designated HMIS Lead Agency		The Continuum-Designated HMIS Lead is responsible for managing the HMIS for the CoC's geographic area, in accordance with the requirements of the ***CoC Program Interim Rule*** and any HMIS requirements prescribed by HUD. Any additional responsibilities assigned to the HMIS Lead should be documented in the CoC's governance charter, but may also be clarified in a separate, more detailed written agreement that is incorporated by reference into the CoC's governance charter.
Continuum of Care Participation Agreement		The Agreement between all participating Continuum Designated HMIS Lead Agencies and PromisSE's HMIS Vendor Contract-Holding Agency that specifies the rights and responsibilities of PromisSE's HMIS Vendor Contract-Holding Agency and participating Continuum Designated HMIS Lead Agencies. This document also outlines privacy, inter-Agency sharing, custody of data, data entry standards, and reporting standards. The Agreement prevents the re-release of data and, in combination with the PromisSE License Agreement, defines the rules of sharing. The Agreement between each Continuum Designated HMIS Lead Agency and PromisSE's

Term	Acronym (if used)	Brief Definition or Link
		HMIS Vendor Contract-Holding Agency that supports a regional HMIS operating in a single system environment. (Appendix L)
Contributing HMIS Organizations	CHO	An organization that participates in the HMIS. All Contributing HMIS Organizations must be PromisSE Member Agencies. All Contributing HMIS Organizations must meet the requirements of their Local CoC to be a PromisSE Member Agency.
Coordinated Entry/Coordinated Access/Coordinated Assessment/Coordinated Intake		Coordinated entry is a process developed to ensure that all people experiencing a housing crisis have fair and equal access and are quickly identified, assessed for, referred, and connected to housing and assistance based on their strengths and needs.
Coverage Rate		For Continuum Designated HMIS Lead Agency - The percent of the Homeless Population that is measured in HMIS. Coverage estimates are used to project a total homeless count that includes those served in Domestic Violence Providers and other non-participating Shelters or Outreach Programs. HUD also defines Bed Coverage (beds covered on the HMIS) and Service Coverage (person coverage for non- residential programs).
Electronic Data Interchange	EDI	The direct computer-to-computer exchange of standard formatted business transactions between one or more business partners, known as trading partners. EDI permits organizations to generate, receive, and process data without human intervention.
HMIS Lead Agency		Agency, organization, or government department designated by the CoC to administer and manage the HMIS.
Homeless Definition	Criteria for Defining Homelessness	See Appendix S
Homeless Management Information System	HMIS	Data systems that meet HUD requirements and are used throughout the nation to measure homelessness and the effectiveness of related service delivery systems. The HMIS is also the primary reporting tool for HUD homeless service grants as well as other public monies related to homelessness.
Housing Inventory Count	HIC	All residential programs (both HMIS and non-participating) must specify the number of beds and units available to homeless persons. The numbers are logged into related Provider Pages where the corresponding person data is recorded (for participating programs).
Housing Opportunities for Persons with AIDS	HOPWA	The Housing Opportunities for Persons With AIDS (HOPWA) Program is the only Federal program dedicated to the housing needs of people living with HIV/AIDS. Under the HOPWA Program, HUD makes grants to local communities, States, and nonprofit organizations for projects that benefit low-income persons living with HIV/AIDS and their families. HUD's eligibility requirements for HOPWA can be found at https://www.hudexchange.info/programs/hopwa/hopwa-eligibility-requirements/
HUD Program Types		Appendix T
Length of Stay	LOS	The number of days between the beginning of services and the end of services. It is calculated using entry and exit dates or shelter stay dates. The HMIS offers calculations for discrete stays as well as the total stays across multiple sheltering events.
Local HMIS Lead Agency		The agency that is designated to carry out the activities of the CoC or grant including fiscal and compliance activities. Regular administrative tasks may include, but are not limited to: management of the annual HUD application, coordination of other funding opportunities, project and system monitoring, meeting management, etc. Add clarification to match APR.

Term	Acronym (if used)	Brief Definition or Link
Point In Time Count	PIT	An annual count during the last ten days in January that is required for all Continuums of Care (CoCs). Every odd-numbered year, that count also includes a required "unsheltered" or street count. PIT count may need to be performed more frequently depending on the needs of the community.
PromisSE License Agreement		The Agreement signed by each end user and Agency manager that outlines guidelines for use including; individual privacy, Agency privacy and other PromisSE policy and procedure for use of the System. This document sets the standards of conduct for each HMIS user.
PromisSE Member Agency		A PromisSE Member Agency is an organization that has completed the Agency Participation Agreement (Appendix A) and utilizes the PromisSE System within their agency for the purposes of sharing client data. Member agencies are also referred to as Service Providers throughout this document.
PromisSE Steering Committee		See Steering Committee Section
Release of Information	ROI	A PromisSE Release of Information (Appendix G) must be completed to share or enter any client's data in the System. ROIs must also be documented in the PromisSE (HMIS) system after the client has consented.
Visibility		Visibility refers to the ability to see a client's data between provider pages on the System. Visibility is configured in the System on each Provider Page.
Visibility Groups		Visibility Groups are defined groups of Provider Pages where data is shared. Internal Visibility Groups control internal sharing.

Policy Disclaimers and Updates

Operating policies and procedures defined in this document represent the minimum standards of participation in the PromisSE Implementation (regional), and general best-practice operations procedures. PromisSE CoCs may include additional standards, as long as those additional standards do not affect general best practices, procedures, or operation of the PromisSE (HMIS) system.

Operation standards in this document are not intended to supersede grant-specific requirements and operating procedures as required by HUD or federal partners participating in HMIS.

The PromisSE Policies and Procedures are reviewed an updated at least annually and upon issuance of applicable guidance from HUD or its federal partners. Proposed updates to the PromisSE Policies and Procedures will be presented to duly authorized representatives of the participating CoCs and will be voted upon by a quorum of these representatives, with a simple majority required for adoption. Additional changes made will supersede previous PromisSE HMIS Policies & Procedures. All changes made in compliance with HIPAA regulations or additional federal statutes will also be highlighted. A current copy of the PromisSE HMIS Policy and Procedures may also be found on One Roof's website www.oneroofonline.org.

Privacy Statement

PromisSE is committed to making the HMIS safe for all types of programs in the PromisSE implementation service area, and the clients whose information is recorded, with the goal of maximizing opportunities to improve services through automation.

The purpose of these HMIS Policies and Procedures is to provide guidelines, requirements, responsibilities, processes, and procedures governing the operation of the HMIS, with an emphasis on protecting the privacy of Clients and the security of Client information. These Policies and Procedures apply to designated HMIS Staff, Agencies utilizing HMIS, Agency Users, the HMIS Software Vendor, and any other entity involved in the administration of HMIS.

Sharing information is a planned activity guided by Participation Agreements between PromisSE-participating HMIS Lead Agencies and local participating agencies. The Continuum Designated HMIS Lead Agency may elect to keep private some or all of the client record, including all identifying data. If the client requests their personal data release, it may be given at the agency level. The CoC-designated HMIS lead must approve any other requests for client-level information to be shared outside of PromisSE. If approval is granted, the Community Partner Agreement must be signed (Appendix Q). If a client is able, they must sign a statement releasing their information to a non-Contributing HMIS Organization. Upon receiving their signed statement, the Local Lead System Administrator will upload the statement in the System. HMIS information may be released to a Community Partner in a life-threatening situation or upon a client's death.

Uses and disclosures of client level data must comply with requirements as set by HUD, the Federal Partners, and as governed by local, state, or federal laws. HUD has authorized the following uses and disclosures without participant consent, provided they are clearly stated in the Privacy Notice: Providing or coordinating services to an individual; Creating de-identified client records from PII; Carrying out administrative functions; Functions related to payment or reimbursement for services; Sharing identifiable HMIS data with the U.S. Department of Veterans Affairs (VA) for the purpose of coordinating housing and supportive services for veterans experiencing homelessness, including participation in the VA's HMIS Data Integration Project and submission of data to the VA HMIS Repository. Providers are additionally permitted, and in some instances required, to disclose information without participant consent for the following purposes, provided they are clearly stated in the Privacy Notice: Uses and disclosures required by law; Uses and disclosures to avert a serious threat to health or safety; Uses and disclosures about victims of abuse, neglect or domestic violence; Uses and disclosures for research purposes; Uses and disclosures for law enforcement purposes. Uses and Disclosures not expressly described in the Privacy Notice require participant consent. To the greatest extent practicable, participant consent should be affirmed and confirmed through a signed release of information (ROI) clearly describing the intent and circumstances surrounding the use and disclosure of their personal information. Signed ROI’s must be uploaded to the participant’s HMIS record. Continuum Designated Lead Agencies may elect to require the signing of a Release of Information prior to sharing participant level information with non-HMIS partners. Those Continuum Designated Lead Agencies who elect not to require a signed statement must ensure Privacy Notices and related disclosures accurately reflect sharing practices and submit plans to address changes to sharing practices to the PromisSE steering committee for review prior to implementation, which must include steps to address retroactive changes to participant sharing.

Agreements, Certifications, Licenses, and Disclaimers

- Each Continuum Designated HMIS Lead Agency signs an Agreement and Authorization that designates the use of an implementation-wide HMIS Vendor and identifies PromisSE's HMIS vendor contract-holding agency as the lead Agency for the administration of the HMIS. Each Continuum Designated HMIS Lead Agency will also collaborate with PromisSE's HMIS vendor contract-holding agency for specific tasks. The Agreement and Authorization supports the ability for multiple Continuums of Care to participate in a single HMIS.
- PromisSE's HMIS vendor contract-holding agency will keep all Continuum Designated HMIS Lead Agency Partnership Agreements on file. Continuum Designated HMIS Lead Agencies will keep all PromisSE License Agreement and Agency Participation Agreements on file. Training Certifications are kept by the Continuum Designated HMIS Lead Agency, and partner Agencies are given a copy for reference and maintenance of their files.
- All CoC-Designated HMIS Lead Agencies and HMIS-Participating Agencies must have fully executed, and be in compliance with, the following Agreements and Policies:
    a. Participation Agreement (See Appendix A for Agencies and Appendix L for Continuum Designated HMIS Lead Agencies) governing the basic operating principles of the System and rules of membership.
    b. A Board of Directors approved Confidentiality Policy governing the Privacy and Security standards for the Agency or Continuum Designated HMIS Lead Agency.
    c. User Agreement governing the individual's participation in the System.
    d. Agency Administrator Agreement for Agencies (See Appendix B) or HMIS System Administrator Agreement for Continuum Designated HMIS Lead Agencies (See Appendix M) governing the role and responsibility thereof.
    e. Security Officer Agreement (See Appendix C for Agencies or Appendix N for Continuum Designated HMIS Lead Agencies) governing the role and responsibility thereof.
- Continuum Designated HMIS Lead Agencies must have an assigned System Administrator. The System Administrator:
    a. Has completed, at a minimum, System Admin training.
    b. Ensures that all Agency End Users have signed User Agreements documents on file.
    c. Ensures that all Agency Administrators have signed Agency Admin agreements on file.
    d. Ensures that all Security Officers have signed Security Officer Agreements on file.
    e. Ensures that all End Users complete an annual End User Certification Test, which includes Privacy and Security training, found on the PromisSE Learning Management System – www.learnhmis.org.
    f. Ensures that all End Users have completed workflow training and related updates, and have documentation of training.
    g. Ensures that the Continuum Designated HMIS Lead Agency complies with the Continuum Designated HMIS Lead Agency Data Security standards.
    h. Ensures that the Continuum Designated HMIS Lead Agency complies with the PromisSE Policies and Procedures.
    i. Ensures that all End Users have submitted a criminal background check.

- Agencies must have an assigned Agency Administrator. The Agency Administrator:
    a. Has completed, at a minimum, basic HMIS data entry training. HMIS data entry training must include at a minimum: basic data quality, an overview of data quality reports, and common processes such as the proper procedures for password resets.
    b. Ensures that all Agency End Users have signed User Agreements documents on file.
    c. Ensures that all End Users will complete an annual End User Certification Test, which includes Privacy and Security training.
    d. Ensures that all End Users have completed workflow training and related updates, and have documentation of training.
    e. Ensures that the Agency complies with the Continuum Designated HMIS Lead Agency Data Security standards.
    f. Ensures that the Agency complies with the HMIS Policies and Procedures, has completed the Compliance Checklist (see Appendix D), and is responsible for returning it to the local Lead Agency System Administrator.
    g. Ensures that all End Users have submitted a criminal background check to the local Lead Agency System Administrator.
    h. Resets the password of all non-Agency Administrators at your agency, unless an HMIS Lead System Administrator assumes the role of resetting passwords if they so choose.

Privacy and Security Plan

All records entered into the HMIS and downloaded from the HMIS are required to be kept in a confidential and secure manner.

Oversight

- All Continuum Designated HMIS Lead Agencies must assign a System Security Officer. The **System Security Officer:**

    a. Ensures that all users/agents using the System complete annual privacy and security training. Training must be provided by Continuum-designated HMIS lead agencies and be based on the PromisSE Privacy and Security standards. This training can be accessed through the PromisSE Learning Management System – www.learnhmis.org.
    b. Conducts an annual security review of local HMIS-participating agencies that includes reviewing compliance with the Privacy and Security sections of this document. The Continuum Designated HMIS Lead Agency must document the findings of the review on the Privacy and Security Checklist (see Appendix E).
    c. Notifies the Continuum-designated HMIS lead agency when a System Administrator leaves the organization or when revision of the user's access level is needed because of changes in job responsibilities. The notification must be made immediately or within 24 hours. If termination is for cause, then notification must be made prior to termination. If the Continuum-designated Lead HMIS System Administrator is unable to remove End User from the System, PromisSE's HMIS vendor contract-holding Agency System Administrator can remove the user.
    d. Reports any security or privacy incidents to the HMIS System Administrator for the Continuum Designated HMIS Lead Agency . The System Administrator investigates the incident, including running applicable audit reports. If the System Administrator and Security Officer determine that a breach has occurred and/or the users/agents involved violated privacy or security guidelines, the System Administrator will report to the Continuum Designated HMIS Lead Agency. A Corrective Action Plan will be implemented. Components of the Plan must include, at a minimum, internal due diligence. It may also include removal of HMIS license, client notification if a breach has occurred, supervision, retraining, and any appropriate legal action.

