



AL-501 Homeless Coalition of the Alabama Gulf Coast Continuum of Care

**Homeless Management Information System
Operating Policies and Procedures**

Table of Contents

AL-501 CoC HMIS Operating Policies & Procedures.....	1-17
Appendix A AL-501 CoC Participation Agreement.....	18-24
Appendix B AL-501 CoC Agency Administrator Agreement.....	25
Appendix C AL-501 CoC Security Officer Agreement.....	26-27
Appendix D AL-501 CoC Policies & Procedures Compliance Checklist.....	28
Appendix E AL-501 CoC Privacy and Security Checklist.....	29-33
Appendix F AL-501 CoC End User License Agreement & Statement of Confidentiality....	34-36
Appendix G AL-501 CoC Client Release of Information and Sharing Plan.....	37-39
Appendix H AL-501 CoC Public Notice.....	40
Appendix I AL-501 CoC Privacy Notice to Clients.....	41-47
Appendix J AL-501 CoC Privacy Policy.....	48-53
Appendix K Universal Data Elements.....	54
Appendix L PromisSE Participation Agreement.....	55-58
Appendix M AL-501 CoC System Administrator Agreement.....	59
Appendix N AL-501 CoC System Security Officer Agreement.....	60-61
Appendix O AL-501 CoC Agency Audit Checklist.....	62
Appendix P AL-501 CoC HMIS Contract Agreement Policy.....	63
Appendix Q AL-501 CoC Outreach Privacy Notice.....	64
Appendix R AL-501 CoC Outreach Consent Certification.....	65
Appendix S AL-501 CoC HMIS Criminal Background Check Certification.....	66
Appendix T AL-501 CoC HMIS Privacy Statement.....	67-68
Appendix U HUD Homeless Definition Crosswalk.....	69

AL-501 Homeless Coalition of the Alabama Gulf Coast Continuum of Care (AL-501 CoC) Homeless Management Information System (HMIS) Operating Policies and Procedures

The HMIS Operating Policies and Procedures were developed in accordance with the proposed rule for HMIS Requirements (FR-5475-P-01) under the HEARTH Act, requiring the adoption of policies and procedures for the operation of a Homeless Management Information System (“HMIS” or “System”), which is an information technology system and database that HUD recipients and subrecipients are required to use for homeless assistance programs authorized by the McKinney-Vento Act. The HMIS is used collect client-level data and data on the provision of housing and services to homeless individuals, families, and persons at risk of homelessness. Specifically, an HMIS can be used to produce an unduplicated count of homeless persons for each Continuum of Care (“CoC”); describe the extent and nature of homelessness locally, regionally and nationally; to understand and identify patterns of service use; and to measure the effectiveness of programs and systems of care. **The following operating policies and procedures apply to all agencies or organizations within the AL-501 CoC using the HMIS, which is also referred to as the Program Information System of the Southeast (“PromisSE”).**

Key Terms & Acronyms

Term	Acronym (if used)	Brief Definition
Agency		An organization participating in the HMIS (including its employees, volunteers, affiliates, contractors, and associates), oftentimes referred to as a Covered Homeless Organization (CHO) or Participating Agency.
Agency Administrator		Agency staff member responsible for ensuring the Agency is in compliance with the HMIS Operating Policies and Procedures.
Agency Official		Agency staff member authorized to contractually obligate the Agency to the HMIS Participation Agreement, Operating Policies & Procedures, Contract Agreement, and all other core documents.
Agreement and Authorization		Agreement in which the CoC Board of Directors authorizes the Continuum Designated HMIS Lead Agency to operate the CoC’s HMIS on the CoC’s behalf.
Annual Assessment		An Annual Assessment is required for all clients with an enrollment into a project for 365 days, and has to be completed no more than 30 days before or after the anniversary date of the client’s entry into the project. (U.S. Department of Housing and Urban Development, 2016, p. 14) ¹
Balance of State Continuums of Care	BoS	Many states have large areas (often rural in nature) not covered by regional, county or city CoCs. These areas, often including both highly functional local continuums and weak local organizations, join together to form one combined CoC for the geographic area. (U.S. Department of Housing and Urban Development, 2009, p. 8) ²
Basic Information		Basic Information consists of a client’s name, date of birth, social security number, program enrollments, case managers, military background (veteran status), and photo.
Bowman Systems, LLC		Vendor producing the ServicePoint HMIS software used by the HMIS Regional Implementation.
Continuum Designated HMIS Lead Agency		The entity designated by the CoC in accordance with the HMIS Proposed Rule1 (24 CFR Part 580) to operate the CoC’s HMIS on the CoC’s behalf. (Department of Housing and Urban Development, 2012, p. 45444) ³ Duties include developing written policies and procedures for all Covered Homeless Organizations (CHOs), executing an HMIS participation agreement with each CHO, serving as the applicant to HUD for any HMIS grants that will cover the CoC geographic area, and

¹ U.S Department of Housing and Urban Development (2016). *2014 HMIS Data Standards Manual* (Version 5.1) Washington, DC: HUD and Federal Partners.

² U.S. Department of Housing and Urban Development (2009). *Continuum of Care 101*. Washington, DC: Office of Community Planning and Development.

³ Department of Housing and Urban Development (2012). *Federal Register: (HMIS); Data and Technical Standards Final Notice; Notice*. (Vol. 77, No. 147) Washington, DC: United States Government Printing Office

		monitoring compliance by all CHOs of the CoC. The Continuum Designated HMIS Lead Agency referenced in this document is responsible for operating the local HMIS database.
Continuum of Care	CoC	Continuum of Care, or Continuum, is the group organized to carry out the responsibilities required under the CoC Program Interim Rule (24 CFR Part 578). The CoC is comprised of representatives of organizations, including nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, and law enforcement, and organizations that serve homeless and formerly homeless persons to the extent that these groups are represented within the geographic area and are available to participate.
Coordinated Entry (Coordinated Intake or Assessment)		Centralized or coordinated assessment system means a centralized or coordinated process designed to coordinate program participant intake assessment and provision of referrals. A centralized or coordinated assessment system covers the geographic area, is easily accessed by individuals and families seeking housing or services, is well advertised, and includes a comprehensive and standardized assessment tool. (24 CFR § 578.3) ⁴
Corrective Action Plan	CAP	The plan implemented in the event a privacy or security breach occurs, which must include supervision and retraining of the offending party at minimum. It may also include the removal of HMIS end user license, client notification, and/or appropriate legal action. The Continuum Designated HMIS Lead Agency may request, or independently order, an updated criminal background check on any end user suspected of violating one or more of the standards or requirements outlined in the AL-501 CoC HMIS Operating Policies and Procedures and the AL-501 CoC End User License Agreement & Statement of Confidentiality.
Covered Homeless Organization (Contributing HMIS Organization)	CHO	Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes personal protected information (PPI) on homeless clients for an HMIS, which is also referred to as a Participating Agency in this document (69 FR 45887, p. 45928) ⁵
Data Security Standards		Baseline standards required of all programs that record, use or process HMIS data. The baseline standards are based on principles of fair information practices and security standards recognized by the information privacy and technology communities as appropriate for securing and protecting personal information. (Department of Housing and Urban Development, 2004) ⁶
Decryption		Conversion of scrambled text back into understandable, plain text form. Decryption uses an algorithm that reverses the process used during encryption.
Detailed Information		Detailed Information includes the following client level data: case plan(s), including goals, action steps, and case notes; communicable and venereal diseases (e.g. hepatitis, syphilis, gonorrhea, tuberculosis, HIV/AIDS); disability information, including chronic health condition(s), developmental, HIV/AIDS, physical and mental health; drug and/or alcohol abuse and treatment history; educational attainment; employment history; ethnicity; gender; health insurance (sources); household members; incidents and bans; income and non-cash benefits (amounts and sources); living situation, housing history, and circumstances of need; race; risk factors; services (requested and received) and referrals.
Digital Certificate		An attachment to a message or data that verifies the identity of a sender.
Encryption		The conversion of plain text into encrypted data by scrambling it with a code that masks the meaning of the data to any unauthorized viewer. Computers encrypt data by using algorithms or formulas. Encrypted data isn't readable unless it's converted back into plain text via decryption.
End User		The Participating Agency staff person who will be using the HMIS to enter and/or extract data. (HMIS Implementation Guide - Glossary). (U.S. Department of Housing and Urban Development, 2010) ⁷

⁴ 24 CFR 578.3 (n.d.). *Definitions*. Retrieved from <https://www.law.cornell.edu/cfr/text/24/578.3>

⁵ U.S. Department of Housing and Urban Development (2004) *Federal Register: (HMIS) Data and Technical Standards Final Notice*. Washington, DC: Office of the Assistant Secretary for Community Planning and Development.

⁶ U.S. Department of Housing and Urban Development (2004) *Federal Register: (HMIS) (HMIS) Data and Technical Standards Final Notice (Vol. 69, No. 146)*. Washington, DC: HUD

⁷ Department of Housing and Urban Development (2010) *Glossary*. Retrieved from

End User Certification Test		Certification Test completed by an End User after initial training, and subsequently on an annual basis, to obtain and maintain an End User license. Includes sections related to HUD definitions, ServicePoint specific workflow requirements, and Privacy & Security Standards.
End User License Agreement & Statement of Confidentiality		The agreement signed by each HMIS End User and Agency Administrator outlining the guidelines for use of the system, including individual privacy, Agency privacy and other policies and procedures for use of the HMIS. The said document sets the standards of conduct for each HMIS End User, and must be signed by all new End Users, in addition to existing End Users on an annual basis.
End User Training		Training required to obtain access to the HMIS. Includes Privacy and Security Training, program specific workflow training, definition of homelessness, review of HUD guidance, and applicable ServicePoint modules (ClientPoint / SkanPoint / ShelterPoint / ActivityPoint / Advanced Reporting Tool). Training provided on an ongoing basis.
Federal Partners	HUD HHS VA	U.S. Department of Housing and Urban Development U.S. Department of Health and Human Services U.S. Department of Veteran Affairs
Firewall		A hardware and/or software system that enforces access control policies between two networks, usually between a Local Area Network (LAN) and the Internet. A firewall allows only specific kinds of information to flow in and out of the local network. This protects the computers and data on the LAN from intruders or hackers who might try to use the internet to break into those systems.
Health Insurance Portability and Accountability Act	HIPPA	U.S. law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. Developed by the Department of Health and Human Services, these standards provide patients access to their medical records and give them more control over how their personal health information is used and disclosed. (U.S. Department of Housing and Urban Development, 2008, p. 153) ⁸
HMIS Contract Agreement		Agreement executed between the Continuum Designated HMIS Lead Agency and each Agency participating in the HMIS, outlining the rights and responsibilities of each party, and the amount of the HMIS contract.
HMIS Fee Schedule		An Agency's contract fees for use of the HMIS, including: software licenses, software annual support, training, data entry, data analysis, reporting, and administration of the HMIS.
HMIS Operating Policies and Procedures	HMIS P&Ps	Document governing the operation of the HMIS. An HMIS Lead must adopt written policies and procedures for the operation of the HMIS that apply to the HMIS Lead, its CHOs, and the Continuum of Care. These policies and procedures must comply with all applicable Federal law and regulations, and applicable state or local governmental requirements. An HMIS Lead may not establish local standards for any CHO that contradicts, undermines, or interferes with the implementation of the HMIS standards as prescribed in this part. (U.S. Department of Housing and Urban Development, 2011) ¹¹
HMIS Regional Implementation		Multiple CoCs partner together to jointly implement a single HMIS application. (U.S. Department of Housing and Urban Development, 2008, p. 41) ⁸ The HMIS Regional Implementation consists of agencies in Alabama and Florida, and is called PromisSE.
Homeless Definition		HUD defines 4 categories of homelessness. Not all programs can serve all categories and some may utilize a different definition when delivering services. The HMIS Regional Implementation has adopted the HUD definition homelessness. <ul style="list-style-type: none"> • Category 1: Literally Homeless • Category 2: Imminent Risk of Homelessness • Category 3: Homeless under other Federal Statute • Category 4: Fleeing/Attempting to Flee DV Homeless Definition Crosswalk (Appendix U)

<http://portal.hud.gov/hudportal/documents/huddoc?id=HMIS-glossary.pdf>

⁸ U.S. Department of Housing and Urban Development (2008). *2008 HMIS Training: HMIS 101 (page 153)*. Washington DC: HUD

Updated 12/2016

Homeless Management Information System	HMIS	A local information technology system used to collect client-level data and data on the provision of housing and services to homeless individuals and families and persons at risk of homelessness. Each CoC is responsible for selecting an HMIS software solution that complies with HUD's data collection, management, and reporting standards.
Interagency Data Sharing Agreement		A legally binding data-sharing agreement between agencies that share client-identified information. The agreement includes the vehicles through which information is shared (i.e. system), and the name and signatories of the responsible party for each agency.
Interim Update		The data elements in this assessment represent information that is either collected at multiple points during project enrollment in order to track changes over time (e.g., Income and Sources) or is entered to record project activities as they occur (e.g., Services Provided). (U.S. Department of Housing and Urban Development, 2016) 1
Participating Agency		An organization that uses, inputs or processes data into an HMIS. Also referred to as a Covered Homeless Organization or CHO.
Participation Agreement		An agreement executed between the Continuum Designated Lead Agency and each Participating Agency, specifying the rights and responsibilities of the agencies for the operation of the HMIS. A Participation Agreement is also executed between the HMIS Lead Agency and the Continuum Designated Lead Agency. (U.S. Department of Housing and Urban Development , 2011) 11
Personal Protected Information	PPI	Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual. (Department of Housing and Urban Development, 2004) 6
Policies & Procedures Compliance Checklist		Checklist completed by the Agency Administrator certifying the Agency's compliance with requirements outlined in the HMIS Operating Policies and Procedures.
Portable Storage Device	PSD	A secondary storage device that holds data, including small plug-and-play devices such as USB drives, recordable discs, external hard disks, etc.
Privacy and Security Checklist		A checklist completed annually by each Agency's Security Officer, including the Continuum Designated HMIS Lead Agency's System Security Officer, certifying their respective Agency is in compliance with the Privacy and Security Plan, detailed in the HMIS Operating Policies and Procedures.
Privacy and Security Training		End User training required prior to obtaining access to the HMIS, and on an annual basis after initial certification. Training curriculum is based on CoC guidelines, HMIS Operating Policies & Procedures, and all other privacy and security standards as outlined by the Federal Partners.
Privacy Notice		A written, public statement of an agency's privacy practices. A notice informing clients of how personal information is used and disclosed. (U.S. Department of Housing and Urban Development, 2008, p. 155) 8
Privacy Policy		All HMIS Participating Agencies must adopt a privacy policy, which has to be approved by its board of directors. At a minimum, the privacy policy must include the following: data collection limitations; purpose and use limitations; allowable uses and disclosures; openness description; access and correction standards; accountability standards; protections for victims of domestic violence, dating violence, sexual assault, and stalking; and such additional information and standards as may be established by HUD in notice. (U.S. Department of Housing and Urban Development , 2011)11
Program Management Information System of the Southeast	PromisSE	The name given to the HMIS Regional Implementation and its HMIS database. The implementation consists of Participating Agencies in Alabama and Florida.
Project Descriptor Data Elements	PDDEs	HUD's standard data fields that contain general information about projects, and help ensure the HMIS is the central repository for information about homelessness within the CoC, including information about projects and clients. The PDDEs are completed by the System Administrator at initial project setup in the HMIS, and should be reviewed at least once annually, and updated as needed to ensure accurate data collection and reporting. (U.S. Housing and Urban Development,

		2014, p. 3) ⁹
PromisSE HMIS Lead Agency		The PromisSE HMIS Lead Agency is the lead agency designated by the PromisSE Steering Committee. It is responsible for operating the regional HMIS database, and ascertaining contractual obligations are fulfilled relating to the HMIS software, inclusive of the following: <ul style="list-style-type: none"> a) Establishing a fee structure. b) Invoicing participating local CoCs. c) Ordering End User licenses as requested by local HMIS Lead Agencies.
PromisSE Steering Committee		The PromisSE Steering Committee is the governing entity of the HMIS Regional Implementation known as PromisSE, and responsible for the following: <ol style="list-style-type: none"> 1) The Steering Committee will designate a HMIS Lead Agency. 2) The Steering Committee structure will be as follows: one voting seat will be provided to each local, participating HMIS Lead Agency and one voting seat will be provided to each local participating CoC. The Steering Committee can add non-voting advisory seats as needed for additional partners and subject matter experts. 3) The Steering Committee will be responsible for the development and revision of the HMIS Operating Policies and Procedures and their enforcement, expansion of the implementation, determine the HMIS software, determine the HMIS Lead Agency, and identify a HMIS Coordinator, in addition to the HMIS Lead Agency to facilitate Bowman support. 4) The Steering Committee will be meet at least quarterly, with at least one meeting occurring in person. 5) The Steering Committee will identify three officers to serve a one-year term and they will be as follows: <ul style="list-style-type: none"> a) The Steering Committee Chair will be responsible for calling and facilitating meetings, designating committees, and assigning committee duties. b) The Steering Committee Vice-Chair will be responsible for assuming the duties of the Chair in the case the Chair is unable to fulfill them. c) The Steering Committee Secretary will be responsible for maintaining minutes and documentation relating to the Steering Committee.
Provider		A Participating Agency and its project in the HMIS are referenced as the Provider.
Public Key Infrastructure	PKI	An encryption method authenticating a computer is authorized to access a network by verifying its identity and location, enabling users and computers to securely exchange data. PKI requires a matching server certificate / client certificate pair, and is used to decrypt the data that is sent from the End User's ServicePoint (HMIS) site to their web browser.
Release of Information	ROI	Document provides notice to clients of how their personal information is used within the HMIS, and requires consent from the clients on how the personal information is shared.
Secure Sockets Layer	SSL	SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
Security Officer		An individual assigned by the Agency tasked with ensuring compliance with applicable security standards
ServicePoint		The name of the HMIS software selected by the PromisSE Steering Committee for use in the regional implementation.
System Administrator		The individual(s) whose job it is to manage the HMIS implementation at the local level, inclusive of enrolling programs and managing appropriate use of the HMIS, supporting users through the connection to or direct provision of the HMIS, End User training, and overseeing system setup. (U.S. Department of Housing and Urban Development, 2016, p. 9) ¹⁰

⁹ U.S. Department of Housing and Urban Development (2014) *HMIS Project Descriptor Data Elements (p.3)*. Washington, DC: HUD

¹⁰ U.S. Department of Housing and Urban Development (2016) *HMIS Data Standards Data Dictionary (p.9)*. Washington, DC: HUD

¹¹ U.S. Department of Housing and Urban Development (2011) *Federal Register: (HMIS) Data and Technical Standards Final Notice (Vol. 76, No. 237)*. Washington, DC: HUD

Two Factor Authentication	2FA or TFA	TFA is a two-step verification process also known as "multi-factor authentication," which requires not only a password and username, but also something that is unique to a particular End User (i.e. PKI Client Certificate). TFA provides an additional layer of security, making it harder for potential intruders to gain access and steal a person's personal data or identity.
U.S. Department of Health and Human Services	HHS	A Cabinet department of the United States government with the goal of protecting the health of all Americans and providing essential human services.
U.S. Department of Housing and Urban Development	HUD	The Federal agency responsible for national policy and programs that address America's housing needs that improve and develop the Nation's communities, and enforce fair housing laws.
Universal Data Elements	UDEs	HMIS Universal Data Elements are elements required to be collected by all projects using an HMIS. HMIS Data and Technical Standards. (U.S. Department of Housing and Urban Development, 2014) ¹¹
Veterans Affairs	VA	A government-run military veteran benefit system. It is responsible for administering programs of veterans' benefits for veterans, their families, and survivors. The benefits provided include disability compensation, pension, education, home loans, life insurance, vocational rehabilitation, survivors' benefits, medical benefits, and burial benefits.
Visibility		Refers to the ability to see a client's data between provider pages on the HMIS. Visibility is configured on the HMIS system in 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 procedures defined in this document represent the minimum standards of participation in the HMIS and general "best practice" operating procedures. Local Participating Agencies, in coordination with the Continuum Designated HMIS Lead Agency (Housing First, Inc.), may include additional standards. Operational standards in this document are not intended to supersede grant-specific requirements or operating procedures as required by funding entities.

The AL-501 CoC HMIS Operating Policies and Procedures are updated routinely as the Federal Partners publish additional guidance, or as part of the annual review process. Updates will be reviewed by the PromisSE HMIS Lead Agency's administration and the Continuum Designated HMIS Lead Agency. **To allow for evolution of compliance standards without re-issuing core agreements, updated policies supersede related policies in previously published AL-501 CoC HMIS Operating Policies and Procedures or Agreements. Any changes from the previous year will be highlighted. A current copy of the AL-501 CoC HMIS Operating Policies and Procedures may be found on Housing First's website: www.hfal.org/services/hmis-department/policy-and-procedures/.**

Privacy Statement

The AL-501 Homeless Coalition of the Alabama Gulf Coast Continuum of Care ("AL-501 CoC") is committed to making the HMIS safe for all types of programs in the AL-501 CoC, and the clients whose information is recorded within the database. This privacy statement describes our privacy policy regarding clients' personal protected information (information which can be used to identify a specific client or "PPI") residing in PromisSE, and explains what PPI is collected, why it is collected, and how it is used and disclosed. PromisSE is a Homeless Management Information System ("HMIS" or "System"), which is a computer system that the U.S. Department of Housing and Urban Development ("HUD") requires us to use for homeless assistance programs. The HMIS is used collect client data and data on the provision of housing and services to homeless individuals, families, and persons at risk of homelessness. The information that we collect allows us to work with other Agencies to help our clients, coordinate their case management, and to reduce the number of times that they have to re-tell their story or repeat information.

¹¹ U.S. Department of Housing and Urban Development (2014) *HMIS Data and Technical Standards*. Retrieved from <https://www.hudexchange.info/programs/hmis/hmis-data-and-technical-standards/>.

Confidentiality Rights

The HMIS is operated by the AL-501 CoC's Continuum Designated HMIS Lead Agency (Housing First, Inc.) in accordance with HUD confidentiality regulations, including those covering programs that receive HUD funding for homeless services (Federal Register/Vol. 69, No. 146). Agencies covered under the Health Insurance Portability and Accountability Act (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, must notify Housing First's System Administrator of their HIPAA status to allow Housing First to handle their client data in compliance with HIPAA. Other rules that may also apply include 42 CFR Part 2 governing drug and alcohol records.

Why We Collect Information

We collect Personal Protected Information directly from our clients for reasons discussed in the AL-501 CoC Privacy Notice to Clients. We may also collect information about the client from other Agencies if the client has given the Agency written consent to share their information. We may be required to collect some personal information by law or by organizations that give us money to operate our programs. Additional personal information that we collect is important to run our programs, to improve the services for homeless persons, and to better understand the needs of homeless persons. The collection and use of PPI is guided by strict standards of confidentiality. We only collect PPI when appropriate, by lawful and fair means, and with the knowledge or consent of the client. Our Privacy Notice is posted on our website at www.hfal.org/services/hmis-department/policy-and-procedures/. A copy of our Privacy Notice is available to all clients upon request.

How We Use and Disclose Information

Protected Personal Information can only be used for the following purposes:

- a. To **provide or coordinate services** for individuals;
- b. for functions related to **payment or reimbursement for services**;
- c. to **carry out administrative functions** such as legal, audits, personnel, oversight, and management functions;
- d. to **create de-identified (anonymous) information** that can be used for reporting, research, and statistical purposes without identifying clients;
- e. for **contractual research purposes** where privacy conditions are met (including a written agreement);
- f. **when required by law** to the extent that use or disclosure complies with and is limited to the requirements of the law;
- g. to **avert a serious threat to health or safety** if:
 - i. we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, **and**
 - ii. the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat;
- h. to comply with **government reporting obligations** for the HMIS and for oversight of compliance with HMIS requirements;
- i. to report criminal activity on Agency premises.

Limited Information Sharing

We require our client's to sign the AL-501 CoC Client Release of Information and Sharing Plan ("ROI" or "Sharing Plan"), which provides notice of how personal information is used within the HMIS, and requires the client's consent on how their personal information is shared and the Participating Agencies with which it is shared. The client may request a copy of the Sharing Plan to see a complete list of agencies with which information may be shared. Although the agencies who participate in the Sharing Plan may change from time to time, a client may always request a copy of the most recent Sharing Plan.

The Limited Sharing Model we use is as follows, and offers three (3) sharing options:

1. **Option 1** - This option allows the most information sharing, and therefore the most coordination of services and the least duplication of efforts in order to serve a client. The information below is shared as follows:

- a. **Basic Information** – Basic Information is shared with Participating Agencies in Alabama and Florida. Basic Information includes the following: name, date of birth, social security number, program enrollments, case managers, military background (veteran status) and photo.
 - b. **Detailed Information** – Detailed Information is only shared with local agencies in Mobile and Baldwin counties listed in the Sharing Plan, and includes the following: case plan(s), including goals, action steps, and case notes; communicable and venereal diseases (e.g. hepatitis, syphilis, gonorrhea, tuberculosis, HIV/AIDS); disability information, including chronic health condition(s), developmental, HIV/AIDS, physical and mental health; drug and/or alcohol abuse and treatment history; educational attainment; employment history; ethnicity; gender; health insurance (sources); household members; incidents and bans; income and non-cash benefits (amounts and sources); living situation, housing history, and circumstances of need; race; risk factors; services (requested and received) and referrals.
2. **Option 2** - Under Option 2, **only** the agencies a client specifies will be able to see their Detailed Information, including their healthcare and drug treatment information.
 3. **Option 3** - Under Option 3, a client's information **will not** be shared, and they **will not** be denied access to services because they choose not to share their information.