All local HMIS-participating Agencies must assign an Agency Security Officer. **The Agency Security Officer**:

e. Ensures that all users/agents using the HMIS complete annual privacy and security training. Training must be provided by the Continuum-designated HMIS System Administrator or designated users/agents and be based on the PromisSE Privacy and Security standards.
f. Conducts an annual security review of the Agency that includes reviewing compliance with the Privacy and Security sections of this document. The Agency must document the findings of the review on the Privacy and Security Checklist (see Appendix E). The Agency must submit the findings to the local Lead HMIS System Administrator no later than December 31st of each year.
g. Notifies the local Continuum-designated HMIS Lead Agency System Administrator when staff leaves the organization or when revision of user's access levels is needed because of a change in job responsibilities. The notification must be made immediately, if not within 24 hours of the change. In addition, if the termination is for cause, then the local Lead HMIS System Administrator should be notified - prior to the termination.

h. Reports any security or privacy incidents to the local Continuum-designated Lead HMIS System. The HMIS System Administrator investigates the incident, including running applicable audit reports. If the System Administrator and Security Officer determine that a breach has occurred and/or the users/agents involved violated privacy or security guidelines, the System Administrator will report to the chair of the Continuum Designated HMIS Lead Agency. A Corrective Action Plan will be implemented. Components of the Plan must include, at a minimum, supervision and retraining. It may also include removal of HMIS license, client notification if a breach has occurred, and any appropriate legal action.

National criminal background checks must be completed on all End Users and the background check or the certification (see Appendix R) of the background check must be submitted to the local Lead Agency System Administrator prior to End Users gaining access to the System. For current End Users, the background check must be submitted on or before the date of the next End User Agreement.

i. If a national background check has been completed within 30 days of the training request for a new End User an additional background check does not need to be completed.
j. Any prior convictions of either embezzlement or identity theft forbid an End User from using the System permanently.
k. Any convictions of domestic violence, fraud, or any other crime of a predatory nature within the past seven years forbid an End User from using the System. Exemptions may be made on a case-by-case basis to allow the End User to utilize the System. If an end user with a history of any of these offenses requests access to the system, a written statement of explanation must be referred to your local CoC Lead Agency.
l. Background checks must be safeguarded according to local HMIS Agency policy for confidential information.
m. Sufficient documentation of a cleared background check includes either the full background check maintained by the HMIS Lead or a background check certification maintained by the HMIS Lead that explicitly states that the prohibited offenses were checked and cleared for the user (see Appendix R).
n. Continuum-designated HMIS Lead Agency conducts routine audits to ensure compliance with the HMIS Policies and Procedures. The audit could include a mix of System and on-site reviews. Continuum- designated HMIS Lead Agency will make recommendations for corrections as needed.

Privacy Standards

- All HMIS-contributing Agencies are required to have the HUD Public Notice (see Appendix H) posted and visible to clients where information is collected.
- All Agencies and Continuum Designated HMIS Lead Agencies must have a Privacy Notice (see Appendix I). They may adopt the PromisSE sample notice or integrate the sample into their existing Notice. All Privacy Notices must define the uses and disclosures of data collected on HMIS including:
    a. The purpose of collection of client information.
    b. A brief description of Policies and Procedures governing privacy, including protections for vulnerable populations.
    c. Data collection, use and purpose limitations. The Uses of data must include de-identified data.
    d. The client right to copy/inspect/correct their record.
    e. The client complaint procedure.
    f. Notice to the consumer that the Privacy Notice may be updated over time and that the Privacy Notice applies to all client information held by the Agency or Continuum Designated HMIS Lead Agency.
- All Notices must be posted on the HMIS-contributing Agency's website. Monitoring is the responsibility of the Continuum-designated HMIS Lead Agency System Security Officer.
- HMIS-contributing Agencies are required to have a Privacy Policy (see Appendix I). Agencies and Continuum Designated HMIS Lead Agencies may elect to use the Sample Privacy Policy provided by PromisSE. All Privacy Policies must include:
    a. Procedures defined in the Agency's or Continuum Designated HMIS Lead Agency's Privacy Notice
    b. Protections afforded those with increased privacy risks such as protections for victims of domestic violence, dating violence, sexual assault, and stalking. At the Agency's or Continuum Designated HMIS Lead Agency's request, protection could include at a minimum:
    c. Setting closed visibility so that only the serving Agency may see the record.
    d. The right to have a record marked as inactive.
    e. The right to remove their record from the System, upon presentation of written authorization.
    f. Security of hard copy files.
    g. The policy covers client data generated from the HMIS.
    h. Client Information Storage and Disposal.
    i. Remote Access and Usage.
    j. Use of Portable Storage/Media (Significant Security Risk).
    k. Downloads of any identifiable client information to any portable media or unsecured cloud-based system are strictly prohibited.
- Agencies and Continuum Designated HMIS Lead Agencies must protect hard copy data that includes client identifying information from unauthorized viewing or access.
    a. Client files are locked in a drawer/file cabinet.
    b. Offices that contain files are locked when not occupied.
    c. Files are not left visible to unauthorized individuals.

- Agencies and Continuum Designated HMIS Lead Agencies must have appropriate Release(s) of Information.
- The Agency or the Continuum Designated HMIS Lead Agency has adopted the PromisSE Release of Information (see Appendix G) as their Release.
- The Agency or the Continuum Designated HMIS Lead Agency can integrate the PromisSE Release of Information into their existing Releases.
- Agencies and Continuum Designated HMIS Lead Agencies are required to maintain a culture that supports privacy.
    a. Users/Agents do not discuss client information in the presence of others without a need to know.
    b. Users/Agents will eliminate unique client identifiers before releasing data to the public.
    c. The Agency configures intake workspaces that support the privacy of client interaction and data entry.
    d. User accounts and passwords are not shared among End Users or left visible for others to see. (See Appendix F).
    e. Program staff is educated to not save reports with client identifying data on portable media or cloud-based storage.
    f. Staff is trained regarding appropriate use of email communication.
- Any users who have the ability to modify data must log in every 30 days, with the exception of End Users who have read-only access levels. If an End User exceeds 30 days without logging in, they may have their system access revoked and may be required to complete retraining.
- All users/agents using the System must complete an annual End User Certification Test, which includes Privacy and Security training. Certificates documenting completion of training must be stored for review upon audit.
- Domestic Violence Victim Service Providers are precluded from entering client-level data in HMIS or providing client identified data to the System. Victim Service Providers must use a comparable database.
    a. Continuums of Care, Continuum-designated HMIS lead agencies, and Victim Service Providers must work together to determine whether the comparable database meets applicable system requirements.
    b. Continuum-Designated HMIS Lead Agency is responsible for ensuring comparable databases are HMIS-compliant.

Data Security Standards

- Information security is the responsibility of all End Users with access to the System. The risk of a data breach is the burden of each End User and all other individuals with whom they collaborate. If a data breach occurs, the knowledgeable party is required to notify the Continuum-designated HMIS Lead Agency immediately. A complete investigation into the End User's access to the system will be completed. Unless otherwise noted, monitoring items listed below must be completed on an annual basis at minimum.
- All licensed End Users of the System must be assigned Access Levels that are consistent with their job responsibilities and their business "need to know".
- All computers have virus protection with automatic updates.
- Agency Administrators and Security Officers are responsible for monitoring all computers that connect to the HMIS to ensure:
    a. The Anti-Virus Software is using the up-to-date virus database.
    b. That updates are automatic.
    c. Operating system updates are scheduled to run regularly.
    d. All computers are protected by a Firewall.
- Agency Administrators and Security Officers are responsible for ensuring Physical access to computers that connect to the HMIS is controlled.
    a. All workstations are in secured locations (locked offices).
    b. Workstations are logged off when not manned.
    c. All workstations (computers, laptops, tablets, etc.) are password protected.
    d. All HMIS End Users are prohibited from using a computer that is available to the public or from accessing the System from a public location through an internet connection that is not secured. That is, staff are not allowed to use Internet Cafes, Libraries, Airport Wi-Fi or other non-secure internet connections to connect to the HMIS.
- Agency Administrators and Security Officers are responsible for the development and implementation of a plan for remote access if staff will be using the System outside of the office, such as doing entry from home. Concerns addressed in this plan should include the privacy surrounding the off-site entry.
    a. The computer and environment of data entry must meet all the standards defined above.
    b. Downloads from the computer may not include client identifying information.
    c. System access settings should reflect the job responsibilities of the person using the System. Certain access levels do not allow for downloads.

WellSky Housing & Community Services Data Security

- SSL Encryption - Data transported across the internet to the End User's web browser is encrypted through a protected data transfer mechanism called Secure Socket Layer (SSL) encryption, which keeps data private while it is being transmitted. When an End User accesses the PromisSE (HMIS) system, an SSL (encrypted) negotiation is performed between the server at Wellsky's data center and the End User's web browser. The traffic that then flows between the server and the End User's workstation is encrypted using the SSL certificate installed on that server.

- PKI Encryption - An additional layer of encryption in the PromisSE (HMIS) system is provided by the use of a Public Key Infrastructure (PKI) Client Certificate, which requires a matching server certificate/client certificate pair, in order to decrypt the data that is sent from the End User's PromisSE (HMIS) system site to their web browser. Without the appropriate PKI Client Certificate installed on the End User's computer, their web browser is not able to decrypt the data, therefore prohibiting access the PromisSE (HMIS) system. The PKI Client Certificate is installed on an End User's computer before the End User can access the PromisSE (HMIS) system, which allows agencies to regulate exactly which devices can and cannot access the PromisSE (HMIS) system.
- Two Factor Authentication - The requirement of a username and password to access the PromisSE (HMIS) system along with the use of the PKI, is known as Two Factor Authentication, which makes it harder for potential hackers to gain access to and steal client information.
- The PromisSE (HMIS) system database lives on a server protected by a firewall, which is a device meant to keep hackers and viruses away from the server. Firewalls are in place on all servers hosted by WellSky Housing & Community Services.
- Only authorized personnel at WellSky have access to the equipment used to host the customer's data.

Disaster Recovery Plan

- WellSky Housing & Community Services is responsible for providing a disaster recovery plan, in cases of system outages. As outlined by WellSky, the basic Disaster Recovery Plan is included in our PromisSE (HMIS) system contract and "includes the following:

  a. Nightly database backups.
  b. Offsite storage of backups.
  c. 7-day backup history stored locally on instantly accessible RAID storage.
  d. 1-month backup history stored off-site
  e. 24 x 7 access to WellSky emergency line to provide assistance related to "outages" or "downtime".
  f. 24 hours backed up locally on instantly-accessible disk storage
- Standard Recovery: All customer site databases are stored online, and are readily accessible for approximately 24 hours; backups are kept for approximately one (1) month. Upon recognition of a system failure, a site can be copied to a standby server, and a database can be restored, and site recreated within three (3) to four (4) hours if online backups are accessible. As a rule, a site restoration can be made within six (6) to eight (8) hours. On-site backups are made once daily and a restore of this backup may incur some data loss between when the backup was made and when the system failure occurred.
- All internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Our Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary Core routers are configured with redundant power supplies and are configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup unites that in turn are all connected to electrical circuits that are connected to a building generator.

- All client data is backed-up online and stored on a central file server repository for 24 hours. Each night an encrypted backup is made of these client databases and secured in an offsite datacenter.
- Historical data can be restored from backups as long as the data requested is 30 days or newer. As a rule, the data can be restored to a standby server within 6-8 hours without affecting the current live site. Data can then be selectively queried and/or restored to the live site.
- For power outage, our systems are backed up via APC battery back-up units, which are also in turn connected via generator-backed up electrical circuits. For a system crash, Non-Premium Disaster Recovery Customers can expect six (6) to eight (8) hours before a system restore with potential for some small data loss (data that was entered between the last backup and the failure occurred) if a restore is necessary. If the failure is not hard drive related these times will possibly be much less since the drives themselves can be repopulated into a standby server.
- All major outages are immediately brought to the attention of executive management. WellSky supports staff helps manage communication or messaging to customers as progress is made to address the service outage. WellSky takes major outages seriously, understands, and appreciates that the customer becomes a tool and utility for daily activity and client service workflow."
- Communication between PromisSE's HMIS Vendor Contract-holding Agency, the Continuum Designated HMIS Lead Agency, and the Agencies in the event of a disaster is a shared responsibility and will be based on location and type of disaster.

System Administration and Data Quality Plan

Provider Page Set-Up

All PromisSE (HMIS) system providers are required to have provider pages accurately setup to properly record and report on data entered for that provider. The local Lead Agency System Administrator is responsible for setting up and maintaining Provider pages.

- Provider Pages are appropriately named per the PromisSE naming standards: <CoC #/Name> - <Agency name> - <Program Name><Program Type>. Example: “AL501- Housing First – Victory (TH)”.
- Inactive Provider Pages are properly identified with “ZZZ”><Provider Page Name.
- Provider Pages maintained from the PromisSE (HMIS) system, but not actively used by the local Lead HMIS Agency, are properly identified with the following prefix: “Historic<CoC #”>Provider Page Name. Example: “HistoricAL500 – Aletheia House – HUD Men (TH)”.
- Provider Pages that are used as placeholders in the PromisSE (HMIS) system are properly identified with the following prefix: “DB<CoC #> Provider Page Name. Example: “DBAL500 - Aletheia House”.