A client's Basic Information (name, date of birth, social security number, program enrollments, case managers, military background/veteran status and photo) collected in the field by outreach workers may be entered into the HMIS prior to the execution of a signed ROI. However, the outreach worker must provide the client with the AL-501 CoC Outreach Privacy Notice (Appendix Q) and sign the AL-501 CoC Outreach Consent Certification (Appendix R), affirming receipt of the client's verbal consent before entering, updating, editing, printing, or disclosing their Basic Information. Otherwise, limited visibility must be coordinated with Housing First. Detailed Information may not be entered into the HMIS prior to execution of the ROI.

Client Information Rights

1. All requests for personal information located within the HMIS should be made to the Agency or organization that collected, entered and/or updated a client's information.
2. We may not disclose Personal Protected Information located within the HMIS, except as required by law, or to help Participating Agencies that collected/entered/updated the information operate the System.
3. We 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.

A client has the right to refuse consent to share their information between Participating Agencies. A client cannot be denied services that they would otherwise qualify for if they refuse to share information. If the client refuses this permission, their information will still be entered into the HMIS for statistical purposes, but their information will be closed so that only that Agency they gave their information to and System Administrator(s) operating the HMIS database will see their information.

Agreements, Certifications, Licenses and Disclaimers

- 1) Each Continuum Designated HMIS Lead Agency signs an **Agreement and Authorization** that designates the use of a regional HMIS system and identifies the Continuum Designated HMIS Lead Agency as the lead Agency for the administration of the local HMIS database. The Continuum Designated HMIS Lead Agency will also collaborate with PromisSE's HMIS Lead Agency. PromisSE's HMIS Lead Agency is responsible for specific tasks. The Agreement and Authorization supports the ability for multiple jurisdictions to participate in a single HMIS information system.
- 2) PromisSE's HMIS Lead Agency must execute a Participation Agreement (Appendix L) with all Continuum Designated HMIS Lead Agencies, specifying the rights and responsibilities of the agencies for the operation of the HMIS and client-level data sharing. The PromisSE HMIS Lead Agency retains record of all interagency agreements executed with the Continuum Designated HMIS Lead Agencies.
- 3) Continuum Designated HMIS Lead Agencies must execute a Participation Agreement (Appendix A) with all Participating Agencies, specifying the rights and responsibilities of the agencies for the operation of the HMIS and client-level data sharing. The Continuum Designated HMIS Lead Agency retains record of all interagency agreements executed with the Participating Agencies.

Updated 12/2016

- 4) Continuum Designated HMIS Lead Agencies and Participating Agencies must also adopt and/or execute the following policies and agreements:
 - a) Privacy Policy (Appendix J), which outlines Agency privacy and security standards, and has to be approved by each agency's board of directors.
 - b) Privacy Notice to Clients (Appendix I), which discloses Agency privacy practices and informs clients of how their personal information is used and disclosed. This notice was developed in close collaboration with the Participating Agencies that manage information that may put a client at risk. All privacy practices are designed to ensure the broadest range of agencies may participate in the HMIS.
 - c) End User License Agreement & Statement of Confidentiality (Appendix F), which governs the individual End User's participation in the HMIS, and acknowledges their receipt of the Privacy Notice to Clients. Copies of the agreements must be retained by both the Continuum Designated HMIS Lead Agencies and the Participating Agencies.
 - d) Agency Administrator Agreement for Agencies (Appendix B) or the System Administrator Agreement for Continuum Designated HMIS Lead Agencies (Appendix M), which govern the roles and responsibilities thereof.
 - e) Agency Security Officer Agreement (Appendix C) or the System Security Officer Agreement for Continuum Designated HMIS Lead Agencies (Appendix N), which govern the roles and responsibilities thereof.
 - f) Agency Administrators must execute the HMIS Criminal Background Check Certification (Appendix S) form, certifying a prospective End User has successfully cleared their criminal background check, before access is granted to the HMIS.
 - g) Agencies who wish to share information with other Agencies participating in the PromisSE outside of the AL-501 CoC, must sign interagency agreements describing the PromisSE privacy rules the agencies are required to follow. The agreement must also acknowledge the agencies are prohibited from making further disclosure of the information shared, unless it is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by law.
 - h) Taken together, the aforementioned documents obligate participants to core privacy procedures.

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:

- 1) All End Users must successfully clear a criminal background check before gaining access to the HMIS. Successful clearance is certified in writing by the Agency Administrator on the AL-501 CoC HMIS Criminal Background Check Certification (Appendix S) form, and submitted to the Continuum Designated HMIS Lead Agency's System Administrator before access to the HMIS is granted. Successful clearance means the individual has not been convicted of a crime involving deception, or a felony involving violence or the threat of violence against another person within the last seven (7) years. Participating Agencies may use more restrictive requirements for passing criminal background checks, but may not use less restrictive requirements.
- 2) **Agency Administrator** - Agencies must assign an Agency Administrator responsible for the following:
 - a) Completing, at a minimum, initial HMIS training and Advanced Reporting Tool training if the Agency holds an HMIS reporting license.
 - b) Ensuring all Agency End Users have a signed End User License Agreement & Statement of Confidentiality on file.
 - c) Ensuring all End Users complete the annual End User Certification Test, to include Privacy and Security Training.
 - d) Ensuring all End Users complete workflow training and related updates, and have documentation of training.
 - e) Ensuring the Agency is in compliance with the Data Security Standards outlined in this document.
 - f) Ensuring the Agency is in compliance with the HMIS Operating Policies and Procedures, completes the HMIS Policies and Procedures Compliance Checklist (Appendix D), and returns it to the Continuum Designated HMIS Lead Agency's System Administrator.

g) Ensuring all End Users have successfully cleared a criminal background check. The Agency Administrator certifies successful clearance by completing the HMIS Criminal Background Check Certification form, and submitting it to the Continuum Designated HMIS Lead Agency's System Administrator, which is required prior to gaining access to the HMIS.

3) **Agency Security Officer** - All Agencies must assign an Agency Security Officer responsible for the following:

- a) Ensuring Agency computers connected to the HMIS are automatically updated on a regular basis, have current antivirus software, and firewall protection.
- b) Ensuring all Agency End Users complete annual Privacy and Security Training. Training must be provided by the Continuum Designated HMIS Lead Agency and based on the Privacy and Security Plan.
- c) Conducting an annual security review of the Agency that includes reviewing compliance with the Privacy and Security Plan. The Agency must document the findings of the review on the AL-501 CoC Privacy and Security Checklist (Appendix E). The Agency must submit the findings to the Continuum Designated HMIS Lead Agency's System Administrator no later than December 31st of each year.
- d) Notifying the Continuum Designated HMIS Lead Agency's System Administrator when an End User leaves the organization or when revision of the End User's access level is needed because of a change in job responsibilities. The notification must be made within 24 hours of the change.
- a) Reporting any security or privacy incidents to the Continuum Designated HMIS Lead Agency's System Administrator. 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 End Users involved violated privacy or security guidelines, the System Administrator will report the breach to the chair of the AL-501 CoC Board of Directors and the CEO of Housing First. A Corrective Action Plan will be implemented, which must include supervision and the retraining of the offending party, at minimum. It may also include the removal of HMIS End User licenses, client notification, and/or appropriate legal action. The Continuum Designated HMIS Lead Agency may request, or independently order an updated criminal background check on any End User suspected of violating one or more of the standards or requirements outlined in the AL-501 CoC HMIS Operating Policies and Procedures and the AL-501 CoC End User License Agreement & Statement of Confidentiality.

4) **System Administrator** - Continuum Designated HMIS Lead Agencies must have an assigned System Administrator responsible for the following:

- a) Completing, at minimum, System Administrator training.
- b) Ensuring all End Users have a signed End User License Agreement & Statement of Confidentiality on file.
- c) Ensuring all Agency Administrators have a signed Agency Administrator Agreement on file.
- d) Ensuring all Security Officers have a signed Security Officer Agreement on file.
- e) Ensuring all End Users complete the annual End User Certification Test, to include Privacy and Security Training.
- f) Ensuring all End Users complete workflow training and related updates, and are provided documentation of the training.
- g) Ensuring the Participating Agencies are in compliance with the Data Security Standards outlined in this document.
- h) Ensuring the Participating Agencies are in compliance with the HMIS Operating Policies and Procedures.
- i) Ensuring all End Users have successfully cleared a criminal background check, evidenced by the receipt of the HMIS Criminal Background Check Certification from the Agency Administrator, prior to gaining access to the HMIS.

5) **System Security Officer** - All Continuum Designated HMIS Lead Agencies must assign a System Security Officer responsible for the following:

- a) Ensuring the Continuum Designated HMIS Lead Agency's computers connected to the HMIS are automatically updated on a regular basis, have current antivirus software, and firewall protection.
- b) Ensuring all End Users complete annual Privacy and Security Training. Training must be provided by the Continuum Designated HMIS Lead Agency and based on the Privacy and Security Plan.
- c) Conducting an annual security review of the Continuum Designated HMIS Lead Agency that

- includes reviewing compliance with the Privacy and Security Plan. The System Security Officer must document the findings of the review on the Privacy and Security Checklist (Appendix E), which must be submitted to the PromisSE HMIS Lead Agency's System Administrator no later than December 31st of each year.
- d) The PromisSE HMIS Lead Agency conducts routine audits to ensure compliance with the HMIS Operating Policies and Procedures. The audit could include a mix of System and onsite reviews. The PromisSE HMIS Lead Agency will make recommendations for corrections as needed.
 - e) Notifying the PromisSE HMIS Lead Agency's System Administrator when a System Administrator leaves the organization or when revision of a System Administrator's access level is needed because of changes to job responsibilities. **The notification must be made within 24 hours of the change.**
 - f) Reporting any security or privacy incidents to the Continuum Designated HMIS Lead Agency's System Administrator. The System Administrator investigates the incident, including running applicable audit reports. If the System Administrator and System Security Officer determine that a breach has occurred and/or the End Users involved violated privacy or security guidelines, the System Administrator will report the breach to the chair of the AL-501 CoC Board of Directors and the CEO of Housing First. A Corrective Action Plan will be implemented, which must include supervision and retraining of the offending party, at minimum. It may also include the removal of HMIS End User licenses, client notification, and/or appropriate legal action. The Continuum Designated HMIS Lead Agency may request, or independently order an updated criminal background check on any End User suspected of violating one or more of the standards or requirements outlined in the AL-501 CoC HMIS Operating Policies and Procedures and the AL-501 CoC End User License Agreement & Statement of Confidentiality.

Privacy Standards:

- 1) **Public Notice** - All Agencies and Continuum Designated HMIS Lead Agencies are required to have the Public Notice (Appendix H) posted and visible to clients where information is collected.
- 2) **Privacy Notice to Clients** - All Agencies and the Continuum Designated HMIS Lead Agency are required to adopt the AL-501 CoC Privacy Notice to Clients (Appendix I), which must be posted to their respective websites. Requests to modify the Privacy Notice must be submitted to the Continuum Designated Lead Agency for approval. All privacy notices must define the uses and disclosures of data collected in the HMIS, in addition to the following:
 - a) The purpose for collection of client information.
 - b) A brief description of the 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, and/or correct their record.
 - e) The client complaint procedure.
 - f) Notice to the client 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.
- 3) **Privacy Policy** - All Agencies and the Continuum Designated HMIS Lead Agency are required to adopt the AL-501 CoC Privacy Policy (Appendix J). Requests to modify the Privacy Policy must be submitted to the Continuum Designated Lead Agency for approval. All privacy policies must include the following:
 - a) Procedures defined in the Privacy Notice
 - b) Protections afforded to 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 shall include the following at minimum:
 - i. Setting closed visibility so that only the serving Agency may see the record. The End User must notify the Continuum Designated HMIS Lead Agency's System Administrator within 24 hours of input of this information into the System to close the record.
 - ii. The right to have a record marked as inactive.
 - iii. The right to remove the record from the System.

- c) Security of hard copy files
 - d) Policy covering uses of client data generated from the HMIS
 - e) Client information storage and disposal
 - f) Remote access and usage requirements
 - g) Prohibition from transferring HMIS data to Portable Storage Devices, including small plug-and-play devices such as USB drives, recordable discs, and external hard disks.
- 5) 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 for unauthorized individuals.
 - 6) **Client ROI** - All Agencies and Continuum Designated HMIS Lead Agencies are required to adopt the AL-501 CoC Client Release of Information and Sharing Plan. Requests to modify the ROI must be submitted to the Continuum Designated Lead Agency for approval. All ROIs must provide notice to clients of how their personal information is used within the HMIS, and requires consent from the clients on how the personal information is shared.
 - 7) Agencies and Continuum Designated HMIS Lead Agencies are required to maintain a culture that supports privacy.
 - a) Staff does not discuss client information in the presence of others without a "need-to-know."
 - b) Staff removes unique client identifiers before releasing data to the public.
 - c) Agencies configure intake workspaces to support privacy of client interaction and data entry.
 - d) User accounts and passwords are not shared between End Users, or left visible for others to see.
 - e) Staff are trained regarding appropriate use of electronic communication.
 - 8) All staff 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.
 - 9) Providers that are covered under the Violence Against Women Act (VAWA) are prohibited from entering data into the HMIS.

Data Security Standards:

- 1) All licensed End Users of the System must be assigned access levels consistent with their job responsibilities and their business "need-to-know."
- 2) All computers have virus protection with automatic updates.
 - a) Agency Security Officers are responsible for monitoring all computers that connect to the HMIS to ensure:
 - i. Antivirus software is up-to-date.
 - ii. Updates are automatic.
 - iii. Operating system updates are scheduled to run regularly.
- 3) All computers are protected by a firewall.
 - a) Agency Security Officers are responsible for monitoring all computers that connect to the HMIS to ensure:
 - i. For single computers, the software and version are current.
 - ii. For network computers, the firewall model and version are current.
 - iii. Operating system updates are scheduled to run regularly.
- 4) Physical access to computers that connect to the HMIS is controlled.
 - a) All workstations are in secured locations (locked offices).
 - b) End Users must log out of the HMIS and their computer when leaving the workstation.
 - c) All workstations are password protected.
 - d) After a short period of time a password protected screen saver will be activated during the time the computer is not in use.
 - e) End Users are prohibited from accessing the HMIS from a computer that is available to the public **or** through an internet connection that is not secure. End Users are not permitted to use public Wi-Fi to access the HMIS, including that provided by internet cafes, libraries, airports or other non-secure internet connections.
- 5) A plan for remote access if staff will be using the HMIS outside of the office, such as accessing HMIS from home or in the field. Concerns addressed in this plan should include the privacy surrounding the off-

site entry.

- a) The computer and environment for data entry must meet all the standards defined above.
- b) Downloads from the computer may not include client identifying information.
- c) End Users are prohibited from transferring HMIS data to Portable Storage Devices, including small plug-and-play devices such as USB drives, recordable discs, and external hard disks.

Remember that your information security is never better than the trustworthiness of the staff you license to use the System. The data at risk is your own, that of your sharing partners, and of our clients. If an accidental or purposeful breach occurs, you are required to notify the System Administrator of the Continuum Designated HMIS Lead Agency and the PromisSE HMIS Lead Agency immediately.

Bowman Systems Data Security:

- 1) **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's being transmitted. When an End User accesses their ServicePoint site, an SSL (encrypted) negotiation is performed between the server at Bowman System'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.
- 2) **PKI Encryption** - An additional layer of encryption in ServicePoint 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 ServicePoint site to their web browser. Without the appropriate PKI Client Certificate installed on the End User's computer, their web browser isn't able to decrypt the data, therefore prohibiting access the ServicePoint site. The PKI Client Certificate is installed on an End User's computer by the System Administrator before the End User can access ServicePoint, which allows agencies to regulate exactly which devices can and cannot access ServicePoint.
- 3) **Two Factor Authentication** - The requirement of a username and password to access ServicePoint 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.
- 4) The ServicePoint 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 Bowman Systems.
- 5) Only authorized personnel at Bowman Systems have access to the equipment used to host the customer's data.

Bowman Systems Disaster Recovery Plan:

The HMIS can be a critically important tool in the response to catastrophic events. PromisSE contracts with Bowman Systems to provide disaster recovery services for ServicePoint. ServicePoint's data is housed in a secure server bank in Shreveport, LA. There is a nightly backup of the ServicePoint system, which is comprised of a backup of the database and a backup of the application code. Bowman's standard protocol includes nightly tape backup of the client's database that is carried three miles off-site and stored in a fireproof facility. Bowman Systems maintains redundant power for all on-site servers via building power and building generator, and redundant bandwidth is provided via two separate upstream providers. Bowman's data center contains a state-of-the-art, nondestructive fire-suppression system, and has two separate, fully redundant HVAC systems for server areas. Bowman Systems also utilizes RAID technologies (Redundant Array of Independent Disks) to mirror the hard drives, provide faster data throughput and ensure reliable data.

- 1) Bowman Systems' disaster recovery includes:
 - a) Nightly database tape backups.
 - b) Offsite storage of tape backups
 - c) Seven day backup history stored locally on instantly accessible Raid 10 storage
 - d) One month backup history stored off site
 - e) 24 x 7 access to Bowman Systems emergency line to provide assistance related to "outages" or "downtime."
 - f) 24 hours backed up locally on instantly-accessible disk storage

- 2) All customer site databases are stored online, and are readily accessible for approximately 24 hours; tape backups are kept for approximately one (1) month, and are stored off-site in a fireproof facility. 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 tape 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.
- 3) Communication between the staff of the PromisSE HMIS Lead 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 the location and type of disaster.
- 4) Please see “Bowman Systems Securing Client Data” posted to www.hfal.org/services/hmis-department/policy-and-procedures/ for a detailed description of Bowman’s data security standards and disaster recovery plans.

System Administration:

HMIS Provider Set-Up:

- 1) Providers in the HMIS are properly identified in the HMIS per the AL-501 CoC naming standards:
 - a) CoC Name-(Project Type Acronym) Agency name - Project Name
 - i. Example: AL501-(PH) Agency ABC – Community Housing Program
- 2) Inactive providers are properly identified in the HMIS per the AL-501 naming standards:
 - a) ZZZ><Coc Name-(Project Type Acronym) Agency name - Project Name
 - i. Example: ZZZ><AL501-(PH) Agency ABC – Rapid Re-housing Program
- 3) Inactive providers are properly identified in the HMIS per the AL-501 naming standards:
 - a) Database Only><Coc Name- Agency name – Project Name
- 4) Example: Database Only><AL501-Provider ABC – Hospital
- 5) The Continuum Designated HMIS Lead Agency is responsible for setting up and maintaining Providers in the HMIS.

HUD Project Descriptor Data Elements:

The HUD Data Standards or Project Descriptor Data Elements (PDDEs), below, must be completed for each of the Continuum projects participating in HMIS. Please see the HMIS PDDE Manual on HUD’s website for more information (www.hudexchange.info/resource/4055/hmis-project-descriptor-data-elements-manual/).

- a) 2.1 Organization Identifiers
- b) 2.2 Project Identifiers
- c) 2.3 Continuum of Care Code
- d) 2.4 Project Type
- e) 2.5 Method for Tracking Emergency Shelter Utilization
- f) 2.6 Federal Partner Funding Sources
- g) 2.7 Bed and Unit Inventory Information
- h) 2.8 Site Information – Optional*
- i) 2.9 Target Population – Optional*

*Data elements 2.8 and 2.9 are required if the HMIS is used to generate the HIC.

Data Quality Plan:

- 1) Agencies and Continuum Designated HMIS Lead Agencies must require documentation at intake on the homeless status of clients according to the reporting and eligibility guidelines issued by HUD. The preferred “order of priority” for obtaining evidence of homeless status is (1) third-party documentation, (2) worker observations, then (3) certification from the person. Lack of third-party documentation may not be used to refuse emergency shelter, outreach or domestic violence services.

- 2) All staff are required to be trained on the HUD definition of Homelessness.
 - a) There is congruity between the HMIS data elements Residence Prior to Project Entry and Housing Status, based on the applicable homeless definition.
- 3) Agencies and Continuum Designated HMIS Lead Agencies have a process to ensure the first and last names are spelled properly and the DOB is accurate.
 - a) An ID is requested at intake to support proper spelling of the client's name and accurate recording of the DOB.
 - b) If no ID is available, staff will request the legal spelling of the client's name.
 - c) High volume programs, especially those serving chronic and high risk populations, are offered use of the SkanPoint module within ServicePoint to reduce duplication and improve the efficiency of recording services.
- 4) Client records are updated annually, at minimum, by emergency shelters. All other program types are required to update client records on a quarterly basis via Interim Updates and annually via an Annual Assessment. Annual Assessments must be completed within 30 days +/- of the anniversary date of the client's entry into the program for a client enrolled for 365 days or more.
- 5) Agency Administrators will run data quality reports on the 5th (fifth) of each month. All missing and inaccurate information should be corrected by the 20th (twentieth) of each month. All participating programs should have a Data Quality Report Card score of "95%" by the 25th (twenty-fifth) of each month.
 - a) The End Users associated with any Program maintaining a data quality score of less than "80%" for three (3) consecutive months will be required to participate in a refresher training.
 - b) Data quality screening and correction activities must include, at minimum, completion or correction of missing or inaccurate Universal Data Elements.
 - c) Report frequency for funded programs is governed by grant agreements, HUD reporting cycles, and Continuum Designated HMIS Lead Agency standards. However, all programs will be reviewed and asked to make corrections at least monthly.

Workflow Requirements:

- 1) Assessments assigned to the Provider meet HMIS minimum data entry requirements and additional funder requirements if applicable.
- 2) End Users performing data entry follow the most recent version of their program's workflow.
- 3) Live data entry is the preferred method of client level data entry. If data collection is done via paper forms, the program is responsible for ensuring all data collection forms align with the workflow, HMIS minimum requirements, and funder requirements if applicable.
 - a) All HMIS participating programs are required to enter, at minimum, the Universal Data Elements and funder required data elements if applicable.
 - b) 100% of collected client level data is entered within 48 hours of data collection.
- 4) Agencies and Continuum Designated HMIS Lead Agencies actively monitor program participation and existing clients. Clients are exited within 30 days of last contact unless program guidelines specify otherwise.
- 5) Data sharing is properly configured for sharing information internally between programs, including the use of visibility groups.
- 6) External data sharing aligns with local, state, and federal laws, including the use of visibility groups.

Electronic Data Exchanges:

- 1) Agencies must request permission from the Continuum Designated HMIS Lead Agency to import or export data to or from the HMIS. The Continuum Designated HMIS Lead Agency will review the request and provide approval or denial.
- 2) Continuum Designated HMIS Lead Agencies may elect to participate in de-identified (anonymous) research data sets to support research and planning.
 - a) De-identification includes the masking or removal of all identifying, or potentially identifying, information such as: name, unique client ID, social security number, date of birth, address, Agency name, and Agency location.
 - b) Geographic analysis is restricted to prevent any data pools small enough to inadvertently identify a client by other characteristics or combination of characteristics.
 - c) Programs used to match and/or remove identifying information do 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 must certify they meet medical/behavioral health security standards and that all identifiers are kept strictly confidential and separate from the de-identified data set.
- d) Agencies and Continuum Designated HMIS Lead Agencies are provided a description of each study being implemented. Agencies may opt out of the study through written notice to the Continuum Designated HMIS Lead Agency or the study owner.

End User Requirements:

- 1) All prospective End Users must successfully clear a criminal background check before gaining access to the HMIS, which is certified by the Agency Administrator to the Continuum Designated HMIS Lead Agency's System Administrator.
- 1) All prospective End Users must participate in initial HMIS training, to include Privacy and Security Training, complete the End User Certification Test, and submit the End User License Agreement & Statement of Confidentiality to obtain an End User license.
 - a) Prospective End Users must successfully complete the End User Certification Test within two (2) weeks of training. End Users must score a minimum of "90%" on the End User Certification Test.
 - b) End Users must log into ServicePoint within one week from receipt of End User credentials.
- 2) End Users with the assigned user level "Agency Administrator" are required to log in at least monthly.
- 3) End Users with the assigned user level "Case Manager I", "Case Manager II", "Case Manager III", or "System Administrator" are required to log in at least weekly.
 - a. End Users logging in at a lesser frequency may be required to attend refresher training and/or have their assigned level evaluated for relevance.
 - b. System access settings will reflect the job responsibilities of the person using the System.
- 4) All current End Users must successfully complete the End User Certification Test annually.
- 5) All End Users participate in workflow and update training for their assigned workflows.
- 6) All End Users are provided with a list of HUD Data Standards Universal Data Elements (Appendix K).
- 7) End Users must notify the Continuum Designated HMIS Lead Agency's System Administrator of an ROI's expiration within 48 hours, so that the client record can be "closed," unless the client signs a new ROI.

AL-501 CoC HMIS Contract Agreement Policy

HMIS Contract Agreement

The Continuum Designated HMIS Lead Agency will execute the AL-501 CoC HMIS Contract Agreement with each Participating Agency within the AL-501 CoC, outlining the rights and responsibilities of each party. The contract term operates on the Continuum Designated HMIS Lead Agency's fiscal year (October 1 – September 30). Additional services must be formally requested by the Agency. The cost of the additional services will be billed to the Agency on the statement immediately following the request.

HMIS Fee Schedule

The HMIS Fee Schedule (see Attachment B of the AL-501 CoC HMIS Contract Agreement) provides a detailed itemization of the amount of the HMIS Contract Agreement, and is designed to ensure high quality HMIS customer service, technical assistance, and data management through equitable cost sharing amongst participating Agencies. The HMIS Fee Schedule may be amended as needed by the Continuum Designated HMIS Lead Agency. Changes must be reviewed and approved by the CoC Board of Directors prior to public distribution and implementation.

Payments

Agencies may choose to pay on a monthly or an annual basis. If a new Agency joins the HMIS, or if an existing Agency implements a new project within the contract year, the HMIS contract amount will be prorated. The Continuum Designated HMIS Lead Agency expects payment at the time it is due. Statements will be submitted to the Agency by the 15th of each month. Payment is due upon receipt, and is considered late after a grace period of 30 days from date of issue. Payments must be issued on a company check and made payable to the Continuum Designated HMIS Lead Agency. At the close of the grace period, the Continuum Designated HMIS Lead Agency reserves the right to suspend the accounts of all End Users associated with the Agency until full payment is received.