HUD HMIS Data Standards

Project Descriptor Data Elements

Project Descriptor Data Elements are completed for all projects in HMIS using the standards set forth in the most recent HMIS Data Standards Manual published by HUD. (Appendix K)

Universal Data Elements

Universal Data Elements are required to be collected by all participating in HMIS using the standards set forth in the most recent HMIS Data Standards Manual published by HUD. (Appendix K)

Program Specific Data Elements

Program Specific Data Elements are required to be collected by all participating in HMIS using the standards set forth in the most recent HMIS Data Standards Manual published by HUD. (Appendix K)

Federal Partner Program Data Elements

Federal Partner Program Data Elements, as required by HMIS Federal Partner programs, are required to be completed. Refer to the most recent HMIS Federal Partner Manuals for program specific data elements:

- ESG Program HMIS Manual
- HOPWA Program HMIS Manual
- PATH Program HMIS Manual
- RHY Program HMIS Manual
- VA Program HMIS Manual
- VASH Program HMIS Manual

Data Quality Plan

All PromisSE-participating HMIS Leads are expected to develop and implement a data quality plan using the HUD Data Quality Toolkit as a guide. Each data quality plan should address the following areas:

- Timeliness
- Completeness
- Accuracy
- Monitoring

Data Quality Monitoring Plan

All PromisSE-participating HMIS Leads are expected to develop and implement a data quality monitoring plan using the HUD Data Quality Toolkit as a guide. Each data quality monitoring plan should address the following areas:

- Establishing Data Quality Benchmarks and Goals
- Defining Roles and Responsibilities
- Establishing Timelines
- Calculating Compliance Rates
- Establishing Timeframes for Data Quality Reports
- Data Quality Reports
- Null/Missing and Unknown/Don't Know/Refused Report
- Universal Data Elements by Client ID
- Length of Stay Report by Client ID
- Intake and Data Entry Date Timeliness Report
- Bed Utilization Tool

Artificial Intelligence, Machine Learning, and Client Data

Any AI/ML tool using HMIS data may only work on de-identified or aggregated data—no raw PII (names, birthdates, SSNs, addresses, or other unique IDs) can be included. Suitable uses include trend spotting, drafting reports, and predicting service needs, but all AI output must be encrypted and reviewed by staff for errors or bias. AI is a support tool only; it does not replace a caseworker's judgment or a client's signed Release of Information.

Workflow Requirements

- Assessments set in the Provider Page Configuration are appropriate for the funding stream.
- End Users performing data entry have latest copies of the workflow guidance documents.
- If using paper, the intake data collection forms correctly align with the workflow.
- 100% of clients are entered into the System immediately, and if not immediately, within 24 hours of client intake.
- Continuum Designated HMIS Lead Agencies are actively monitoring program participation and existing clients. Clients are exited within 30 days of last contact unless program guidelines specify otherwise.
- If exiting after 30 days without contact, exit date should reflect the last date of contact with client.

- All required program information is being collected.
- All HMIS participants are required to enter, at a minimum, the Universal Data Elements (Appendix K) as well as the program-specific data elements.
- Programs that serve over time are required to complete additional program elements as defined by the funding stream.
- Data sharing is properly configured for sharing information internally between programs, including the use of visibility groups.
- External data sharing aligns with any local, state or Federal laws; including the use of visibility groups.

Electronic Data Interchange

Electronic Data Interchange (EDI) is the direct computer-to-computer exchange of standard formatted business transactions between one or more business partners, known as trading partners. EDI permits organizations to generate, receive, and process data without human intervention.

- Agencies requesting the ability to import or export data from the HMIS must receive permission from the Continuum-designated HMIS Lead Agency. Change to "sharing data" language.
    a. Importing data from one database to another (i.e. mass data dump) requires permission from the Continuum-designated Lead HMIS System Administrator.
    b. Uploading client-specific documents such as case notes or identity documents such as birth certificates, marriage licenses, etc. do not require the permission of the Continuum-designated Lead Agency.
- Continuum Designated HMIS Lead Agencies may elect to participate in de-identified research data sets to support research and planning.
    a. De-identification will involve the masking or removal of all identifying or potentially identifying information such as the name, Unique Client ID, SS#, DOB, address, Agency name, and Agency location.
    b. A geographic analysis will be restricted to prevent any data pools that are small enough to inadvertently identify a client by other characteristics or combination of characteristics.
    c. Programs used to match and/or remove identifying information will not allow a re-identification process to occur. If retention of identifying information is maintained by a "trusted party" to allow for updates of an otherwise de-identified data set, the organization/person charged with retaining that data set will certify that they meet medical/behavioral health security standards and that all identifiers are kept strictly confidential and separate from the de-identified data set.
    d. Continuum Designated HMIS Lead Agencies will be provided a description of each Study being implemented when including data from that Continuum Designated HMIS Lead Agency. Continuum Designated HMIS Lead Agencies may opt out of the Study through a written notice to the requesting Continuum Designated HMIS Lead Agency.

Staff Training and Required Meetings

- All End Users are recertified through User Recertification Test annually, found on the PromisSE Learning Management System – www.learnhmis.org.
- All End Users participate in Workflow Training and Training Updates for their assigned Workflows.
- All End Users will have access to the list of HUD Universal Data Elements (see Appendix K).

Appendix A – CoC and Agency Participation Agreement

Continuum of Care Program Management Information System of the Southeast

Participation Agreement between the COC and

_____

(Name of Agency)

This agreement is entered into on _____ (mm/dd/yy) between _____ (COC NAME), hereafter known as the CoC, and _____ (Agency name), hereafter known as "Agency," regarding access and use of the CoC Program Management Information System of the Southeast, hereafter known as "PromisSE."

Introduction

PromisSE, a shared human services database, allows authorized personnel at homeless and human service provider agencies throughout the participating regions of the Southeast to enter, track, and report on information concerning their own clients and to share information, subject to appropriate inter-Agency agreements, on common clients.

PromisSE's goals are to:

- Improve coordinated care for and services to homeless persons in the PromiSE implementation service area.
- Provide a user-friendly and high quality automated records System that expedites client intake procedures, improves referral accuracy, increases case management and administrative tools, creates a tool to follow demographic trends and service utilization patterns of families and individuals either currently experiencing or about to experience homelessness, and supports the collection of quality information that can be used for program improvement and service-planning.
- Meet the reporting requirements of the U.S. Department of Housing and Urban Development (HUD) and other funders as needed.

In compliance with all State and Federal requirements regarding client confidentiality and data security. PromisSE is designed to collect and deliver timely, credible, quality data about services and homeless persons or persons at risk of being homeless. The CoC administers PromisSE through a contract with HUD.

COC Responsibilities

- The CoC will provide the Agency 24-hour access to PromisSE data-gathering System via an internet connection, with which the Agency is responsible for maintaining connectivity.
- The CoC will provide model Privacy Notices, Client Release forms and other templates for agreements that may be adopted or adapted at the participating Agency.
- The CoC will provide both initial training and periodic updates to that training for core Agency staff regarding the use of PromisSE, with the expectation that the Agency will take responsibility for conveying this information to all Agency staff using the System.
- The CoC will provide basic user support and technical assistance (i.e., general troubleshooting and assistance with standard report generation). Access to this basic technical assistance will normally be

available from 8:30 AM. to 4:30 PM. on Monday through Friday (with the exclusion of holidays) and limited availability after regular hours.

- The CoC will not publish reports on client data that identify specific agencies or persons, without prior Agency (and where necessary, client) permission. Public reports otherwise published will be limited to the presentation of aggregated data within the PromisSE database.

Agency Responsibilities

- The Agency will comply with the PromisSE Homeless Management Information System (HMIS) Operating Policies and Procedures.
- The Agency will designate and staff one HMIS Agency Administrator who shall abide by the policies and procedures set out in the PromisSE Homeless Management Information System (HMIS) Operating Policies and Procedures.
- The Agency will designate and staff one HMIS Security Officer who shall abide by the policies and procedures set out in the PromisSE Homeless Management Information System (HMIS) Operating Policies and Procedures.
- The Agency will ensure that both initial training and periodic updates to that training for core Agency staff regarding the use of PromisSE is completed in accordance with the requirements set out in the CoC Homeless Management Information System (HMIS) Operating Policies and Procedures.
- Agencies serving clients in more than one CoC must participate in each CoC where clients are located. Participation necessitates that the agency must adhere to each CoC's procedures, policies, participation requirements, etc.

Privacy and Confidentiality

Protection of Client Privacy

- The Agency will comply with all applicable Federal and State laws regarding the protection of client privacy.
- The Agency will comply specifically with Federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2, regarding disclosure of alcohol and/or drug abuse records. A general authorization for the release of medical or other information is NOT sufficient for this purpose. Member Agencies shall recognize that Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.
- The Agency will comply specifically with the Health Insurance Portability and Accountability Act of 1996, 45 C.F.R., Parts 160 & 164, and corresponding regulations established by the U.S. Department of Health and Human Services.
- The Agency will comply with all policies and procedures established by the CoC pertaining to the protection of client privacy.
- Each Agency will abide by local Laws, which in general terms, require an individual to be informed that any and all medical records she/he authorizes to be released, whether related to physical or mental health, may include information indicating the presence of a communicable or venereal disease. The Agency is required to inform the individual that these records may include, but are not limited to, the inclusion of information on diseases such as hepatitis, syphilis, gonorrhea, tuberculosis, and HIV/AIDS.

- Each Agency will abide specifically by local Mental Health Law. In general terms, this law prohibits agencies from releasing any information that would identify a person as a client of a mental health facility, unless client consent is granted.

Client Confidentiality

- The Agency agrees to provide a copy of the CoC Privacy Notice (Appendix I) or an acceptable Agency-specific alternative) to each client. The Agency will provide a verbal explanation of PromisSE and arrange for a qualified interpreter/translator in the event that an individual is not literate in English or has difficulty understanding the Privacy Notice or associated Consent Form(s).
- The Agency will not solicit or enter information from clients into the PromisSE database unless it is essential to provide services or conduct evaluation or research.
- The Agency will not divulge any confidential information received from PromisSE to any organization or individual without proper written consent by the client unless otherwise permitted by applicable regulations or laws.
- The Agency will ensure that all persons who are issued an End User Identification and Password to PromisSE abide by this Participation Agreement, including all associated confidentiality provisions. The Agency will be responsible for oversight of its own related confidentiality requirements.
- The Agency agrees that it will ensure that all persons issued an End User ID and Password complete a formal training on privacy and confidentiality, demonstrate mastery of that information, and sign a PromisSE End User Agreement prior to activation of the End User License.
- The Agency acknowledges that ensuring the confidentiality, security, and privacy of any information downloaded from the System by the Agency is strictly the responsibility of the Agency.

Inter-Agency Sharing of Information

- The Agency acknowledges that all forms provided by PromisSE regarding client privacy and confidentiality are shared with the Agency as generally applicable models that may require specific modification in accord with Agency-specific rules. The Agency will review and revise (as necessary) all forms provided by PromisSE to assure that they comply with the laws, rules, and regulations that govern its organization.
- The Agency acknowledges that informed client consent is required before any basic identifying client information is shared with other Agencies in the System. The Agency will document client consent on the PromisSE Client Release of Information Form.
- If the client has given approval through a completed PromisSE Client Release of Information Form, the Agency may elect to share information with other partnering agencies in PromisSE.
- The Agency will incorporate a PromisSE release clause into its existing Agency Authorization for Release of Information Form(s) if the Agency intends to share restricted client data within PromisSE. Restricted information, including progress notes and psychotherapy notes about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence concerns shall not be shared with other participating Agencies without the client's written, informed consent. Agencies with visibility set to "closed" may not share "closed" client information without the client's written, informed consent, as well as a fully executed inter-Agency "closed" data sharing agreement.

- Agencies with which information is shared are each responsible for obtaining, at a minimum, an updated PromisSE Release of Information, before allowing further sharing of client records. The local System Administrator will facilitate any sharing of "closed" data in PromisSE.
- The Agency acknowledges that the Agency itself bears primary responsibility for oversight of the sharing of all data it has collected via PromisSE.
- The Agency agrees to place all Client Authorization for Release of Information forms related to PromisSE in a file in a secure location controlled by the Agency and that such forms will be made available to the CoC for periodic audits. The Agency will retain these PromisSE-related Authorizations for Release of Information forms for a period of 7 years from the date of creation, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
- The Agency acknowledges that clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.

Custody of Data

- The Agency and the CoC understand that the Agency and the CoC as an administrator are custodians – NOT owners - of the data.
- In the event that the PromisSE Lead Agency ceases to exist, Member Agencies will be notified and provided reasonable time to access and save client data on those served by the Agency, as well as statistical and frequency data from the entire System. Thereafter, the information collected on the centralized server will be purged or appropriately stored.
- In the event that the CoC ceases to exist, the custodianship of the data within PromisSE will be transferred to another authorized organization for continuing administration, and all PromisSE Member Agencies will be informed in a timely manner.

Data Entry and Regular Use of PromisSE

- The Agency will not permit End User IDs and Passwords to be shared among End Users.
- If a client has previously given the Agency permission to share information with multiple agencies (beyond basic identifying information and non-restricted service transactions), and then chooses to revoke that permission with regard to one or more of these agencies, the Agency will contact its partner Agency/agencies and explain that, at the client's request, portions of that client record will no longer be shared. The Agency will then "lock" those portions of the record impacted by the revocation to the other Agency or agencies.
- If the Agency receives information that necessitates a client's information be entirely removed from the PromisSE, the Agency will work with the client to complete a brief Delete Request Form, which will be sent to the CoC for de-activation of the client record.
- The Agency will enter all minimum required data elements as defined for all persons who are participating in services funded by the U.S. Department of Housing and Urban Development (HUD) Permanent Housing Program, Permanent Supportive Housing Program, Supportive Services Program, Transitional Housing Program, Safe Haven Program, Joint Transitional Housing and Rapid Rehousing Program, Housing Opportunities for Persons with HIV/AIDS Program, or Emergency Shelter Grant Program.