Contract Termination

Both parties reserve the right to terminate the HMIS Contract Agreement. The terminating party must submit in writing a notice of termination no less than 30 days prior to the intended termination date. The terminating Agency is responsible for payment through the 30-day notice, and subject to a termination fee equal to two (2) months of the HMIS contract amount or payment of the contract in full, whichever is the lesser amount. Refunds to Agencies paying annually will be made after the notice period. Should the Continuum Designated HMIS Lead Agency wish to terminate the HMIS Contract Agreement, the request will be brought before the CoC Board of Directors for review to determine the validity of the request and subsequent fees. Should the violation include a breach of the AL-501 CoC HMIS Operating Policies and Procedures, the Continuum Designated HMIS Lead Agency reserves the right to collect or withhold the full balance of the HMIS contract amount after termination.

Project Defunding

If the HMIS Contract Agreement includes a federally funded subrecipient project that is defunded, and the Agency wishes to terminate the project within the HMIS, the Continuum Designated HMIS Lead Agency must be notified in writing prior to the project's date of closure. A termination fee will not be assessed. If the annual contract amount was paid in full, the Agency will be reimbursed the prorated contract amount for the defunded project within 30 days from the date of the project's closure.

Hardship Clause

The Continuum Designated HMIS Lead Agency understands unforeseen events may arise that impede an Agency's ability to meet the financial obligation of the contract. Should such an event occur, the Agency must inform the Continuum Designated HMIS Lead Agency by written notice 15 days prior to the close of the grace period. The Continuum Designated HMIS Lead Agency will present the case to the CoC Board of Directors, the body responsible for determining whether the circumstances meet the basic requirements of the Hardship Clause. If accepted, reasonable accommodations will be determined on an individual basis.

AL-501 CoC Participation Agreement

**Between HOUSING FIRST, Inc.
And:**

(Agency Name)

This agreement is entered into on (dd/mm/yy) between HOUSING FIRST, INC., hereafter known as "Housing First" or the "Continuum Designated HMIS Lead Agency," and _____, hereafter known as the "Agency," regarding access and use of the AL-501 Continuum of Care Homeless Management Information System ("HMIS"), hereafter known as Program Management Information System of the Southeast ("PromisSE" or "the System").

I. Introduction

The **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 interagency agreements, on common clients.

PromisSE's goals are to:

- Improve coordinated care for and services to homeless persons in the states of Alabama and Florida.
- Provide a user friendly and high quality automated record system to expedite client intake procedures, improve referral accuracy, increase case management and administrative tools, facilitate reporting on demographic trends and service utilization patterns for households currently experiencing or about to experience homelessness, and support the collection of quality information to inform program improvement and service-planning.
- Meet the reporting requirements of the U.S. Department of Housing and Urban Development (HUD) and the Federal Partners.

In compliance with all state and federal requirements regarding client 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. HOUSING FIRST administers the **PromisSE** through a contract with the AL-501 Homeless Coalition of The Alabama Gulf Coast Continuum of Care ("AL-501 CoC").

II. HOUSING FIRST Responsibilities

1. HOUSING FIRST will provide the Agency 24-hour access to the **PromisSE**. The **PromisSE** is accessed via an internet connection, for which the Agency is responsible for maintaining.
2. HOUSING FIRST will provide required documents, including the AL-501 CoC Privacy Notice to Clients, the AL-501 CoC Privacy Policy, and the AL-501 CoC HMIS Client Release of Information and Sharing Plan ("ROI" or "Sharing Plan") for adoption by the participating Agency.
3. HOUSING FIRST will provide initial training and periodic updates to that training for Agency staff regarding the use of the **PromisSE**.
4. HOUSING FIRST will provide basic user support and technical assistance. Access to this basic technical assistance will normally be available from 8:30 a.m. to 4:30 p.m. on Monday through Friday (with the exclusion of holidays) and limited availability after regular hours.
5. HOUSING FIRST will not publish reports including client data that identifies specific agencies or persons without prior Agency permission or client permission, if applicable. Public reports otherwise published will be limited to the presentation of aggregated data that does not disclose personal identifying information.

III. AGENCY Responsibilities

1. The Agency will comply with the AL-501 Homeless Coalition of The Alabama Gulf Coast Continuum of Care Homeless Management Information System Operating Policies and Procedures (“AL-501 CoC HMIS Operating Policies and Procedures”).
2. The Agency will designate and staff one HMIS Agency Administrator, who shall abide by the policies and procedures set out in the AL-501CoC HMIS Operating Policies & Procedures.
3. The Agency will designate and staff one HMIS Security Officer, who shall abide by the policies and procedures set out in the AL-501 CoC HMIS Operating Policies & Procedures.
4. The Agency will ensure that both initial training and periodic updates to that training for Agency staff regarding the use of the **PromisSE** is completed in accordance with the requirements set out in the AL-501 CoC HMIS Operating Policies & Procedures.

IV. Privacy and Confidentiality

A. Protection of Client Privacy

1. The Agency will comply with all applicable federal and state laws regarding protection of client privacy.
2. 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. Agencies shall recognize that federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.
3. 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, if it meets the definition of a covered entity under the act.
4. The Agency will comply with all policies and procedures established by HOUSING FIRST pertaining to protection of client privacy.
5. Each Agency will abide specifically by its respective state law, 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.

B. Client Confidentiality

1. The Agency agrees to provide a copy of the AL-501 CoC Privacy Notice to Clients to any client making request and post a copy on the Agency website. The Agency will provide a verbal explanation of the **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).
2. 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.
3. The Agency will not divulge any confidential information received from the **PromisSE** to any organization or individual without proper written consent by the client, unless otherwise permitted by applicable regulations or laws.
4. The Agency will ensure that all persons who are issued a license through the AL-501 CoC End User License Agreement & Statement of Confidentiality and access to the **PromisSE** (“End User”), abide by the said Participation Agreement, including all associated confidentiality provisions. The Agency will be responsible for oversight of its own related confidentiality requirements.

APPENDIX A

5. The Agency agrees that it will ensure that all persons issued an End User license complete formal training on privacy and confidentiality, demonstrate mastery of the information, complete the End User Certification Test, and sign the AL-501 CoC End User License Agreement & Statement of Confidentiality, prior to activation of the End User license.
6. 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.

C. Interagency Sharing of Information

1. The Agency acknowledges that all forms provided by HOUSING FIRST 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 all forms provided by HOUSING FIRST to assure that they are in compliance with the laws, rules and regulations that govern its organization. Requests to modify the forms must be submitted to HOUSING FIRST for approval.
2. 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 ROI.
3. If the client has given approval through the completed ROI and Sharing Plan, the Agency may elect to share information with other participating agencies in **PromisSE**.
4. Agencies whose visibility is set to "closed" may not share "closed" client information without the client's written, informed consent, documented by the signed ROI.
5. Agencies who wish to share information with other Agencies participating in the PromisSE outside of the AL-501 CoC, must sign interagency agreements describing the PromisSE privacy rules the agencies are required to follow. The agreement must also acknowledge the agencies are prohibited from making further disclosure of the information shared, unless it is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by law.
6. The Agency acknowledges that the Agency itself bears primary responsibility for oversight of the sharing of all data it has collected via the **PromisSE**.
7. The Agency agrees to place all ROI forms related to the **PromisSE** in a file to be located at the Agency's business address, and that such forms will be made available to the HOUSING FIRST for periodic audits. The Agency will retain the forms for a period of seven (7) years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
8. The Agency acknowledges that clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.

D. Custody of Data

1. The Agency and HOUSING FIRST understand that the Agency and HOUSING FIRST are custodians, **not** owners of the data.
2. In the event that the **PromisSE** project ceases to exist, 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 by the centralized server will be purged or appropriately stored.
3. In the event that HOUSING FIRST ceases to exist, the custody of the data within the **PromisSE** associated with the AL-501 CoC will be transferred to another authorized organization for continuing administration, and all AL-501 **PromisSE** participating Agencies will be informed in a timely manner.

APPENDIX A

V. Data Entry and Regular Use of *PromisSE*

1. The Agency will not permit usernames and passwords to be shared among End Users.
2. If a client has previously given the Agency permission to share information, and then chooses to revoke that permission with regard to one or more of these agencies, the Agency will contact HOUSING FIRST in writing to request update to the client's visibility settings. HOUSING FIRST will then "lock" those portions of the record impacted by the revocation to the other agency or agencies.
3. 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.
4. The Agency will enter all Universal Data Elements and additionally required data elements as mandated by the funder or program.
5. The Agency will enter data in a consistent manner and will strive for real-time, or close to real-time, data entry. 100% of collected client level data will be entered within 48 hours of data collection
6. The Agency will routinely review records it has entered in the *PromisSE* for completeness and data accuracy. The review and data correction process will be made according to the AL-501 CoC HMIS Operating Policies & Procedures.
7. The Agency acknowledges that once the ROI expires, it is the Agency's responsibility to obtain an updated ROI. End Users must notify HOUSING FIRST's System Administrator in writing of an ROI's expiration within 48 hours, so that the client record can be "closed," unless the client signs a new ROI. If the End User is unable to contact the client to sign a new ROI, or if the client refuses to sign a new ROI, then the client's record will be "closed."
8. The Agency is required to adopt the AL-501 CoC Client Release of Information and Sharing Plan. Requests to modify the ROI must be submitted to HOUSING FIRST for approval.
9. The Agency will prohibit anyone with an Agency-assigned End User license from entering offensive language, profanity, or discriminatory comments based on race, color, religion, creed, national origin, ancestry, handicap, socioeconomic status, marital status, age, gender, and/or sexual orientation.
10. The Agency will utilize the *PromisSE* for business purposes only.
11. The Agency will keep updated virus protection software on Agency computers that access the *PromisSE*.
12. Transmission of material in violation of any United States Federal or state regulations is prohibited.
13. The Agency will not use the *PromisSE* with intent to defraud the federal, state, or local governments, or an individual entity, or to conduct any illegal activity.
14. The Agency agrees that the *PromisSE* Implementation, or the AL-501 CoC HMIS 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 attend End User meetings.
15. 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 HOUSING FIRST publishes from time to time.

VI. Publication of Reports

1. The Agency agrees that it may release only de-identified (anonymous) information generated by the *PromisSE* that is specific to its own services.

VII. Database Integrity

1. The Agency will not share assigned usernames and passwords to access the *PromisSE* with any other organization, governmental entity, business, or individual.

APPENDIX A

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

VIII. HMIS Contract Agreement Policy

1. HOUSING FIRST has adopted the AL-501 CoC HMIS Contract Agreement Policy for all participating Agencies.
2. HOUSING FIRST, as the Continuum Designated HMIS Lead Agency, will provide the specified amount of End User licensing, training, technical assistance, and other services or activities relevant to the participation in **PromisSE** as listed in the HMIS Contract Agreement Policy.
3. The Agency will remunerate HOUSING FIRST per End User for missed training and per End User for reactivation of an inactive license, as set out in the HMIS Contract Agreement Policy.

VIII. Hold Harmless

1. HOUSING FIRST makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold HOUSING FIRST 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 HOUSING FIRST harmless for loss or damage resulting in the loss of data due to delays, nondeliveries, mis-deliveries, or service interruption caused by Bowman Systems, by the Agency's or other Agencies' negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. HOUSING FIRST 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 HOUSING FIRST. HOUSING FIRST agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of HOUSING FIRST.
2. 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.

X. Terms and Conditions

1. The parties hereto agree that this Participation 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.
2. The Agency shall not transfer or assign any rights or obligations under the Participation Agreement without the written consent of HOUSING FIRST.
3. 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** HMIS Lead Agency's System Administrator or the Continuum Designated HMIS Lead Agency's System Administrator may immediately suspend access to **PromisSE** until the allegations are resolved in order to protect the integrity of the System.
4. This agreement may be modified or amended by written agreement executed by both parties with 30 days advance written notice.

APPENDIX A

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

Agency Name

Agency Name

Telephone Number

Agency Telephone Number

Representative Printed Name

Agency Rep Printed Name

Representative Title

Agency Representative Title

HOUSING FIRST, INC. Representative Signature

Agency Representative Signature

Date (mm/dd/yy)

Date (mm/dd/yy)

**AL-501 Homeless Coalition of The Alabama Gulf Coast Continuum of Care
PromisSE ASSURANCE**

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

- ✓ The Agency's Privacy Notice to Clients for **PromisSE** clients.
- ✓ Executed AL-501 CoC Client Release of Information and Sharing Plan forms.
- ✓ Executed interagency agreements for releases of information as needed.
- ✓ Certificates of Completion for required training for all **PromisSE** System End Users.
- ✓ A fully executed AL-501 CoC End User License Agreement & Statement of Confidentiality for all **PromisSE** System End Users.
- ✓ Current AL-501 CoC HMIS Operating Policies and Procedures.