- The Agency will enter data in a consistent manner and will strive for real-time, or close to real-time, data entry.
- The Agency will routinely review records it has entered in PromisSE for completeness and data accuracy. The review and data correction process will be made according to PromisSE published Data Quality Policies and Procedures.
- The Agency will not knowingly enter inaccurate information into PromisSE, with the exception of specific clients for which the agency is permitted to input coded data into the System.
- The Agency acknowledges that with a current standard PromisSE Client Release of Information form on file, it can update, edit, and print out a client's information. Once the PromisSE Client Release of Information expires, the Agency can no longer edit or print the record.
- The Agency acknowledges that once that Client Release of Information expires, any new information entered into the database will be closed to sharing until a new Client Release of Information is signed. Information entered before the date of the expired release will continue to be available to the sharing partners.
- The Agency acknowledges that a modified Agency Authorization to Release Information form, with a PromisSE clause, permits it to share restricted client information with select agencies in compliance with the Agency's approved Confidentiality Policies and Procedures.
- The Agency will prohibit anyone with an Agency-assigned End User ID and Password from entering offensive language, profanity, or discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation.
- The Agency will utilize PromisSE for business purposes only.
- The Agency will keep updated virus protection software on Agency computers that access PromisSE.
- Transmission of material in violation of any United States Federal or State regulations is prohibited.
- The Agency will not use PromisSE with intent to defraud the Federal, State, or local government, or an individual entity, or to conduct any illegal activity.
- The Agency agrees that PromisSE or the local Continuum of Care PromisSE Planning Committee may convene local or regional End User Meetings to discuss procedures, updates, policy and practice guidelines, data analysis, and software/ hardware upgrades. The Agency will designate at least one specific Staff member to regularly attend End User Meetings.
- Notwithstanding any other provision of this Participation Agreement, the Agency agrees to abide by all policies and procedures relevant to the use of PromisSE that the CoC publishes from time to time

Publication of Reports

- The Agency agrees that it may release only aggregated information generated by HMIS that is specific to its own services.

Database Integrity

- The Agency will not share assigned End User IDs and Passwords to access PromisSE with any other organization, governmental entity, business, or individual.

- The Agency will not intentionally cause corruption of PromisSE in any manner. Any unauthorized access or unauthorized modification to the System information or interference with normal System operations will result in immediate suspension of services, and, where appropriate, legal action against the offending entities.

Hold Harmless

- The CoC makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold the CoC harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in the PromisSE; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold the CoC harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, misdeliveries, or service interruption caused by WellSky, by the Agency's or other member Agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. The CoC shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of the CoC. The CoC agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of the CoC.
- It is the responsibility of each Agency to maintain a current insurance policy that is sufficient to cover theft of or damage to ALL PromisSE -related hardware and software.

Terms and Conditions

- The parties hereto agree that this agreement is the complete and exclusive statement of the agreement between parties and supersedes all prior proposals and understandings, oral and written, relating to the subject matter of this agreement.
- The Agency shall not transfer or assign any rights or obligations under the Participation Agreement without the written consent of the CoC.
- This agreement shall remain in force until revoked in writing by either party, with 30 days advance written notice. The exception to this term occurs if allegations or actual incidences arise regarding possible or actual breaches of this agreement. Should such situations arise, the PromisSE System Administrator may immediately suspend access to PromisSE until the allegations are resolved in order to protect the integrity of the System.
- This agreement may be modified or amended by written agreement executed by both parties with 30 days advance written notice.
- The parties agree that the CoC, Inc. is a third-party beneficiary of this contract and may enforce the terms and provisions of this contract as applicable.

IN WITNESS WHEREOF, the parties have entered into this Agreement:

CoC Name	Agency Name
CoC Address	Agency Address
CoC Representative Printed Name	Agency Representative Printed Name
CoC Representative Title	Agency Representative Title
CoC Representative Signature	Agency Representative Signature
Date (mm/dd/yy)	Date (mm/dd/yy)

ASSURANCE

_____ (Name of Agency) assures that the following fully executed documents will be on file and available for review.

- The Agency's official Privacy Notice for PromisSE clients.
- Executed PromisSE Client Release of Information forms.
- Executed Agency Authorizations for Release of Information as needed.
- Certificates of Completion for required training for all PromisSE System End Users.
- A fully executed End User Agreement for all PromisSE System End Users.
- A current Agency-Specific PromisSE Policy and Procedure Manual.

By: _____

Title: _____

Appendix B – CoC Agency Administrator Agreement

Name	Agency

All HMIS participating agencies must designate and staff one HMIS Agency Administrator. Agency Administrator requirements and responsibilities include, but are not limited to, the following:

- Has completed, at a minimum, basic system data entry training.
- Ensure that all Agency users have signed End User Agreement documents on file.
- Ensure that all Users complete an annual End User Certification Test, which includes Privacy and Security training. This training can be accessed through the PromisSE Learning Management System – www.learnhmis.org.
- Ensure that all Users have completed workflow training and related updates, and have documentation of training.
- Ensure that the Agency complies with the CoC Data Security standards.
- Ensure that the Agency complies with the HMIS Policies and Procedures, has completed the Compliance Checklist, and is responsible for returning it to the local Lead Agency System Administrator.
- Ensure that all Users have submitted a criminal background check to the local Lead Agency System Administrator.

The original Agency Administrator Agreement shall be kept on file at the Agency. Forms completed by individuals no longer employed by the Agency shall be kept on file for a minimum of five years.

The CoC makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold the CoC harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in PromisSE; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold the CoC harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, misdeliveries, or service interruption caused by WellSky, by the Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. The CoC shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of the CoC. The CoC agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of the CoC.

This agreement is in effect for a period of one (1) year after the date of signing. Agency Administrators are required to complete HMIS End User Certification testing and to document compliance monitoring annually, at which time a new agreement will be provided. Failure to participate in annual Certification and/or maintain a current agreement may result in immediate termination or suspension of the user's PromisSE (HMIS) system license and access to the PromisSE (HMIS) system. Failure to comply with the provisions of this Agency Administrator Agreement is grounds for immediate termination. Your signature below indicates your agreement to comply with this Agency Administrator Agreement.

Employee Printed Name	Agency Official Printed Name
Employee Signature	Agency Official Signature
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix C – Agency Security Officer Agreement

Name **Agency**

All HMIS participating agencies must designate and staff one HMIS Security Officer. Security Officer requirements and responsibilities include, but are not limited to, the following:

- Ensures that all staff using the System complete annual privacy and security training. Training must be provided by the CoC designated trainers and be based on the CoC Privacy and Security standards. This training is also available through the PromisSE Learning Management System – www.learnhmis.org.
- Conducts an annual security review of the agency that includes reviewing compliance with the Privacy and Security sections of the CoC Homeless Management Information System (HMIS) Operating Policy and Procedure. The Agency must document the findings of the review on the Privacy and Security Checklist and submit the findings to the local Lead HMIS System Administrator no later than December 31st of each year.
- Notifies the local Lead Agency System Administrator when a staff person leaves the organization or when revision of the user's access level is needed because of a change in job responsibilities. The notification must be made within 24 hours of the change, if not immediately. If a staff person is being terminated for cause, then notification to the Lead HMIS Agency must be made prior to termination.
- Reports any security or privacy incidents to the local Lead HMIS System Administrator for the CoC Jurisdiction. The System Administrator investigates the incident including running applicable audit reports. If the System Administrator and Security Officer determine that a breach has occurred and/or the staff involved violated privacy or security guidelines, the System Administrator will report to the head of the CoC. A Corrective Action Plan will be implemented. Components of the Plan must include, at a minimum, supervision and retraining. It may also include removal of HMIS license, client notification if a breach has occurred, and any appropriate legal action.

The original Security Officer Agreement shall be kept on file at the Agency. Forms completed by individuals no longer employed by the Agency shall be kept on file for a minimum of five years.

The CoC makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold the CoC harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in ***PromisSE***; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold the CoC harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, misdeliveries, or service interruption caused by WellSky, by the Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. The CoC shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of the CoC. The CoC agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of the CoC.

This agreement is in effect for a period of one (1) year after the date of signing. Security Officers are required to complete HMIS End User Certification testing and documented Privacy & Security compliance monitoring annually, at which time a new agreement will be provided. Failure to participate in annual Certification, Privacy & Security monitoring, and/or maintain a current agreement may result in immediate termination or suspension of the user's PromisSE (HMIS) system license and access to the PromisSE (HMIS) system. Failure to comply with the provisions of this Security Officer Agreement is grounds for immediate termination. Your signature below indicates your agreement to comply with this Security Officer Agreement.

Employee Printed Name

Agency Official Printed Name

Employee Signature

Agency Official Signature

Date (mm/dd/yy)

Date (mm/dd/yy)

Appendix D – CoC Policies and Procedures Compliance Checklist

Agency Name:_____

_____ (Int.) Agency has received a copy of the CoC Operating Policies and Procedures

_____ (Int.) Agency has a fully executed Agency Participation Agreement

_____ (Int.) Agency has a Board-approved Confidentiality Policy governing HMIS Privacy and Security Standards

_____ (Int.) Agency has assigned an HMIS Agency Administrator with an executed agreement

_____ (Int.) Agency has assigned an HMIS Security Officer with an executed agreement

_____ (Int.) Agency has submitted all End User criminal background checks

_____ (Int.) Agency has provided End Users with the HUD Data Elements

_____ (Int.) Agency has provided End User with training on the HUD definition of homelessness and the priority of homelessness documentation

_____ (Int.) Agency and End Users understand and will comply with the CoC Data Quality Plan

Agency Official Printed Name	CoC Official Printed Name
Agency Official Signature	CoC Official Signature
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix E – Privacy and Security Checklist

Agency Official Name

Security Officer Name

_____ (Int.) Agency has the HUD Public Notice posted in an area visible to clients.

_____ (Int.) Agency has an HMIS Privacy Notice that complies with the requirements set forth by the CoC HMIS Operating Policies and Procedures and is available to all clients.

_____ (Int.) Agency has a copy of the HUD Public Notice and the Privacy Notice on its website.

_____ (Int.) Client files with hard copy data that includes client identifying information are protected behind one lock, at a minimum, from unauthorized access.

_____ (Int.) Offices that contain client files are locked when not occupied.

_____ (Int.) Client files are not left visible to unauthorized individuals.

_____ (Int.) Agency has adopted the PromisSE Release of Information and requests this for every client.

_____ (Int.) HMIS workspaces are configured to support the privacy of client interaction and data entry.

_____ (Int.) User accounts and passwords are not shared or left visible for others to see.

_____ (Int.) End Users do not save HMIS reports with identifying client information on portable media.

_____ (Int.) All HMIS workstations, including laptops and remote workstations, have virus protection and automatic updates.

_____ (Int.) End Users are not accessing the HMIS on a public computer or from an internet connection that is not secured.

_____ (Int.) Agency has a documented plan for remote access if End Users are accessing the HMIS outside of the office setting.

Findings _____

Corrective Actions _____

Deadline for Completion _____

Security Officer Printed Name

Agency Official Printed Name

Security Officer Signature

Agency Official Signature

Date (mm/dd/yy)

Date (mm/dd/yy)

Appendix F – License Agreement and Statement of Confidentiality

Name _____ Agency _____

Employees, volunteers, staff and any persons with access to the **Program Management Information System Southeast *(PromisSE)*** are subject to certain guidelines regarding its use. *PromisSE* contains a wide range of personal and private information on individuals and ALL such information must be treated carefully, confidentially, and professionally by those who access it. Guidelines for use of *PromisSE* include, but are not limited to, the following:

- User IDs and passwords must be kept secure and confidential and shall not be shared.
- Current client or Legal Guardian consent, as documented by a Release of Information (ROI), is required before entering, updating, editing, printing, or disclosing basic identifying and non-confidential service transactions/information with other Member Agencies and/or their employees, volunteers and/or staff. Otherwise, limited visibility must be coordinated with the CoC.
- Only general, non-confidential information is to be entered in the "other notes/comments" section of the Client Profile in *PromisSE*. Confidential information, including TB diagnosis, domestic violence, and mental/physical health information shall not be entered in this section.
- Confidential information obtained via *PromisSE* is to remain confidential, even if the end user's relationship with the Agency changes or concludes for any reason.
- Information beyond basic identifying data, which includes all assessment screens (all screens beyond profile, agency, and community fields), is not to be edited. If an update or correction is needed, a new assessment must be created.
- The agency/organization end user is allowed to enter or modify data ONLY for clients being served by that agency.
- Misrepresentation of the client through the deliberate entry of inaccurate information is prohibited.
- Client records shall NOT be deleted from *PromisSE*. If a client or legal guardian of a client chooses to rescind *PromisSE* Release of Information, the appropriate record shall immediately become "inactive".
- Discriminatory comments based on race, color, religion, creed, national origin, ancestry, handicap, socioeconomic status, marital status, age, gender, and/or sexual orientation are NOT permitted in *PromisSE*. Profanity and offensive language are NOT permitted in *PromisSE*. Violators shall have their System privileges revoked and they will NOT be allowed further access to HMIS.
- All end users who have the ability to enter data into PromisSE must log in to the PromisSE (HMIS) system at least ONCE every 30 days. Failure to login in for 30 days may result in the revocation of access to the PromisSE (HMIS) system. Basic training may be required to regain access, as determined by the CoC/HMIS Lead Administrator.
- *PromisSE* is to be used for business purposes only. Transmission of material in violation of any United States Federal or State of Alabama regulation/laws is prohibited, including material that is copyrighted, legally judged to be threatening or obscene, and/or considered protected by trade secret. *PromisSE* shall NOT be used to defraud the Federal, State, Local or City government nor any individual entity nor to conduct any illegal activity.
- Users must log off of the System before leaving their computer/workstation unattended; Failure to log off the System appropriately may result in a breach of client confidentiality and System security.
- Hard copies of the PromisSE (HMIS) system information must be kept in a secure file.

- When hard copies of the PromisSE (HMIS) system information are no longer needed, they must be properly destroyed to maintain confidentiality.
- Any unauthorized access or unauthorized modification to the System information/*PromisSE* database or
- Interference with normal System operations will result in immediate suspension of your access to the *PromisSE* and may jeopardize your employment status with the Agency.

I have submitted a national background check to the Local Lead System Administrator and verify that I have never been convicted of identity theft or embezzlement. I verify that I have not been convicted of a domestic violence, fraud offense, or any other crime of a predatory nature within the past seven years. The CoC/HMIS Lead Administrator must give any waiver of this requirement.

The original PromisSE License Agreement & Statement of Confidentiality shall be kept on file at the Agency. Forms completed by individuals no longer employed by the Agency shall be kept on file for a minimum of five years.

The CoC makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold the CoC harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in PromisSE; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold the CoC harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, misdeliveries, or service interruption caused by WellSky, by the Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, and/or technological difficulties. The CoC shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of the CoC. The CoC agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of the CoC.

This agreement is in effect for a period of one (1) year after the date of signing. End users are required to complete HMIS End User Certification testing annually, at which time a new agreement will be provided. Failure to participate in annual Certification and/or maintain a current agreement may result in immediate termination or suspension of the user's The PromisSE (HMIS) system license and access to The PromisSE (HMIS) system. Failure to comply with the provisions of this Statement of Confidentiality is grounds for immediate termination. Your signature below indicates your agreement to comply with this Statement of Confidentiality.

Employee Printed Name	Agency Official Printed Name
Employee Signature	Agency Official Signature
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix G – PromisSE Release of Information (ROI)

Continuum of Care (CoC) Program Management Information System of the Southeast (PromisSE)

Client's Last Name_____ First Name_____ MI_____

Date of Birth_____ Social Security Number_____

*** The Federal Privacy Act of 1974 requires that you be notified that disclosure of your Social Security number is voluntary under this record-keeping System. This System was authorized pursuant to directives from Congress and the Department of Housing and Urban Development (HUD). The Social Security number is used to verify identity, assure timely delivery of services, prevent duplication of services, and generate accurate required reports to HUD.**

PromisSE is a shared, electronic record keeping System that captures information about people experiencing homelessness or near homelessness, including their service needs. Our Agency is participating in PromisSE, a database that collects information on clients served by its member agencies and the services they provide.

I understand that all information gathered about me is personal and private and that I do not have to share information collected in PromisSE. It has been explained to me that all information collected will serve for reporting purposes and as a precaution to prevent duplication of services to ineligible individuals and families. I have had an opportunity to ask questions about PromisSE and to review the identifying information, which is authorized by this release for the PromisSE Member Agencies to share. I also understand that information about non-confidential services provided to me by human service agencies in the CoC may be shared with other participating in PromisSE agencies. This Release of Information will remain in effect for **5 (five) years** and will expire on _____ unless I make a formal request to this Agency that I no longer wish to participate in PromisSE.

Upon a life-threatening emergency or death, my System information will be used for identification purposes.

Upon written consent, a community partner that is a non-System participating agency, including many state or local service agencies can utilize your System information to provide additional services. **This is dependent upon the receipt of a signed document verifying your consent to release your information to a Community Partner.**

_____I authorize sharing my data.

_____I do not authorize sharing my data,

The CoC, as PromisSE Member Agency, to share my information between all participating PromisSE agencies. I authorize the use of a copy of this original document to serve as a verification for the purposes stated above.

Client's (Head of Household) Printed Name	Other Adult in HH Printed Name
Client's (Head of Household) Signature	Other Adult in HH Signature
Date (mm/dd/yy)	Date (mm/dd/yy)

Based on the information on the previous page:

_____I authorize sharing my dependent's data.

_____I do not authorize sharing my dependent's data.

The CoC, as PromisSE Member Agency, to share my information between all participating PromisSE agencies. I authorize the use of a copy of this original document to serve as a verification for the purposes stated above.

Dependent's Name	DOB	Dependent's Name	DOB
Dependent's Name	DOB	Dependent's Name	DOB
Dependent's Name	DOB	Dependent's Name	DOB
Dependent's Name	DOB	Dependent's Name	DOB
Dependent's Name	DOB	Dependent's Name	DOB
Dependent's Name	DOB	Dependent's Name	DOB

Legal Guardian's Authorizing Signature

Date (mm/dd/yy)

Agency Representative's Authorizing Signature

Agency Representative's Printed Name

Date (mm/dd/yy)

FOR STAFF USE ONLY	
_____	Staff obtained telephonic consent from client and dependents under 18 as listed above
_____	Staff did not obtain telephonic consent from client and dependents under 18 as listed above.

Appendix H – Public Notice

Continuum of Care

Program Management Information System of the Southeast (PromisSE)

Also known as Homeless Management Information System (HMIS)

We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that fund and/or operate these programs. Other personal information that we collect is important to run our programs, to improve services for homeless and at-risk persons, and to better understand the needs of homeless and at-risk persons. We only collect information that we consider appropriate.

The Homeless Management Information System (HMIS) was developed to meet a data collection requirement made by the United States Congress to the Department of Housing and Urban Development (HUD). Congress passed this requirement in order to get a more accurate count of individuals who are homeless and to identify the need for and use of different services by those individuals and families. Your information may be shared among the CoCs that participate in PromisSE.

Your information can be shared with other HMIS participating Agencies throughout the Implementation. The information entered by participating providers includes basic identifying demographic data (e.g., name, birth date, and gender), the nature of your situation, and the services and referrals received from the participating Agency. Your information may be shared with other HMIS-participating agencies and users during both in-person and virtual (online) meetings. Virtual meetings are secured through the meeting software vendor's security protocols (e.g., data encryption and the ability to only allow authorized individuals into meetings).

Participating Agencies collect personal information directly from you for reasons that are discussed in their privacy Policy. They may be required to collect personal information by law or by the organizations that fund and/or operate these programs. Other personal information that is collected is important to operate programs, to improve services, and to better understand client needs. They only collect information that they consider appropriate and accurate. The collection and use of all personal information is guided by strict standards of confidentiality.

Maintaining the privacy and safety of those clients whose records reside in HMIS and the /Agencies that use the HMIS is very important to us. Information gathered about each client and each Agency is personal and private. We collect information only when appropriate to provide services, manage our organization and the Database, or as required by law. The ownership of all records contained within the HMIS is retained by the organization/Agency that collected and entered or updated the client's information.

The collection and use of all personal information is guided by strict standards of confidentiality. A copy of our Privacy Policy describing our privacy practice is available to all clients upon request.

This policy may be amended at any time and amendments may affect information obtained before the date of change.

Appendix I – Privacy Policy to Clients

The Homeless Management Information System (HMIS) was developed to meet a data collection requirement made by the United States Congress to the Department of Housing and Urban Development (HUD). Congress passed this requirement in order to get a more accurate count of individuals who are homeless and to identify the need for and use of different services by those individuals and families. Your information may be shared among the CoCs that participate in PromisSE.

Client information can be shared with other HMIS participating Agencies throughout the Implementation. The information entered by participating providers includes basic identifying demographic data (e.g., name, birth date, and gender), the nature of the client's situation, and the services and referrals received from the participating Agency. Client information may be shared with other HMIS-participating agencies and users during both in-person and virtual (online) meetings. Virtual meetings are secured through the meeting software vendor's security protocols (e.g., data encryption and the ability to only allow authorized individuals into meetings).

Participating Agencies collect personal information directly from you for reasons that are discussed in their privacy Policy. They may be required to collect personal information by law or by the organizations that fund and/or operate these programs. Other personal information that is collected is important to operate programs, to improve services, and to better understand client needs. They only collect information that they consider appropriate and accurate. The collection and use of all personal information is guided by strict standards of confidentiality.

Maintaining the privacy and safety of those clients whose records reside in HMIS and the /Agencies that use the HMIS is very important to us. Information gathered about each client and each Agency is personal and private. We collect information only when appropriate to provide services, manage our organization and the Database, or as required by law. The ownership of all records contained within the HMIS is retained by the organization/Agency that collected and entered or updated the client's information.

Confidentiality Rights

Each participating Agency is required to have a confidentiality policy that has been approved by its Board of Directors. _____ (Continuum-designated HMIS lead agency) must also have a Board Approved confidentiality policy. _____ (Continuum-designated HMIS lead agency) operates the HMIS in accordance with HUD and HIPAA confidentiality regulations, including those covering programs that receive HUD funding for homeless services (Federal Register/Vol. 69, No. 146), and those covered under the HIPAA privacy and security rules which govern confidential health information such as the diagnosis, treatment, of a mental health disorder, a drug or alcohol disorder, and AIDS/HIV condition or a domestic violence situation. Other rules that may also apply include 42 CFR Part 2 governing drug and alcohol records.

_____ (CoC #) is restricted to using or disclosing personal information from the HMIS to the following circumstances:

- For functions related to payment or reimbursement for services.
- For functions related to helping Agencies operate the System.
- For functions related to the development of reports to better plan services.
- To carry out administrative functions including but not limited to legal, audit, personnel, planning, oversight and management functions;
- To develop databases used for research, where all identifying information has been removed.
- For coordinating housing and supportive services for veterans experiencing homelessness, including disclosure to

the U.S. Department of Veterans Affairs through the VA HMIS Repository.

- To support contractual research where privacy conditions are met with an approved Institutional Review Board (IRB), and only if the shared information includes no identifying information about the client.
- Where a disclosure is required by law and disclosure complies with, and is limited to, the requirements of the law. Instances, where this might occur, are during a medical emergency, to report a crime against the staff of the Agency, or to avert a serious threat to health or safety.

Your Information Rights

All requests for client personal information located within the HMIS will be routed to the Agency/organization that collected and entered or updated the information.

_____ (CoC #) may not disclose your personal protected information located within the HMIS except as required by law or to help the participating Agency/organization that collected/entered/updated the information operate the System.

_____ (CoC #) may not publish reports on client data that identifies specific Agencies or persons. Public reports otherwise published will be limited to the presentation of aggregated data that does not disclose personal identifying information.

Please contact the Agency to which you gave your personal information in order to:

- Access or see your record.
- Correct your record
- Request that your record by shared with another person or organization.
- Terminate or withdraw a consent to release information.
- File a grievance if you feel that your rights have been violated.

Please note that you have the right to refuse consent to share your information between participating Agencies. You cannot be denied services that you would otherwise qualify for if you refuse to share information. Please note that if you refuse this permission, information will still be entered into the System for statistical purposes, but your information will be closed so that only that Agency you gave the information to and System Administrators operating the Database may see your information.

Please feel free to contact us if you feel that your information rights have been violated. Please address your written communication to the CoC (One Roof 1515 6th Ave S 5th Floor, Birmingham, AL 35233). Please include your contact information. We will respond in writing within 7 working days of the receipt of your letter.

How Your Information Will Be Kept Secure

Protecting the safety and privacy of individuals receiving services and the confidentiality of their records is of paramount importance to us. Through training, policies and procedures, and software we have done several things to make sure your information is kept safe and secure:

- The computer program we use has the highest degree of security protection available.
- Only trained and authorized individuals will enter or view your personal information.
- Your name and other identifying information will not be contained in HMIS reports that are issued to local, state, or national Agencies.
- Employees receive training in privacy protection and agree to follow strict confidentiality standards before using the System.
- The server/database/software only allows authorized individuals access to the information. Only those who should see certain information will be allowed to see that information.

- The server/database will communicate using 128-bit encryption – an Internet technology intended to keep information private while it is transported back and forth across the Internet. Furthermore, identifying data stored on the server is also encrypted or coded so that it cannot be recognized.
- The server/database exists behind a firewall –a device meant to keep hackers/crackers/viruses/etc. away from the server.
- The main database will be kept physically secure, meaning only authorized personnel will have access to the server/database.
- System Administrators employed by _____ (Continuum-designated HMIS Lead Agency) support the daily operation of the database. Administration of the database is governed by agreements that limit the use of personal information to providing administrative support and generating reports using aggregated information. These agreements further ensure the confidentiality of your personal information.

Benefits of HMIS and Agency Information Sharing

The information you provide us can play an important role in our ability and the ability of other Agencies to continue to provide the services that you and others in our community are requesting.

Allowing us to share your real name, even in the absence of other information, results in a more accurate count of individuals and the services they use. The security system is designed to create a code that will protect your identity on the System. A more accurate count is important because it can help us and other Agencies:

- Better demonstrate the need for services and the specific types of assistance needed in our area.
- Obtain more money and other resources to provide services.
- Plan and deliver quality services to you and your family.
- Assist the Agency to improve its work with families and individuals who are homeless.
- Keep required statistics for state and federal funders (such as HUD).

Risks in Sharing Information

While the HMIS was designed to promote better services for those who are homeless or might become homelessness, there are risks that may lead some individuals to choose to do one or more of the following:

- Allow only your name, gender, year of birth, and partial social security number (optional) to be shared with all participating Agencies. All other information, including your date of birth, full SS#, where you are being served and your particular situation, is kept confidential or shared with only select Agencies.
- Allow some statistical or demographic information to be shared with select other Agencies, but do not allow other more personal data such as health, mental health, drug/alcohol use history or domestic violence information to be shared.
- Close all information including identifying information from all sharing. Only the Agency that collects the information and System Administrative staff may see the information.

PRIVACY NOTICE AMENDMENTS: The policies covered under this Privacy Notice may be amended over time and those amendments may affect information obtained by the Agency before the date of the change. All amendments to the Privacy Notice must be consistent with the requirements of the Federal Standards that protect the privacy of clients and guide the HMIS implementation and operation.

Appendix J – Partner Agency Privacy Policy

Reasons for Policy:

- To protect the privacy of Agency clients
- To comply with applicable laws and regulations
- To ensure fair information practices as to:

a. Openness
b. Accountability
c. Collection limitations
d. Purpose and use limitations
e. Access and correction
f. Data Quality
g. Security

Statement of Policy:

- Compliance: Agency privacy practices will comply with all applicable laws governing the HMIS client privacy/confidentiality. Applicable standards include, but are not limited to the following:

a. Federal Register Vol. 69, No. 146 (HMIS FR 4848-N-02) - Federal statute governing HMIS information.
b. HIPAA - the Health Insurance Portability Act.
c. 42 CFR Part 2. - Federal statute governing drug and alcohol treatment.
d. CoC HMIS Policy and Procedures
e. NOTE: HIPAA statutes are more restrictive than the HMIS FR 4848-N-02 standards and in cases where both apply, HIPAA over-rides the HMIS FR 4848-N-02 standards. In cases where an Agency already has a confidentiality policy designed around the HIPAA standards, that policy can be modified to include the HMIS data collection or can be amended to create one set of standards for clients covered under HIPAA, and a second set of standards for those covered only under HMIS FR 4848-N-02. Agencies should indicate in their Privacy Notice which standards apply to their situation.