By: _____

Title: _____

Signature: _____

Date: _____

APPENDIX B

AL-501 CoC Agency Administrator Agreement

Name: _____

Agency Name: _____

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:

- Completing, at a minimum, initial HMIS training and Advanced Reporting Tool training if the Agency holds an HMIS reporting license.
- Ensuring all Agency End Users have a signed AL-501 CoC End User License Agreement & Statement of Confidentiality on file.
- Ensuring all End Users complete the annual End User Certification Test, to include Privacy and Security Training.
- Ensuring all End Users complete workflow training and related updates, and have documentation of training.
- Ensuring the Agency is in compliance with the Data Security Standards listed in the AL-501 CoC HMIS Operating Policies and Procedures.
- Ensuring the Agency is in compliance with the AL-501 CoC HMIS Operating Policies and Procedures, completes the AL-501 CoC HMIS Policies and Procedures Compliance Checklist, and returns it to the Continuum Designated HMIS Lead Agency's System Administrator.
- Ensuring all End Users have successfully cleared a criminal background check. The Agency Administrator certifies successful clearance by completing the AL-501 CoC HMIS Criminal Background Check Certification form, and submitting it to the Continuum Designated HMIS Lead Agency's System Administrator, which is required prior to gaining access to the HMIS.

The original AL-501 CoC Agency Administrator Agreement shall be kept on file at the Agency, and all subsequent Agreements shall be kept on file at the Agency for a minimum of five (5) years.

Housing First, Inc. makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold Housing First 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 Housing First harmless for loss or damage resulting in the loss of data due to delays, nondeliveries, mis-deliveries, or service interruption caused by Bowman Systems; by the Agency's or other Participating Agencies' negligence or errors or omissions; as well as natural disasters, technological difficulties, and/ or acts of God. Housing First 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 Housing First. Housing First agrees to hold the Agency harmless from any damages, liabilities, claims, or expenses caused solely by the negligence or misconduct of Housing First.

The AL-501 CoC Agency Administrator Agreement is in effect for a period of one (1) year from the date of signing. Agency Administrators are required to complete the End User Certification Test with a score of 90% or better, and document compliance monitoring annually, at which time a new agreement will be provided. Failure to comply with the provisions of this Agreement is grounds for termination or suspension of your ServicePoint license and access to ServicePoint. Failure to comply with the provisions of this Agreement may additionally result in termination or suspension of the Agency's AL-501 CoC Participation Agreement. Your signature below indicates your agreement to comply with the AL-501 CoC Agency Administrator Agreement.

Employee Printed Name

Agency Official Printed Name

Employee Signature

Agency Official Signature

Date (mm/dd/yy)

Date (mm/dd/yy)

Updated 9/2016

APPENDIX C

AL-501 CoC Agency Security Officer Agreement

Name: _____

Agency Name: _____

All HMIS Participating Agencies must designate and staff one HMIS Agency Security Officer. The Agency Security Officer requirements and responsibilities include, but are not limited to, the following:

- Ensuring Agency computers connected to the HMIS are automatically updated on a regular basis, have current antivirus software, and firewall protection.
- Ensuring all Agency HMIS End Users complete annual Privacy and Security Training. Training must be provided by the Continuum Designated HMIS Lead Agency and based on the Privacy and Security Plan.
- Conducting an annual security review of the Agency that includes reviewing compliance with the Privacy and Security Plan. The Agency must document the findings of the review on the AL-501 CoC Privacy and Security Checklist. The Agency must submit the findings to the Continuum Designated HMIS Lead Agency's System Administrator no later than December 31st of each year.
- Notifying the Continuum Designated HMIS Lead Agency's System Administrator when an End User leaves the organization or when revision of the End User's access level is needed because of a change in job responsibilities. The notification must be made within 24 hours of the change.
- Reporting any security or privacy incidents to the Continuum Designated HMIS Lead Agency's System Administrator. 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 End Users involved violated privacy or security guidelines, the System Administrator will report the breach to the chair of the AL-501 CoC Board of Directors and the CEO of Housing First. A Corrective Action Plan will be implemented, which must include supervision and the retraining of the offending party, at minimum. It may also include the removal of HMIS End User licenses, client notification, and/or appropriate legal action. The Continuum Designated HMIS Lead Agency may request, or independently order an updated criminal background check on any End User suspected of violating one or more of the standards or requirements outlined in the AL-501 CoC HMIS Operating Policies and Procedures and the AL-501 CoC End User License Agreement & Statement of Confidentiality.

The original AL-501 CoC Agency Security Officer Agreement shall be kept on file at the Agency, and all subsequent Agreements shall be kept on file at the Agency for a minimum of five (5) years.

Housing First, Inc. makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold Housing First 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 Housing First harmless for loss or damage resulting in the loss of data due to delays, nondeliveries, mis-deliveries, or service interruption caused by Bowman Systems; by the Agency's or other Participating Agencies' negligence or errors or omissions; as well as natural disasters, technological difficulties, and/ or acts of God. Housing First 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 Housing First. Housing First agrees to hold the Agency harmless from any damages, liabilities, claims, or expenses caused solely by the negligence or misconduct of Housing First.

The AL-501 CoC Agency Security Officer Agreement is in effect for a period of one (1) year from the date of signing. Security Officers are required to complete the End User Certification Test and document compliance monitoring annually, at which time a new agreement will be provided. Failure to comply with the provisions of this Agreement is grounds for termination or suspension of your ServicePoint license

Updated 9/2016

APPENDIX C

and access to ServicePoint. Failure to comply with the provisions of this Agreement may additionally result in termination or suspension of the Agency's AL-501 CoC Participation Agreement. Your signature below indicates your agreement to comply with the AL-501 CoC Agency 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

AL-501 CoC HMIS Operating Policies and Procedures
Compliance Checklist

Agency Name: _____

- _____ (Int.) Agency has received a copy of the AL-501 CoC HMIS Operating Policies and Procedures.
- _____ (Int.) Agency has a fully executed the AL-501 CoC Participation Agreement (Appendix A).
- _____ (Int.) Agency has adopted the AL-501 CoC Privacy Notice to Clients (Appendix I), governing HMIS privacy and security standards, which has been approved by its board of directors.
- _____ (Int.) Agency has assigned an HMIS Agency Administrator and executed the AL-501 CoC Agency Administrator Agreement (Appendix B).
- _____ (Int.) Agency has assigned an HMIS Agency Security Officer and executed the AL-501 CoC Agency Security Officer Agreement (Appendix C).
- _____ (Int.) Agency has certified all End Users have successfully cleared criminal background checks according to the AL-501 CoC HMIS Operating Policies and Procedures, and submitted the AL-501 CoC HMIS Criminal Background Check Certification forms (Appendix S) to Housing First's System Administrator.
- _____ (Int.) Agency has provided End Users with the HUD Data Elements.
- _____ (Int.) End Users have been trained on the HUD definition of homelessness and the priority of homelessness documentation.
- _____ (Int.) Agency and End Users understand and will comply with the Data Quality Plan detailed in the AL-501 CoC HMIS Operating Policies and Procedures.

Agency Official Printed Name

CoC Official Printed Name

Agency Official Signature

CoC Official Signature

Date (mm/dd/yy)

Date (mm/dd/yy)

AL-501 CoC Privacy and Security Checklist

Agency Name: _____

Security Officer Name: _____

____ (Int.) **Public Notice is posted in an area visible to clients.**

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

____ (Int.) **AL-501 CoC Privacy Notice to Clients is adopted and available to clients.**

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

____ (Int.) **Agency has a copy of the Public Notice and the AL-501 CoC Privacy Notice to Clients on its website.**

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

APPENDIX E

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

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

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

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

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

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

APPENDIX E

_____ (Int.) **Agency has adopted the AL-501 CoC Client Release of Information and Sharing Plan and requests this from every client.**

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

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

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

_____ (Int.) **Usernames and passwords are not shared between End Users, or left visible for others to see.**

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

APPENDIX E

_____ (Int.) **End Users are prohibited from transferring HMIS data onto Portable Storage Devices (e.g. USB drives, recordable discs, external hard disks, etc.)**

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

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

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

_____ (Int.) **All HMIS workstations, including laptops and remote workstations, are protected by a firewall.**

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

APPENDIX E

_____ (Int.) **End Users are not accessing the HMIS on a public computer, or from an internet connection that is not secured. End Users are not using public Wi-Fi to access the HMIS, including that provided by internet cafes, libraries, airports or other non-secure internet connections.**

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

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

Finding(s):

Corrective Action(s):

Deadline for Completion: _____

By signing below, you certify the Agency has met all of the requirements for compliance with the AL-501 CoC HMIS Operating Policies and Procedures and the Privacy and Security Plan. Failure to report compliance concerns or findings to the Continuum Designated Lead Agency's System Administrator is grounds for revocation of Security Officer status and termination or suspension of the End User's ServicePoint license, and may additionally result in termination or suspension of the Agency's AL-501 CoC Participation Agreement.

Security Officer Printed Name

Agency Official Printed Name

Security Officer Signature

Agency Official Signature

Date

Date

Updated 9/2016

AL-501 CoC End User License Agreement & Statement of Confidentiality

Name: _____

Employees, volunteers, staff and any persons with access to the Program Management Information System of the Southeast ("PromisSE" or "HMIS" or "ServicePoint") are subject to certain guidelines regarding its use. The HMIS 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 the HMIS include, but are not limited to, the following:

Consent & Confidentiality Standards:

- Current client or legal guardian consent, as documented by the AL-501 CoC Client Release of Information and Sharing Plan ("ROI" or "Sharing Plan"), is required before entering, updating, editing, printing, or disclosing basic identifying and non-confidential service transactions/information with other Agencies participating in the HMIS ("Participating Agencies") and/or their employees, volunteers and/or staff. Otherwise, limited visibility must be coordinated with Housing First, Inc.
- Outreach staff gathering information in the field, prior to execution of an ROI, must provide the client with the AL-501 CoC Outreach Privacy Notice (Appendix Q) and sign the AL-501 CoC Outreach Consent Certification (Appendix R), affirming receipt of the client's verbal consent before entering, updating, editing, printing, or disclosing their Basic Information (name, date of birth, social security number, program enrollments, case managers, military background/veteran status, and photo). Otherwise, limited visibility must be coordinated with Housing First. Detailed Information, as indicated in the AL-501 CoC Sharing Plan, may not be entered into the HMIS prior to execution of the ROI.
- Only general, non-confidential information is to be entered in the "Client Notes" section of the Client Profile in ServicePoint. Confidential information, including TB diagnosis, domestic violence, drug/alcohol abuse, communicable diseases and mental/physical health information shall not be entered in this section.
- Confidential information obtained via the HMIS is to remain confidential, regardless of the End User's relationship with the Agency or usage of the HMIS.

Privacy Standards:

- Visibility of client records **shall not** be modified by the End User. If a client, or legal guardian of a client, chooses to rescind the ROI, the End User must notify Housing First to request appropriate changes to the visibility of the record(s).
- End Users entering data related to an individual with increased privacy risks, such as victims of domestic violence, dating violence, sexual assault, or stalking must notify Housing First within 24 hours of data entry to request a "lock" for the record(s).
- End Users do not discuss client information in the presence of others without a need to know.
- End Users remove unique client identifiers before releasing data to the public.
- End Users ensure hard copy data is kept in a locked in a drawer/file cabinet and is not visible to unauthorized individuals. Offices that contain files are locked when not occupied.
- End User accounts and passwords are not shared between End Users, or left visible for others to see.

Data Security Standards:

- All devices accessing the HMIS must have current antivirus software with automatic updates, protection by a firewall, and must be password protected and in a secured location.
- End Users must log out of the HMIS and their computer when leaving the workstation. Failure to log out appropriately may result in a breach in client confidentiality and system security.
- After a short period of time a password protected screen saver will be activated during the time the computer is not in use.
- End Users are prohibited from accessing the HMIS from a computer that is available to the public **or** through an internet connection that is not secure. End Users are not permitted to use public Wi-Fi to access the HMIS, including that provided by internet cafes, libraries, airports or other non-secure internet connections.

APPENDIX F

- Agencies must have a plan for remote access if End Users access ServicePoint outside of the office, such as accessing ServicePoint from home or in the field. The remote computer and environment for data entry must meet the same security requirements as those office HMIS workstations, and downloads from ServicePoint may not include client identifying information.
- End Users are prohibited from transferring HMIS data to Portable Storage Devices, including small plug-and-play devices such as USB drives, recordable discs, and external hard disks.

Workflow Requirements:

- End Users performing data entry follow the most recent version of their program's workflow.
- End Users perform live data entry as the primary method of client-level data entry. If data collection is done via paper forms, the program is responsible for ensuring all data collection forms align with the workflow, HMIS minimum requirements, and funder requirements (if applicable).
- 100% of collected client level data is entered within 48 hours of data collection.
- Client records are updated annually, at minimum, by emergency shelters. All other program types are required to update client records on a quarterly basis via Interim Updates and annually via an Annual Assessment. All Annual Assessments must be completed within 30 days +/- of the anniversary date of the client's entry into the program for a client enrolled for 365 days or more.
- End Users must notify the Continuum Designated HMIS Lead Agency's System Administrator of an ROI's expiration within 48 hours, so that the client record can be "closed," unless the client signs a new ROI.

Initial & Annual End User Requirements:

- Prospective End Users must participate in initial HMIS training, which includes a privacy and security module, must successfully complete of the End User Certification Test (90% score or better), and submit the AL-501 CoC End User License Agreement & Statement of Confidentiality to obtain HMIS licensure. Training must be conducted by Housing First.
- End Users are required to log into ServicePoint within one week of receipt of End User credentials.
- End Users must complete annual Privacy and Security Training. Training must be conducted by Housing First.
- End Users must successfully complete the End User Certification Test annually to maintain HMIS licensure.
- End Users must participate in ongoing workflow and update training for their assigned workflows.
- End Users with the assigned user level of "Agency Administrator" are required to log in at least monthly to ServicePoint.
- End Users with the assigned user level "Case Manager I", "Case Manager II", "Case Manager III", or "System Administrator" are required to log in at least weekly to ServicePoint.

End User Ethical Standards:

- Misrepresentation of the client's current or former circumstances through the deliberate entry of inaccurate information is strictly prohibited. Violation of this requirement will result in immediate and permanent revocation of the End User's license, and access to the HMIS.
- 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 the HMIS. Profanity and offensive language **are not** permitted in the HMIS. Violation of this requirement will result in immediate and permanent revocation of the End User's license and access to the HMIS.
- Any unauthorized access or unauthorized modification to computer system information/the HMIS database or interference with normal system operations will result in immediate and permanent revocation of the End User's license and access to the HMIS, and may jeopardize the End User's employment status with the Agency.
- The HMIS is to be used for business purposes only. Transmission of material in violation of any U.S. 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. The HMIS **shall not** be used to defraud the federal, state, or local governments, nor any individual entity, nor to conduct any illegal activity. Violation of this requirement will result in immediate and permanent revocation of the End User's license and access to the HMIS, at minimum. Housing First will notify appropriate legal entity(s) in cases of suspected or verified illegal activity.

Updated 12/2016

APPENDIX F

The original AL-501 CoC End User License Agreement & Statement of Confidentiality shall be kept on file at the Agency, and all subsequent Agreements shall be kept on file at the Agency for a minimum of five (5) years.

Housing First, Inc. makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold Housing First 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 HMIS; 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 Housing First harmless for loss or damage resulting in the loss of data due to delays, nondeliveries, mis-deliveries, or service interruption caused by Bowman Systems; by the Agency's or other Participating Agencies' negligence or errors or omissions; as well as natural disasters, technological difficulties, and/ or acts of God. Housing First 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 Housing First. Housing First agrees to hold the Agency harmless from any damages, liabilities, claims, or expenses caused solely by the negligence or misconduct of Housing First.

This agreement is in effect for a period of one (1) year from date of signing. End Users are required to complete the annual End User Certification Test with a score of 90% or better, at which time a new agreement will be provided. Failure to comply with the provisions of this Agreement may result in immediate termination or suspension of the End User's ServicePoint license and access to ServicePoint, and may also be grounds for immediate termination.

Your signature below indicates your agreement to comply with the AL-501 CoC End User License Agreement & Statement of Confidentiality and the requirements set forth in the AL-501 CoC HMIS Operating Policies & Procedures. Your signature also acknowledges you've received a copy of the AL-501 CoC Privacy Notice to Clients and will comply with its guidelines.

Employee Printed Name

Agency Administrator Printed Name

Employee Signature

Agency Administrator Signature

Date

Date

APPENDIX G

AL-501 CoC Client Release of Information and Sharing Plan

Agency Authorized to Share: _____

This Agency collects information about people who apply for services. When we meet with you, we will ask you information about you and your household. We will put the information into a computer system called the Program Management Information System of the Southeast (“PromisSE” or “HMIS”). The information that we collect allows us to work with other Participating Agencies (agencies that use the HMIS) in Alabama and Florida to help you, to coordinate your case management, and to reduce the number of times that you have to re-tell your story or repeat your information.

Choose ONE of the following sharing options by initialing next to your choice:

Option 1:

This option allows the most information sharing, and therefore the most coordination of services and the least duplication of efforts in order to serve you.

- Your **basic information** will be shared with all agencies using the HMIS. Basic Information includes your name, date of birth, social security number, program enrollments, case managers, military background (veteran status) and photo.
- Your **detailed information** will be shared with agencies in Mobile and Baldwin counties, and includes the other information that you choose to share with us, including your healthcare and drug treatment information.

Please see the AL-501 CoC Sharing Plan (or “Sharing Plan”) for a complete list of the information shared, and the local agencies with which it is shared. The agencies who participate in the Sharing Plan may change from time to time, but you can always obtain the most recent copy of the Sharing Plan from the Agency upon request.

_____ I authorize the Agency to share my Basic Information among all Participating Agencies, and to share my Detailed Information with local agencies.

Option 2:

Under this option, **only** the Participating Agencies that you list below will be able to see your Detailed Information, including your healthcare and drug treatment information.

_____ I authorize the Agency to share my Detailed Information with **ONLY** the following Agency(s):

APPENDIX G

Option 3:
Under this option, your information will not be shared, and you will not be denied access to services because you choose not to share.
_____ I do not authorize the Agency to share my information.

Notice Regarding Disclosure of Healthcare and Drug Treatment Information

If you choose to share your information under Option 1 or Option 2 of this release, the shared information may include information about your physical and mental health, communicable diseases and venereal diseases such as, hepatitis, syphilis, gonorrhea, tuberculosis, HIV/AIDS, and your drug and/or alcohol abuse and treatment history. If you do not wish to share this information, you should choose Option 3, which states "I do not authorize the Agency to share my information." If you choose to authorize sharing, we will only share your healthcare and drug treatment information according to the sharing option that you choose on this form.

I understand that this Release will remain in effect for five (5) years, after which, I will need to sign a new release if I wish to continue sharing my information. I can revoke this release at any time before it expires by notifying the Agency in writing. I understand that I can refuse to provide any information that is requested from me and that I will not be denied services based on my refusal to answer a question, unless the answer is necessary to determine if I am eligible for the service(s). I have had an opportunity to ask questions about *HMIS*, and I may review a copy the AL-501 CoC Privacy Policy, AL-501 CoC Privacy Notice to Clients, and the Sharing Plan upon my request. No one has offered me anything in exchange for signing this document. I have read it, I understand it, and I sign it under my own free will.

Client Printed Name

Client Date of Birth

Client Signature

Client Social Security Number

Date

Please list authorized dependents included in the sharing option chosen above.
You may use the back of this page if you need additional space.

Dependent Name

Dependent Date of Birth

Dependent Name

Dependent Date of Birth

Dependent Name

Dependent Date of Birth

APPENDIX G

AL-501 CoC Sharing Plan

- 1) **Option 1:** If you choose this option, your Basic and Detailed Information will be shared as follows:
- A. **Basic Information** - The following information will be shared with Participating Agencies in Alabama and Florida.
 - a. Name
 - b. Date of Birth
 - c. Social Security Number
 - d. Program enrollments
 - e. Case Manager(s)
 - f. Military background (veteran status)
 - g. Photo
 - B. **Detailed Information** – In addition to the Basic Information listed above, the information below is considered Detailed Information, which will be shared with Agencies located within Mobile and Baldwin counties.
 - a. Case Plan (goals, action steps, and case notes)
 - b. Communicable and venereal diseases (hepatitis, syphilis, gonorrhea, tuberculosis, HIV/AIDS)
 - c. Demographic information (race, gender, and ethnicity)
 - d. Disability information (including chronic health condition(s), developmental, drug and/or alcohol abuse, HIV/AIDS, physical and mental health)
 - e. Drug and/or alcohol abuse and treatment history
 - f. Educational attainment
 - g. Employment history
 - h. Health Insurance (sources)
 - i. Household members
 - j. Incidents and Bans
 - k. Income (amounts and sources) and non-cash benefits (amounts and sources)
 - l. Living situation, housing history, and circumstances of need
 - m. Risk factors
 - n. Services (requested and received) and Referrals
- 2) **Option 2:** If you choose this option, then your Detailed Information will only be shared with the Participating Agencies you list in the ROI or check below.
- 3) **Option 3:** If you choose this option, none of your data will be shared.

Participating Agencies:

- | | |
|---|--|
| <input type="checkbox"/> AltaPointe Health Systems | <input type="checkbox"/> Mobile Area Interfaith Conference |
| <input type="checkbox"/> Sybil Smith Family Village | <input type="checkbox"/> McKemie Place |
| <input type="checkbox"/> Family Promise of Mobile | <input type="checkbox"/> Salvation Army of Coastal Alabama |
| <input type="checkbox"/> Franklin Primary Health Center | <input type="checkbox"/> Volunteers of America Southeast |
| <input type="checkbox"/> Front Porch Ministries | <input type="checkbox"/> Waterfront Rescue Mission |
| <input type="checkbox"/> Housing First, Inc. | |

AL-501 CoC Public Notice

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 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. A copy of our Privacy Notice describing our privacy practice is available to all clients upon request.

AL-501 CoC Privacy Notice to Clients

Version 2

AL-501 CoC Privacy Notice to Clients

Version 2

Notice Summary

The AL-501 CoC Privacy Notice to Clients describes the privacy policy and practices of Housing First, Inc. We may amend this policy over time. We collect personal information only when appropriate. We may use or disclose your information to provide you with services. We may also use or disclose it to comply with legal and other obligations. You can inspect personal information about you that we maintain. You can also ask us to correct inaccurate or incomplete information. You can ask us about our privacy policy or practices. We respond to questions and complaints. Read the full notice for more details. Anyone can have a copy of this notice upon request.

Brief Summary

This Agency collects information about people who apply for services. When we meet with you, we will ask you information about you and your household. We will put the information into a computer system called the Program Management Information System of the Southeast (“PromisSE” or “HMIS” or “System”). The HMIS is used to collect client-level data, and data on the provision of housing and services to homeless individuals, families, and persons at risk of homelessness. The HMIS complies with the U.S. Department of Housing and Urban Development’s (“HUD”) data collection, management, and reporting standards. The information that we collect allows us to work with other Agencies to help you, to coordinate your case management, and to reduce the number of times that you have to re-tell your story or repeat your information.

Confidentiality Rights

Each Participating Agency (agencies using the HMIS) is required to have a privacy policy that has been approved by its board of directors. Housing First operates the HMIS in accordance with HUD confidentiality regulations, including those covering programs that receive HUD funding for homeless services (Federal Register/Vol. 69, No. 146). Agencies covered under the Health Insurance Portability and Accountability Act (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, must notify Housing First’s System Administrator of their HIPAA status to allow Housing First to handle their client data in compliance with HIPAA. Other rules that may also apply include 42 CFR Part 2 governing drug and alcohol records.

Effective Date: The AL-501 CoC Privacy Notice to Clients governs the privacy of information received on or after January 1, 2017. Information received or entered prior to the effective date is governed under the preceding Privacy Notice.

AL-501 CoC Privacy Notice to Clients

Full Notice

Version 2

A. What This Notice Covers

1. This notice describes the privacy policy and practices of Housing First, Inc., which is the Continuum Designated HMIS Lead Agency for the AL-501 Homeless Coalition of The Alabama Gulf Coast Continuum of Care (AL-501 CoC). Additional information about Housing First may be found at www.hfal.org.
2. The policy and practices in this notice cover the processing of protected personal information for clients of the Continuum Designated Lead Agency or the Agency, and how the information is used and disclosed.
3. Protected Personal Information (PPI) is any information we maintain about a client that:
 - a. allows identification of an individual directly or indirectly
 - b. can be manipulated by a reasonably foreseeable method to identify a specific individual, **or**
 - c. can be linked with other available information to identify a specific client. When this notice refers to personal information, it means PPI.
4. We adopted this policy because of standards for Homeless Management Information Systems issued by HUD. We intend our policy and practices to be consistent with those standards. See 69 Federal Register 45888 (July 30, 2004).
5. This notice tells our clients, our staff, and others how we process personal information. We follow the policy and practices described in this notice.
6. We give a written copy of this privacy notice to any individual who asks.
7. We maintain a copy of this policy on our website at www.hfal.org/services/hmis-department/policy-and-procedures/.

Notice Amendment Process

PRIVACY NOTICE AMENDMENTS: The policies and practices covered under the AL-501 CoC Privacy Notice to Clients may be amended over time and those amendments may affect information obtained by the Agency before the date of the change. All amendments to this notice must be consistent with the requirements of the federal standards that protect the privacy of clients and guide the HMIS implementation and operation.

B. How and Why We Collect Personal Information

We may collect Personal Protected Information only when appropriate to the purposes for which the information is obtained or when required by law. We collect PPI by lawful and fair means and with your knowledge or consent.

1. We may collect information for these purposes:
 - a. To provide or coordinate services for you;
 - b. to locate other programs that may be able to assist you;
 - c. for functions related to payment or reimbursement from others;
 - d. to operate our organization, including administrative functions such as legal, audits, personnel, oversight, and management functions;
 - e. to comply with government reporting obligations when required by law;
 - f. when required by law.
2. We may also get information about you from other Agencies if you've given them written consent to share your information.
3. We post a written notice where Protected Personal Information is collected. The notice reads:

"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. A copy of our Privacy Notice is available to all clients upon request.”