Use of Information: PII (personally identifiable information - information which can be used to identify a specific client) can be used only for the following purposes:

f. To provide or coordinate services to a client.
g. For functions related to payment or reimbursement for services.
h. To carry out administrative functions such as legal, audit, personnel, planning, oversight and management functions.
i. For creating de-personalized client identification for unduplicated counting.
j. Where disclosure is required by law.
k. To prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.
l. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
m. To report abuse, neglect, domestic violence, or any other crime of a predatory nature as required or allowed by law.
n. Contractual research where privacy conditions are met (including a written agreement).
o. To report criminal activity on Agency premises.

p. NOTE: HMIS FR 4848-N-02 standards list items a-d above as allowable reasons for disclosing PII but make provisions for additional uses to meet individual Agency obligations. In some cases, these uses (e-I above) have additional conditions, and HMIS FR 4848-N-02 4.1.3 should be consulted if any of these optional items are to be included in an Agency's policy. It also states, "except for first party access to information and required disclosures for oversight and compliance auditing, all uses and disclosures are permissive and not mandatory."

Collection and Notification: Information will be collected only by fair and lawful means with the knowledge or consent of the client.

q. PII will be collected only for the purposes listed above.
r. Clients will be made aware that personal information is being collected and recorded.
s. A written sign will be posted in locations where PII is collected. This written notice will read:
"We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless and/ or at-risk persons, and to better understand the needs of homeless and/ or at-risk persons. We only collect information that we consider to be appropriate."
"The collection and use of all personal information is guided by strict standards of confidentiality. Our Privacy Notice is posted. A copy of our Privacy Notice is available to all clients upon request."
t. This sign will be explained in cases where the client is unable to read and/or understand it.
u. NOTE: Under HMIS FR 4848-N-02, Agencies are permitted to require a client to express consent to collect PII verbally or in writing, however, this is optional and not a requirement of the statute.

Data Quality: PII data will be accurate, complete, timely, and relevant.

v. All PII collected will be relevant to the purposes for which it is to be used.
w. Data will be entered in a consistent manner by authorized End Users.
x. Data will be entered in as close to real-time data entry as possible.
y. Measures will be developed to monitor data for accuracy and completeness and for the correction of errors.
    i. The Agency runs reports and queries at least monthly to help identify incomplete or inaccurate information.
    ii. The Agency monitors the correction of incomplete or inaccurate information.
    iii. By the 20th of the following month, all monitoring reports will reflect corrected data.
z. Data quality is subject to routine audit by System Administrators who have administrative responsibilities for the database.

Privacy Notice, Purpose Specification, and Use Limitations: The purposes for collecting PII data, as well as its uses and disclosures, will be specified and limited.

aa. The purposes, uses, disclosures, policies, and practices relative to PII data will be outlined in an Agency Privacy Notice.
bb. The Agency Privacy Notice will comply with all applicable regulatory and contractual limitations.
cc. The Agency Privacy Notice will be made available to Agency clients, or their representative, upon request and explained/interpreted as needed.
dd. Reasonable accommodations will be made with regards to the Privacy Notice for persons with disabilities and non-English speaking clients as required by law.

ee. PII will be used and disclosed only as specified in the Privacy Notice, and only for the purposes specified therein.
ff. Uses and disclosures not specified in the Privacy Notice can be made only with the consent of the client.
gg. The Privacy Notice will be posted on the Agency website.
hh. The Privacy Notice will be reviewed and amended as needed.
ii. Amendments to, or revisions, of the Privacy Notice will address the retroactivity of any changes.
jj. Permanent documentation of all Privacy Notice amendments/revisions will be maintained.
kk. All access to and editing of PII data will be tracked by an automated audit trail and will be monitored for violations use/disclosure limitations.
NOTE: Items above are required by HMIS FR 4848-N-02, and/or AL-501 HMIS policy, but Agencies can restrict and limit the use of PII data further by requiring express client consent for various types of uses/disclosures, and/or by putting restriction or limits on various kinds of uses/disclosures.

Record Access and Correction: Provisions will be maintained for the access to, and corrections of, PII records.

ll. Clients will be allowed to review their HMIS record within 5 working days of a request to do so.
mm. During a client review of their record, an Agency staff person must be available to explain any entries the client does not understand.
nn. The client may request to have their record corrected so that information is up-to-date and accurate to ensure fairness in its use.
oo. When a client requests a correction, the request will be documented and the staff will make a corrective entry if the request is valid.
pp. A client may be denied access to their personal information for the following reasons:
  i. Information is compiled in reasonable anticipation of litigation or comparable proceedings;
  ii. Information about another individual other than the Agency staff would be disclosed; and/or
  iii. Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.
qq. A client may be denied access to their personal information in the case of repeated or harassing requests for access or correction. However, if denied, documentation will be provided regarding the request and reason for denial to the individual and be made a part of the client's record.
rr. A grievance process may be initiated if a client feels that their confidentiality rights have been violated, if access has been denied to their personal records, or if they have been put at personal risk, or harmed.
ss. Any client grievances relative to the HMIS will be processed and resolved according to Agency grievance policy.
tt. A copy of any client grievance relative to the HMIS data or other privacy/confidentiality issues and Agency response are forwarded to the CoC.

Accountability: Processes will be maintained to ensure that the privacy and confidentiality of client information is protected and staff is properly prepared and accountable to carry out Agency policies and procedure that govern the use of PII data.

uu. Grievances may be initiated through the Agency grievance process for considering questions or complaints regarding privacy and security policies and practices. All End Users of the HMIS must sign an End Users Agreement that specifies each staff person's obligations with regard to protecting the

privacy of PII and indicates that they have received a copy of the Agency's Privacy Notice and that they will comply with its guidelines.

vv. All System End Users must complete formal Privacy Training at www.learnhmis.org.

ww. A process will be maintained to document and verify completion of training requirements.

xx. A process will be maintained to monitor and audit compliance with basic privacy requirements including, but not limited to, auditing clients entered against signed HMIS Releases.

yy. A copy of any staff grievances initiated relative to privacy, confidentiality, or HMIS data will be forwarded to the CoC.

Sharing of Information: Client data may be shared with any Contributing HMIS Organization within the PromisSE implementation, unless entered by a provider with "closed" or partially "closed" visibility.

zz. Agency defaults within the System will be set to "open" unless otherwise requested by the Agency.

aaa. A completed PromisSE HMIS Client Release of Information (ROI) Form is needed before information may be shared electronically. If the client refuses to have their information shared, their information is still entered into the HMIS but "closed" so that only that Agency and the System Administrators have access.

i. PromisSE HMIS release informs the client about what is shared and with whom it is shared.

bbb. Clients will be informed about and understand the benefits, risks, and available alternatives to sharing their information prior to consenting to the ROI, and their decision to consent shall be voluntary.

ccc. Clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.

ddd. All Client ROI forms related to the HMIS will be placed in a file to be located on premises and will be made available to the CoC for periodic audits. ROI granted via verbal consent will be noted as "Verbal Consent in the ROI section of HMIS.

eee. PromisSE ROI forms will be retained for a period of 7 years, while they are active, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised. ROI forms can be retained electronically in HMIS and discarded immediately after.

fff. No confidential/restricted information received from the HMIS will be shared with any organization or individual without proper written consent by the client unless otherwise permitted by applicable regulations or laws.

ggg. Client information, including progress notes and psychotherapy notes, about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence entered by Agencies with "closed" visibility shall not be shared with other participating Agencies without the client's written, informed consent. Sharing of "closed" information must also be planned and documented through a fully executed agreement between Agencies, as documented through an inter-Agency "closed" data sharing agreement.

i. Sharing of "closed" information is not covered under the general PromisSE ROI.

ii. Once the client has provided written consent, and the involved PromisSE Member Agencies have executed a sharing of "closed" information agreement for an individual client or household, a copy of those documents must be sent to the local System Administrator (SA), along with a ticket outlining the information to be shared and the receiving Agency. The SA will then "open" that information only to the Receiving Agency.

hhh. If a client has previously given permission to share "closed" information with multiple Agencies and then chooses to revoke that permission with regard to one or more of these Agencies, the

affected Agency/Agencies will be contacted accordingly, and those portions of the record, impacted by the revocation, will be "closed" from further sharing.

iii. All client ROI forms will include an expiration date, and once a Client ROI expires, the Agency must contact the client in order to execute a new ROI. If the Agency is not able to contact the client, or if the client refuses to sign a new ROI, the Agency must notify the local SA within 48 hours so that the client record can be "closed".

System Security: The System security provisions will apply to all Systems where PII is stored: Agency networks, desktops, laptops, minicomputers, mainframes, and servers.

jjj. Password Access:

i. Only individuals who have completed Privacy and basic System training may be given access to the System through End User IDs and Passwords.
ii. Temporary/default passwords will be changed on first use.
iii. Access to PII requires an End Username and password at least 8 characters long and using at least two numbers and/or special characters.
iv. End User Name and password may not be stored or displayed in any publicly accessible location
v. End Users must not be able to log onto more than one workstation or location at a time.
vi. Individuals with End User IDs and Passwords will not give or share assigned End User ID and Passwords to access the System with any other organization, governmental entity, business, or individual.

kkk. Virus Protection and Firewalls:

i. Commercial virus protection software will be maintained to protect the System from a virus attack.
ii. Virus protection will include automated scanning of files as they are accessed by End Users.
iii. Virus Definitions will be updated regularly.
iv. All workstations will be protected by a workstation or server firewall.

lll. Physical access to computers and other devices where System data is stored and/or accessible.

i. Computers stationed in public places must be secured when workstations are not in use and staff are not present.
ii. After a short period of time, a password protected screen saver will be activated during the time that the System is temporarily not in use.
iii. Staff must log out of the System when leaving the workstation.

mmm. Stored Data Security and Disposal:

i. All HMIS data downloaded onto a data storage medium must be maintained and stored in a secure location.
ii. Data downloaded for purposes of statistical analysis will exclude PII whenever possible.
iii. HMIS data downloaded onto a data storage medium must be disposed of by reformatting as opposed to erasing or deleting.
iv. A data storage medium will be reformatted a second time before the medium is reused or disposed of.

nnn. Hard Copy Security:

i. i) Any paper or other hard copy containing PII that is either generated by or for the HMIS, including, but not limited to reports, data entry forms and signed consent forms will be secured.
ii. ii) Agency staff will supervise at all times a hard copy with identifying information generated by or for the HMIS when the hard copy is in a public area. If the staff leaves the area, the hard copy must be secured in areas not accessible by the public.

iii. iii) All written information pertaining to the End Username and password must not be stored or displayed in any publicly accessible location.

ooo. Remote Access to the HMIS:

i. All HMIS End Users are prohibited from using a computer that is available to the public or from accessing the System from a public location through an internet connection that is not secured. End Users are not allowed to use Internet Cafes, Libraries, Airport Wi-Fi or other non-secure internet connections.

ii. Staff must use remote laptops or desktops that meet the same security requirements as those office HMIS workstations.

iii. Downloads from the HMIS may not include client PII.

iv. Remote System access should be limited to situations in which it is imperative that the End User access the System outside of the normal office setting.

v. Remote System access should reflect the requirements of job responsibilities.
NOTE: Various important aspects of System security are the contracted responsibility of WellSky and are therefore not covered by the Agency policy. These involve procedures and protections that take place at the site of the central server and include data backup, disaster recovery, data encryption, binary storage requirements, physical storage security, public access controls, location authentication etc.

Procedures:

NOTE: Procedures and roles relative to this policy should be defined in a procedure section. These will vary significantly from Agency to Agency but may include the following.

- Participating Agencies may integrate the System into the Agency's existing Privacy Notice. If the Agency does not have an existing Privacy Notice, Agencies may adopt the HMIS Privacy Notice Example in this manual or may use it as a model. The Privacy Notice must reflect the Agency's privacy policy.
- Board approval of your Confidentiality/Privacy Policy is required. Copies of the Participation Agreement, the End User Agreement, Agency Administrator Agreement, Security Officer Agreement, and Inter-Agency "Closed" Data Sharing Agreement may be attachments to your Policy.

Appendix K - HUD Data Elements

https://www.hudexchange.info/resource/3824/hmis-data-dictionary/

Project Descriptor Data Elements	Universal Data Elements	Program Specific Data Elements
2.01 Organization Information 2.02 Project Information 2.03 Continuum of Care Information 2.06 Funding Sources 2.07 Bed and Unit Inventory Information	3.01 Name 3.02 Social Security Number 3.03 Date of Birth 3.04 Race 3.05 Ethnicity 3.06 Gender 3.07 Veteran Status 3.08 Disabling Condition 3.10 Project Start Date 3.11 Project Exit Date 3.12 Destination 3.15 Relationship to Head of Household 3.16 Client Location 3.20 Housing Move In date 3.917 Prior Living Situation	4.02 Income and Sources 4.03 Non-cash Benefits 4.04 Health Insurance 4.05 Physical Disability 4.06 Developmental Disability 4.07 Chronic Health Condition 4.08 HIV/AIDS 4.09 Mental Health Problem 4.10 Substance Abuse 4.11 Domestic Violence 4.12 Current Living Situation 4.13 Date of Engagement 4.14 Bed-Night Date 4.19 Coordinated Entry Assessment 4.20 Coordinated Entry Event

Appendix L – PromisSE and CoC Participation Agreement

CoC Name: _____

This agreement is entered into on _____(mm/dd/yy) between One Roof, designated as PromisSE's HMIS Vendor Contract-Holding Agency, and the above-stated Continuum designated Lead HMIS Agency hereafter known as "HMIS Lead," regarding access and use of the Program Management Information System, hereafter known as "PromisSE."

I. Introduction

The purpose of HMIS is to record and store client-level information about the numbers, characteristics, and needs of persons who use homeless housing and supportive services, to produce an unduplicated count of homeless persons for each Continuum of Care in addition to the implementation; to understand the extent and nature of homelessness locally, regionally and nationally; and to understand patterns of service usage and measure the effectiveness of programs and systems of care.

PromisSE's goals are to:

- Improve coordinated care for and services to homeless and at-risk persons in the PromisSE service area,
- Provide a user-friendly and high quality automated records system that expedites client intake procedures, improves referral accuracy, increases case management and administrative tools, creates a tool to follow demographic trends and service utilization patterns of families and individuals either currently experiencing or at risk of experiencing homelessness, and supports the collection of quality information that can be used for program improvement and service-planning.
- Meet the reporting requirements of the U.S. Department of Housing and Urban Development (HUD) and other funders as needed.

In compliance with all state and federal requirements regarding client/consumer confidentiality and data security, the PromisSE is designed to collect and deliver timely, credible, quality data about services and homeless persons or persons at risk of being homeless.

II. One Roof Responsibilities

A. One Roof, as PromisSE's HMIS Vendor Contract-holding Agency, will establish and manage the single shared Implementation contract with Wellsky, the HMIS software provider.
B. One Roof, as PromisSE's HMIS Vendor Contract-holding Agency, will offer initial training for the HMIS Coordinator of each local Continuum-designated HMIS Lead Agency, regarding the use of the HMIS compliant software used by PromisSE, so that the HMIS Coordinator will take responsibility for training end users within their Continuum. One Roof will provide notification of any Regional and other periodic training offered to Continuum-designated HMIS Lead Agencies electronically at least two weeks in advance, barring extenuating circumstances.
C. One Roof, as PromisSE's HMIS Vendor Contract-holding Agency, will provide PromisSE software support and technical assistance (i.e., general troubleshooting and assistance with standard report generation) to the HMIS Coordinator of each local Continuum-designated HMIS Lead Agency. Access to this basic technical assistance will be available during normal business hours Monday through Friday (with the exclusion of holidays) and limited availability outside of normal business hours.

D. One Roof will establish a fee structure for financing the software utilized by PromisSE, including an administrative fee. The current fee structure is as follows:
   a) The cost of all WellSky Community Services modules will be divided evenly among all Continuum-designated HMIS Lead Agencies.
   b) The cost of software licenses, reporting licenses, and associated fees allocated to each Continuum-designated HMIS Lead Agency will be the responsibility of that agency, and will be added to the cost of the WellSky Community Services modules.
   c) One Roof will charge a 3% fee for all HMIS software related billing to each Continuum-designated HMIS Lead Agency.
E. One Roof will invoice participants in a timely manner.
F. One Roof will order user licenses at the request of the HMIS Coordinator of each Continuum-designated HMIS Lead Agency.

III. Continuum-designated HMIS Lead Agency's Responsibilities

A. The Continuum-designated HMIS Lead Agency agrees to maintain documentation of their annual designation as HMIS Lead Agency by their local Continuum of Care as established by HUD and notify One Roof, as PromisSE's HMIS Vendor Contract-holding Agency, within 48 hours of any changes in this designation.
B. The Continuum-designated HMIS Lead Agency agrees to participate as a member of the Program Management Information System of the Southeast's Steering Committee, the governing entity of PromisSE.
C. The Continuum-designated HMIS Lead Agency agrees to designate system-level access based on job requirements for their CoC's users and provide appropriate training for each access level.
   a. All users assigned "System Operator", "System Admin I", or "System Admin II" access are required to:
      i. Complete, at a minimum, basic PromisSE system training and system administrator training.
      ii. Have job duties that require a majority of the following permissions within the PromisSE system:
         1. View Inactive Clients, Call Records, and Providers
         2. Delete any Client Record, Call Record, Household, or Provider
         3. Create, Delete, and Manage ALL users in the PromisSE system
         4. Create, Delete, and Manage ALL providers in the PromisSE system
         5. Add, Edit, and Delete EDA groups (system access for other users)
         6. View and Modify PromisSE System Preferences and Settings
         7. Bypass Security and ROIs to Access System Information
         8. Purchase, Allocate, and Assign Licenses
         9. Add, Edit, and Delete Resource, Reporting, EDA, and Visibility Groups
         10. Generate Audit, XML, and System-Wide Reports
         11. Delete Subordinate and Parent Provider Reportwriter Reports
         12. Access and Change Settings to Create, Read, Update, and Delete Assessment Information System-Wide
         13. View and Modify Picklists
      iii. Have PromisSE system access limited only to necessary providers (in users' EDA Group Settings)
D. The Continuum-designated HMIS Lead Agency agrees to support the HMIS Coordinator to ensure the Continuum Agencies who participate in PromisSE follow the basic standards as described in the PromisSE Policies and Procedures Manual and any Federal standards that supersede the Policies and Procedures.
E. The Continuum-designated HMIS Lead Agency agrees to pay One Roof in full and on time for use of the PromisSE software and services associated with the HMIS software.
F. The Continuum-designated HMIS Lead Agency agrees to make end user license and reporting license requests through One Roof.
G. The Continuum-designated HMIS Lead Agency agrees to make WellSky requests through One Roof.

H. The Continuum-designated HMIS Lead Agency agrees that agencies serving clients in more than one CoC must participate in each CoC where clients are located. Participation necessitates that the agency must adhere to each CoC's procedures, policies, participation requirements, etc.

IV. Custody of Data

A. The Continuum-designated HMIS Lead Agency and One Roof understand that the Continuum-designated HMIS Lead Agency, agencies, and One Roof as administrators, are custodians – NOT owners - of the data on behalf of the PromisSE participating agencies, or Contributing HMIS Organizations (CHOs).
B. In the event that PromisSE ceases to exist, Continuums will be notified and provided reasonable time to access and save client data on those served by their Contributing HMIS Organizations (CHOs), as well as statistical and frequency data from the entire system. Thereafter, the information collected by the centralized server will be purged or appropriately stored.
C. In the event that One Roof ceases to exist, the custodianship of the data within PromisSE will be transferred to the agency designated as the new PromisSE HMIS Vendor contract-holding Agency by the PromisSE Steering Committee for continuing administration, and all PromisSE-participating Continuums will be informed in a timely manner.
D. In the event that the Continuum-designated HMIS Lead Agency ceases to exist, the custodianship of the data within PromisSE will be transferred to either the local Continuum of Care or the organization designated by the local Continuum of Care as the new HMIS Lead Agency for continuing administration.

V. Hold Harmless

A. One Roof makes no warranties, expressed or implied. The Continuum-designated HMIS Lead Agency, at all times, will indemnify and hold One Roof harmless from any damages, liabilities, claims, and expenses that may be claimed against the HMIS Lead; or for injuries or damages to the Continuum-designated HMIS Lead Agency or another party arising from participation in the PromisSE; or arising from any acts, omissions, neglect, or fault of the Continuum-designated HMIS Lead Agency or its agents, employees, licensees, or clients; or arising from the Continuum-designated HMIS Lead Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Continuum-designated HMIS Lead Agency will also hold One Roof harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, misdeliveries, or service interruption caused by the chosen software vendor for PromisSE by the Continuum-designated HMIS Lead Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, and/or technological difficulties. One Roof shall not be liable to the Continuum-designated HMIS Lead Agency for damages, losses, or injuries to the Continuum-designated HMIS Lead Agency or another party other than if such is the result of gross negligence or willful misconduct of One Roof. One Roof agrees to hold the Continuum-designated HMIS Lead Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of One Roof.
B. It is the responsibility of the Continuum-designated HMIS Lead Agency to ensure that each participating Agency within the Continuum maintains compliance with all PromisSE Policies and Procedures in addition to any required by Federal standards.

VI. Terms and Conditions

A. The Continuum-designated HMIS Lead Agency shall not transfer or assign any rights or obligations under the Participation Agreement without the written consent of One Roof.
B. This agreement shall remain in force until revoked in writing by either party, with 30 days advance written notice. The exception to this term occurs if allegations or actual incidences arise regarding possible or actual breaches of this agreement. Should such situations arise, the One Roof PromisSE System

Administrator may immediately suspend access to PromisSE until the allegations are resolved in order to protect the integrity of the System.

C. This agreement may be modified or amended by written agreement executed by both parties with 30 days advance written notice.

IN WITNESS WHEREOF, the parties have entered into this Agreement:

One Roof Telephone Number	HMIS Lead Agency Name
One Roof Representative Printed Name	HMIS Lead Agency Address
One Roof Representative Title	HMIS Lead Agency City, State ZIP
One Roof Representative Signature	HMIS Lead Agency Telephone Number
Date (mm/dd/yy)	HMIS Lead Agency Rep. Printed Name
	HMIS Lead Representative Title
	HMIS Lead Representative Signature
	Date (mm/dd/yy)

Assurance

_____(Name of Continuum-Designated HMIS Lead) assures that the following fully executed documents will be on file and available for review.

- Documentation of the designation of the HMIS Lead Agency's by the local Continuum of Care.
- The Continuum-designated HMIS Lead Agency's Board Approved Confidentiality Policy.
- The Continuum-designated HMIS Lead Agency's Official Privacy Notice for PromisSE clients.
- Documentation authenticating completion of required training for all PromisSE System Users in the Continuum.
- A fully executed User Agreement for all PromisSE End Users in the Continuum.
- A fully executed participation agreement for all PromisSE Contributing HMIS Organizations (CHOs)
- A current PromisSE Policies and Procedures Manual.
- The Continuum-designated HMIS Lead Agency's Conflict of Interest Policy.
- The Continuum-designated HMIS Lead Agency's Whistleblower Policy.

By: _____

Title: _____

Signature: _____

Date: _____

Appendix M – CoC System Administrator Agreement

Name: _____

CoC Name: _____

All HMIS participating CoCs must designate and staff one HMIS System Administrator. System Administrator requirements and responsibilities include, but are not limited to, the following:

- Has completed, at a minimum, basic PromisSE system training and System Administrator training.
- Ensure that all Agency users have signed End User Agreement documents on file.
- Ensure that all Users complete an annual End User Certification Test, which includes Privacy and Security training. This training can be accessed through the PromisSE Learning Management System – www.learnhmis.org.
- Ensure that all Users have completed workflow training and related updates, and have documentation of training.
- Ensure that the CoC complies with the CoC Data Security standards.
- Ensure that the CoC complies with the PromisSE HMIS Policies and Procedures.
- Ensure that all Users have submitted a criminal background check.

The original System Administrator Agreement shall be kept on file at the CoC. Forms completed by individuals no longer employed by the CoC shall be kept on file for a minimum of five years.

One Roof makes no warranties, expressed or implied. The CoC, at all times, will indemnify and hold the One Roof harmless from any damages, liabilities, claims, and expenses that may be claimed against the CoC; or for injuries or damages to the CoC or another party arising from participation in ***PromisSE***; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the CoC's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This CoC will also hold One Roof harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, misdeliveries, or service interruption caused by WellSky, by the CoC's or other member agency's negligence or errors or omissions, as well as natural disasters, and/or technological difficulties. One Roof shall not be liable to the CoC for damages, losses, or injuries to the CoC or another party other than if such is the result of gross negligence or willful misconduct of One Roof. One Roof agrees to hold the CoC harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of One Roof.

This agreement is in effect for a period of one (1) year after the date of signing. Failure to comply with the provisions of this System Administrator Agreement is grounds for immediate termination of access. Your signature below indicates your agreement to comply with this System Administrator Agreement.

Employee Printed Name	CoC Official Printed Name
Employee Signature	CoC Official Signature
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix N – CoC System Security Officer Agreement

Name: _____

CoC Name: _____

All HMIS participating CoCs must designate and staff one CoC HMIS Security Officer. Security Officer requirements and responsibilities include, but are not limited to, the following:

- Ensures that all staff using the System complete annual privacy and security training. Training must be provided by the CoC designated trainers and be based on the CoC Privacy and Security standards. This training can be accessed through the PromisSE Learning Management System – www.learnhmis.org.
- Conducts an annual security review of the CoC that includes reviewing compliance with the Privacy and Security sections of the PromisSE Homeless Management Information System (HMIS) Operating Policy and Procedure. The CoC must document the findings of the review on the Privacy and Security Checklist and submit the findings to the Lead HMIS System Administrator no later than December 31st of each year.
- Notifies the local Lead Agency System Administrator when a System Administrator leaves the organization or revision of the user's access level is needed because of a change in job responsibilities. The notification must be made within 48 hours of the change.
- Reports any security or privacy incidents to the local Lead HMIS System Administrator for the CoC Jurisdiction. The System Administrator investigates the incident including running applicable audit reports. If the System Administrator and Security Officer determine that a breach has occurred and/or the staff involved violated privacy or security guidelines, the System Administrator will report to the chair of the CoC. A Corrective Action Plan will be implemented. Components of the Plan must include at minimum supervision and retraining. It may also include removal of HMIS license, client notification if a breach has occurred, and any appropriate legal action.

The original Security Officer Agreement shall be kept on file at the CoC. Forms completed by individuals no longer employed by the Agency shall be kept on file for a minimum of five years.

One Roof makes no warranties, expressed or implied. The CoC, at all times, will indemnify and hold the One Roof harmless from any damages, liabilities, claims, and expenses that may be claimed against the CoC; or for injuries or damages to the CoC or another party arising from participation in ***PromisSE***; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the CoC's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This CoC will also hold One Roof harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, misdeliveries, or service interruption caused by WellSky, by the CoC's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. One Roof shall not be liable to the CoC for damages, losses, or injuries to the CoC or another party other than if such is the result of gross negligence or willful misconduct of One Roof. One Roof agrees to hold the CoC harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of One Roof.

This agreement is in effect for a period of one (1) year after the date of signing. Failure to comply with the provisions of this System Security Officer Agreement is grounds for immediate termination of access. Your signature below indicates your agreement to comply with this System Security Officer Agreement.

Employee Printed Name	CoC Official Printed Name
Employee Signature	CoC Official Signature
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix O – Sample CoC Agency Audit Checklist

____ Has completed annual Privacy and Security Checklist.

____ All End Users have executed End User Agreement.

____ HUD Public Notice is posted and visible to clients.

____ Has HMIS Privacy Notice and is available to clients.

____ Has HMIS Privacy Policy which details the procedures of the Privacy Notice.

____ HMIS Privacy Policy includes a remote access plan.

____ Hard copy data is secure.

____ HMIS workstations are password protected.

____ HMIS workstations are locked when not in use and have a locking capability.

____ All clients are entered into the System within 24 hours, if not immediately.

____ All End Users have access to a copy of the HUD Universal Data Elements and Program Specific Elements.

____ Staff members have been trained on the HUD definition of homelessness and understand the priority of homelessness documentation.

____ Agency has a process to ensure clients name is spelled properly and DOB is accurate.

____ End Users update client information as required for program type through Interim Reviews and Follow-Ups.

____ Agency Admins or assigned staff are running monthly data quality reports and taking corrective action in accordance with the requirements of the CoC Policies and Procedures.

____ All End Users have had at least general System training.

Appendix P – HMIS Data Sharing, Security & Usage Agreement

Continuum of Care

Program Management Information System of the Southeast

Community Partnership Agreement Between

_____**(The CoC)** and

_____(Name of Agency or Individual)

This Data Use Agreement ("Agreement") is entered into on _____(mm/dd/yy) by and between:

_____ _____

Disclosing Party (CoC or Agency Name) Receiving Party (Recieving Organization Name

_____

Contact Person (Name, Title, Email, Phone)

1. Purpose
The purpose of this Agreement is to establish the conditions under which HMIS client-level data may be shared by the Disclosing Party with the Receiving Party, in accordance with applicable laws and the PromisSE HMIS Policies and Procedures.

2. Data Description
The data to be shared includes the following fields: [Specify fields or attach data schema]. No Social Security Numbers or full names will be shared unless explicitly authorized by client ROI.

3. Data Use Restrictions
The Receiving Party agrees to use the data solely for the following purposes:

_____

[Describe Scope of Data Use Here]

The data shall not be used for any other purpose without prior written consent from the Disclosing Party.

4. Data Protection and Confidentiality
The Receiving Party agrees to:

- Store data in a secure, encrypted environment.
- Limit access to authorized personnel only.
- Not re-disclose the data to any third party.
- Report any data breach to the Disclosing Party within 48 hours.

5. Client Consent
The Disclosing Party confirms that clients whose data is being shared have provided informed consent through a signed or verbal Release of Information (ROI), in accordance with PromisSE privacy standards.

Appendix P – HMIS Data Sharing, Security & Usage Agreement

6. Data Retention and Destruction
The Receiving Party agrees to destroy all client-level data by _____(mm/dd/yyyy) and to provide written confirmation of destruction to the Disclosing Party.

7. Term and Termination
This Agreement shall remain in effect until _____(mm/dd/yyyy) or until terminated in writing by either party. Upon termination, all shared data must be deleted as per Section 6.

8. Signatures
IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

Disclosing Party
Name: _____

Title: _____

Signature: _____

Date: _____

Receiving Party
Name: _____

Title: _____

Signature: _____

Date: _____

Appendix Q – Sample HMIS Criminal Background Check Certification

The Program Management Information System of the Southeast ("PromisSE") contains a wide range of personal and private information on individuals, and all such information must be treated carefully, confidentially, and professionally by those who have the ability to access it. As such, an Agency's employees, volunteers, and any persons requesting access to the PromisSE must comply with the PromisSE License Agreement & Statement of Confidentiality (Appendix F) and the requirements set forth in the PromisSE Policies and Procedures, including the successful clearance of a national criminal background check, which must be certified by the Agency Administrator and Executive Director of the agency. **This form must be submitted to the Continuum-designated HMIS Lead Agency before access is granted in HMIS.**

It is noted the HMIS Lead Agency may request an updated criminal background check on any end user suspected of violating any standard or requirement outlined in the PromisSE Policies and Procedures and the PromisSE License Agreement & Statement of Confidentiality (Appendix F).

_____ _____

Prospective HMIS End User Name Today's Date

I affirm the Prospective HMIS End User referenced above has successfully cleared a national criminal background completed check that was within 30 days of the PromisSE Training request.

_____ _____

Training Request Date Background Check Complete Date

I affirm the background check for the Prospective HMIS End User referenced above successfully cleared the following parameters, as set by the PromisSE Implementation. (Initial each parameter to signify certification).

_____ Prospective HMIS End User **DOES HAVE / DOES NOT HAVE** (circle appropriate answer) any prior convictions of either embezzlement or identity theft.

_____ Prospective HMIS End User **HAS/ HAS NOT** (circle appropriate answer) been convicted of domestic violence, fraud offense, or any other crime of a predatory nature **within the past seven (7) years** of today's date.

Note: If a Prospective End User with a history of any of these offenses requests access to the system, a written statement of explanation must be referred to your local CoC Lead Agency.

_____

Agency/ Program Name

_____ _____

Agency Administrator Name Executive Director Name

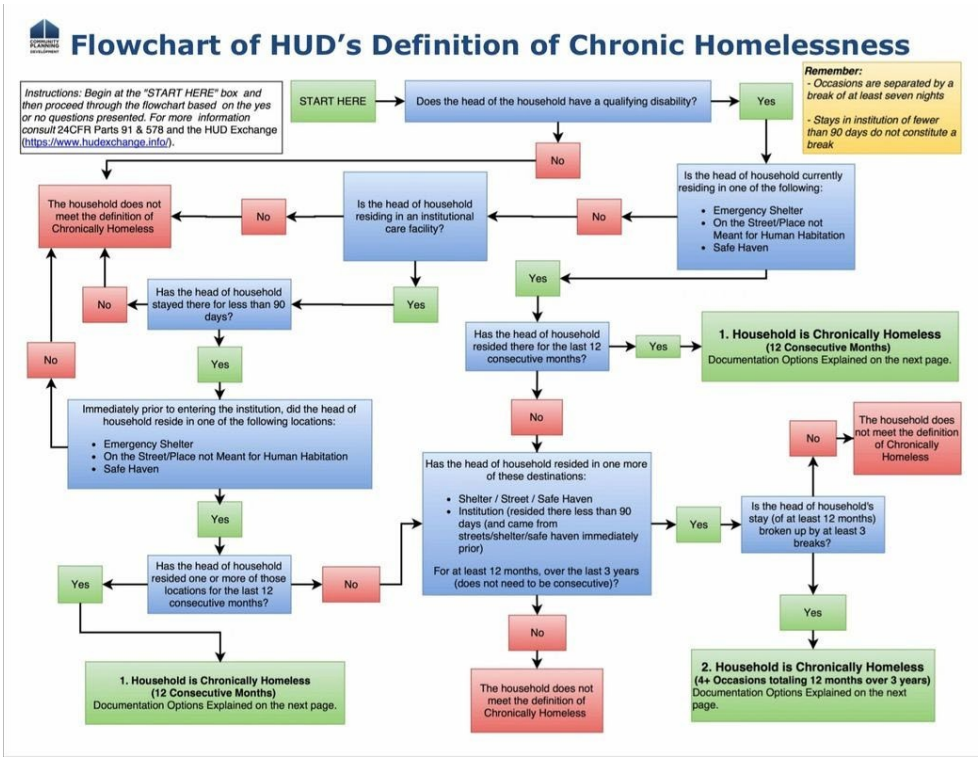
_____ _____

Agency Administrator Signature Executive Director Signature

_____ _____

Today's Date Today's Date

Appendix R – Flowchart of HUD's Definition of Chronic Homelessness



Documentation Standards for Chronic Homelessness

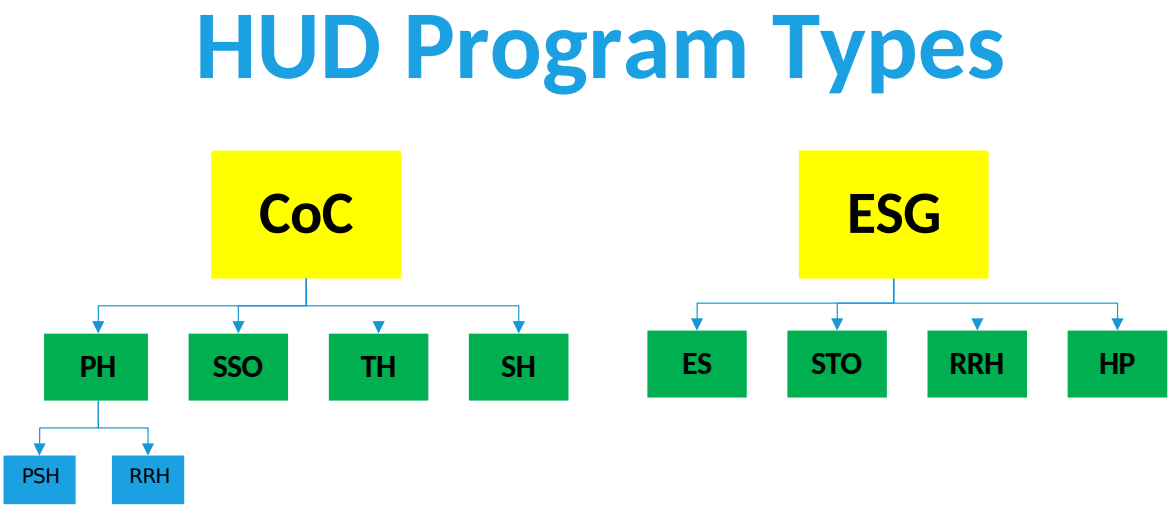
Instructions: *Based on your navigation of the flowchart on the previous page, locate the appropriate numbered situation on this page and follow the documentation standards noted. This tool summarizes the criteria for the new Chronically Homeless Definition. To review the exact language, please refer to 24 CFR Parts 91 & 578 and the HUD Exchange (https://www.hudexchange.info/homelessness-assistance/resources-for-chronic-homelessness/)*

Situation	Documentation of Homelessness	Documentation of Disability
1. Household is Chronically Homeless (12 Consecutive Months)	☐ HMIS record or record from a comparable database; or ☐ Written observation by an outreach worker of the conditions where the individual was living; or ☐ Written referral by another housing or service provider; or ☐ Where the evidence above is unavailable, there must be a certification by the individual seeking assistance, accompanied by the intake worker's documentation of the living situation and the steps taken to obtain the evidence listed above. If the head of household is currently staying in an institution where they have been for less than 90 days (and were in a shelter/street/safe haven immediately prior) their Institutional Stay can be documented by: ☐ Discharge paperwork or written/oral referral from a social worker or appropriate official of the institutional facility, with start/end dates of client's residence, or ☐ Where the evidence above is unavailable, there must be a certification by the individual seeking assistance, accompanied by the intake worker's documentation of the living situation and the steps taken to obtain the evidence listed above.	Documentation of the head of household's disability, including: ☐ Written verification of the disability from a licensed professional; ☐ Written verification from the Social Security Administration; ☐ The receipt of a disability check; or ☐ Intake staff-recorded observation of disability that, no later than 45 days from the application for assistance, accompanied by supporting evidence.
2. Household is Chronically Homeless (4+ Occasions totaling 12 months over 3 years)* **May include institution stays of <90 days*	☐ HMIS record or record from a comparable database; or ☐ Written observation by an outreach worker of the conditions where the individual was living; or ☐ Written referral by another housing or service provider; or ☐ Discharge paperwork or written/oral referral from a social worker or appropriate official of the institutional facility, with start/end dates of client's residence (for institutional stays of less than 90 days) ☐ Where the evidence above is unavailable, there must be a certification by the individual seeking assistance, accompanied by the intake worker's documentation of the living situation and the steps taken to obtain the evidence listed above. * *Each separate occasion MUST be documented (minimum of 3 breaks). 100% of the breaks can be documented by self- report.*	Documentation of the head of household's disability, including: ☐ Written verification of the disability from a licensed professional; ☐ Written verification from the Social Security Administration; ☐ The receipt of a disability check; or ☐ Intake staff-recorded observation of disability that, no later than 45 days from the application for assistance, accompanied by supporting evidence.

Important Notes:

- *Each individual occasion needs to be fully documented.*
- *Breaks can be documented by self-report.*
- *For each Project:*
  - *100% of households served can use self-certification for 3 months of their 12 months,*
  - *75% of households served need to use 3rd Party documentation for 9 months of their 12 months, and*
  - *25% of households served can use self-certification as documentation for any and all months.*

Appendix S – HUD Program Types



Term	Acronym (if used)	Brief Definition or Link
Permanent Housing	PH	Housing that may be supported by a voucher but does not have services attached to the housing.
Supportive Services Only	SSO/SO	A program that provides services with no residential component. These programs often provide case management and other forms of support and meet with clients in an office, at the household's home, or in a shelter. The only HUD-funded SSO is Coordinated Assessment.
Transitional Housing	TH	Transitional environments that have a planned length of stay of not more than 2 years and provide supportive services.
Safe Haven	SH	A program that provides low-demand shelter for hard-to-serve persons with severe disabilities. The clients have often failed in other sheltering environments.
Permanent Supportive Housing	PSH	Permanent Housing for the formerly homeless with services attached to persons served under this program.
Rapid Rehousing	RRH	A program that rapidly rehouses those that are identified as Literally Homeless.
Emergency Shelter	ES	Overnight shelters or shelters with a planned length of stay of fewer than 3 months.
Street Outreach	STO	A program that serves homeless persons who are living on the street or other places not meant for habitation.
Homeless Prevention	HP	A program that helps persons at imminent risk of losing housing, to retain their housing.
CoC Program, formerly known as Shelter Plus Care	S+C (formerly)	A voucher system that provides Permanent Supportive Housing to disabled persons throughout the catchment area and reports to the System.