4. This notice will be explained in cases where the client is unable to read and/or understand it.

C. How We Use and Disclose Personal Information

1. We can only use or disclose Personal Protected Information from the HMIS for the following activities:
 - a. To **provide or coordinate services** for you;
 - b. for functions related to **payment or reimbursement for services**;
 - c. to **carry out administrative functions** such as legal, audits, personnel, oversight, and management functions;
 - d. to **create de-identified (anonymous) information** that can be used for reporting, research, and statistical purposes without identifying clients;
 - e. for **contractual research purposes** where privacy conditions are met (including a written agreement);
 - f. **when required by law** to the extent that use or disclosure complies with and is limited to the requirements of the law;
 - g. to **avert a serious threat to health or safety** if:
 - i. we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, **and**
 - ii. the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat;
 - h. to comply with **government reporting obligations** for the HMIS and for oversight of compliance with HMIS requirements;
 - i. to **report criminal activity** on Agency premises.

D. Limited Information Sharing

We require you to sign the AL-501 CoC Client Release of Information and Sharing Plan (“ROI” or “Sharing Plan”), which provides notice of how your personal information is used within the HMIS, and requires your consent on how your personal information is shared and the Participating Agencies with which it is shared. Please request a copy of the Sharing Plan to see a complete list of agencies with which you may share information. Although the agencies who participate in the Sharing Plan may change from time to time, you may always ask for the most recent copy of the Sharing Plan from this Agency.

The limited sharing model we use is outlined below, and offers three (3) different sharing options.

Limited Sharing Model:

1. **Option 1** - This option allows the most information sharing, and therefore the most coordination of services and the least duplication of efforts in order to serve you. The information below will be shared as follows:
 - a. **Basic Information** – This information will be shared with Participating Agencies in Alabama and Florida. Your Basic Information includes the following: your name, date of birth, social security number, program enrollments, case managers, military background (veteran status), and photo.
 - b. **Detailed Information** – This information will only be shared with local agencies in Mobile and Baldwin counties. Please ask for a copy of the Sharing Plan to see a complete list of these agencies. Your Detailed Information is listed in the AL-501 CoC Sharing Plan, and includes the following: case plan(s), including goals, action steps, and case notes; communicable and venereal diseases (e.g. hepatitis, syphilis, gonorrhea, tuberculosis, HIV/AIDS); disability

information, including chronic health condition(s), developmental, HIV/AIDS, physical and mental health; drug and/or alcohol abuse and treatment history; educational attainment; employment history; ethnicity; gender; health insurance (sources); household members; incidents and bans; income and non-cash benefits (amounts and sources); living situation, housing history, and circumstances of need; race; risk factors; services (requested and received) and referrals.

2. **Option 2** - Under this option, **only** the agencies that you specify will be able to see your Detailed Information, including your healthcare and drug treatment information.
3. **Option 3** - Under this option, your information **will not** be shared, and you **will not** be denied access to services because you choose not to share your information.

A client's Basic Information (name, date of birth, social security number, program enrollments, case managers, military background/veteran status) collected in the field by outreach workers may be entered into the HMIS prior to the execution of a signed ROI. However, the outreach worker must provide the client with the AL-501 CoC Outreach Privacy Notice (Appendix Q) and sign the AL-501 CoC Outreach Consent Certification (Appendix R), affirming receipt of the client's verbal consent before entering, updating, editing, printing, or disclosing their Basic Information. Otherwise, limited visibility must be coordinated with Housing First. Detailed Information may not be entered into the HMIS prior to execution of the ROI.

E. Your Information Rights

1. All requests for personal information located within the HMIS need to be made to the Agency or organization that collected and entered or updated your information.
2. We may not disclose your Personal Protected Information located within the HMIS except as required by law, or to help the Participating Agency that collected/entered/updated the information operate the System.
3. We may not publish reports on your 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 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 Administrator(s) operating the HMIS database may see your information.

F. Benefits of HMIS and Agency Information Sharing

The information you provide to us can play an important role in our ability and the ability of other Agencies to provide the services that you and others in our community request. The benefits of HMIS and Agency information sharing are as follows:

1. Better demonstrate the need for services and the specific types of assistance needed in our area.
2. Obtain more money and resources to provide services.
3. Plan and deliver quality services to you and your household.
4. Assist the Agency to improve its work with households and individuals who are homeless.
5. Keep required statistics for local, state, and federal funders (such as HUD).

G. Risks in Sharing Information

While the HMIS is designed to promote better services for those who are homeless or might become homeless, there may be risks to individuals, especially vulnerable populations and/or individuals with increased privacy concerns (e.g. victims of domestic violence, dating violence, sexual assault and stalking), that lead them to take certain protectionary measures, which include:

- a. Request to close their record so that only the Agency(s) they name and the System Administrator(s) operating the HMIS will see their information. The Agency must notify the System Administrator at the Continuum Designated HMIS Lead Agency within 24 hours of inputting the client information into the System to close the record.
- b. Request to have their record marked as "inactive."

Updated 12/2016

- c. Request to have their record removed from the System.

H. Data Quality

1. We collect only PPI that is relevant to the purposes for which we plan to use it. To the extent necessary for those purposes, we seek to maintain only personal information that is accurate, complete, and timely.
2. ROI forms will be retained for a period of seven (7) years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
3. We may keep information for a longer period if required to do so by statute, regulation, contract, or other requirement.

I. How Your Information Will Be Kept Secure

Protecting the safety and privacy of individuals receiving services and the confidentiality of their records is very importance to us. Through training, policies and procedures, and software, we have taken steps to ensure your information is kept safe and secure, including:

1. All computers are updated regularly, and have current antivirus software with automatic updates.
2. Your name and other identifying information **will not** be contained in HMIS reports that are issued to local, state, or federal agencies.
3. Individuals receive training in privacy protection and agree to follow strict confidentiality standards before using the System.
4. Only licensed individuals are provided with a username and password to access the System, and their access level must be consistent with their job responsibilities and their business “need-to-know.”
5. Data transported over the internet is encrypted, which keeps information private during transmission.
6. Only connections from previously approved computers are allowed to access the HMIS, which is verified through a Public Key Infrastructure (PKI) Client Certificate. A PKI Client Certificate has been installed on each end user’s computer by the System Administrator before the end user can access the HMIS, which allows computers to securely exchange data, providing an additional layer of encryption.
7. The end user requirement of a username and password, in addition to the installation of the PKI Client Certificate on their computer, is known as Two Factor Authentication. Two Factor Authentication makes it harder for potential hackers to steal personal information.
8. The HMIS database lives on a server protected by a firewall, which is a device meant to keep hackers and viruses away from the server.
9. The HMIS database is stored on equipment that’s kept physically secure, which means only authorized personnel have access to it.
10. System Administrators employed by Housing First support the daily operation of the HMIS.

J. How to Inspect and Correct Personal Information

1. You may inspect and have a copy of your personal information that we maintain. We will offer to explain any information that you may not understand.
2. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
3. You may request to share your information with other organizations by completing the AL-501 CoC Client Release of Information and Sharing Plan. You may terminate or withdraw your request to share information by contacting us.
4. If another Agency collected, entered or updated the information you’re requesting, then you will need to contact that Agency to process your request.
5. We may deny your request for inspection or copying of personal information if:
 - a. the information was compiled in reasonable anticipation of litigation or comparable proceedings
 - b. the information about another individual other than the Agency staff would be disclosed
 - c. the information was obtained under a promise or confidentiality (other than a promise from a healthcare provider or homeless provider) and if the disclosure would reveal the source of the information, **or**
 - d. disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

6. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial.
7. We may reject repeated or harassing requests for access or correction.

K. Complaints and Accountability

1. We accept and consider questions or complaints about our privacy and security policies and practices.
2. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy notice. Each staff member must receive and acknowledge receipt of a copy of this privacy notice.

Complaint Procedures

Please feel free to contact us to file a grievance if you feel that your information rights have been violated. Please address your written communication to Eric B. Jefferson, Chief Executive Officer, Housing First, Inc. The mailing address is 273 Azalea Road, Building 3, Suite 110, Mobile, AL, 36609. Please include your contact information. We will respond in writing within seven (7) working days from the receipt of your letter.

L. Privacy Notice Change History

Change History

This is the Version 2 of our Privacy Notice to Clients, which is our first revision.

1. **Version 1 - June 2014. Initial Policy**
2. **Version 2 - September 2016. Updated – Added Notice Summary; labeled and updated Brief Summary; updated Confidentiality Rights; added “What this Notice Covers” section; added “How and Why We Collect Personal Information” section, which contains Public Notice illustrated in paragraph 3 on p. 2 of preceding Privacy Notice, and deleted sentence stating Agency owns HMIS records to correspond with Partnership Agreement stating Agency and Continuum Designated Lead Agency are custodians of the data; revised uses and disclosures, and renamed section “How We Use and Disclose Personal Information;” added “Limited Information Sharing” section to reflect amendments to the ROI and the addition of the Sharing Plan, added the verbal consent exception for outreach workers; revised “Benefits of HMIS and Agency Information Sharing” section in accordance with the Limited Sharing Model by omitting paragraph 2 on p. 6 of preceding Privacy Notice; revised “Risks to Sharing Information” section in accordance with the Limited Sharing Model and added the “vulnerable populations” language; added “Data Quality” section, including record keeping practices for ROIs; updated “How Your Information Will Be Kept Secure” section with encryption information, added the Public Key Infrastructure (PKI) Client Certificate and Two Factor Authentication information; added “How to Inspect and Correct Personal Information” section, and moved access and correction information at the end of p. 4 of the preceding Privacy Notice to this section; added “Complaint and Accountability” section, and moved complaint contact information in paragraph 2 on p. 5 of preceding Privacy Notice to this section.**

AL-501 CoC Privacy Policy
Version 2

REASONS FOR POLICY:

1. To protect the privacy of Agency clients
2. To comply with applicable laws and regulations
3. 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:

1) **Compliance:**

Housing First, Inc. operates the Homeless Management Information System (“HMIS” or “PromisSE” or “System”) in accordance with the U.S. Department of Housing and Urban Development’s (HUD) confidentiality regulations, including those covering programs that receive HUD funding for homeless services (Federal Register/Vol. 69, No. 146). Agencies covered under the Health Insurance Portability and Accountability Act (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, must notify Housing First’s System Administrator of their HIPAA status to allow Housing First to handle their client data in compliance with HIPAA. Other rules that may also apply include 42 CFR Part 2 governing drug and alcohol records.

NOTE: HIPAA statutes are more restrictive than the HMIS FR 4848-N-02 (Federal Register/Vol. 69, No. 146) standards and in cases where both apply, HIPAA overrides 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 to Clients which standards apply to their situation.

- 2) **Uses and Disclosures of Information:** Protected Personal Information or PPI (information which can be used to identify a specific client) can only be used for the following purposes:
- a. To **provide or coordinate services** for individuals;
 - b. for functions related to **payment or reimbursement for services;**
 - c. to **carry out administrative functions** such as legal, audits, personnel, oversight, and management functions;
 - d. to **create de-identified (anonymous) information** that can be used for reporting, research, and statistical purposes without identifying clients;
 - e. for **contractual research purposes** where privacy conditions are met (including a written agreement);
 - f. **when required by law** to the extent that use or disclosure complies with and is limited to the requirements of the law;
 - g. to **avert a serious threat to health or safety** if:
 - i. we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, **and**
 - ii. the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat;

- h. to comply with **government reporting obligations** for the HMIS and for oversight of compliance with HMIS requirements;
- i. to report criminal activity on Agency premises.

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

- a) PPI will be collected only for the purposes listed above.
- b) We may also get information about individuals from other Agencies the client provides the Agency with written consent to share their information.
- c) Clients will be made aware that personal information is being collected and recorded.
- d) A written notice will be posted in locations where PPI 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.”

- e) This notice will be explained in cases where the client is unable to read and/or understand it.

4) **Data Quality:** PPI data will be accurate, complete, timely, and relevant.

- a) All PPI collected will be relevant to the purposes for which it is to be used.
- b) Data will be entered in a consistent manner by authorized End Users.
- c) Data will be entered in as close to real-time data entry as possible, and 100% of collected client-level data will be entered within 48 hours of data collection.
- d) 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.
- e) Data quality is subject to routine audit by System Administrators who have administrative responsibilities for the database.

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

- a) The purposes, uses, disclosures, policies, and practices relative to PPI data are outlined in the AL-501 CoC Privacy Notice to Clients.
- b) The Privacy Notice will comply with all applicable regulatory and contractual limitations.
- c) The Privacy Notice will be made available to Agency clients, or their representative, upon request and explained/interpreted as needed.
- d) Reasonable accommodations will be made with regards to the Privacy Notice for persons with disabilities and non-English speaking clients as required by law.
- e) PPI will be used and disclosed only as specified in the Privacy Notice, and only for the purposes specified therein.
- f) Uses and disclosures not specified in the Privacy Notice can be made only with the consent of the client.
- g) The Privacy Notice will be posted on the Agency website.
- h) The Privacy Notice will be reviewed and amended as needed.
- i) Amendments to, or revisions of the Privacy Notice will address the retroactivity of any changes.
- j) Permanent documentation of all Privacy Notice amendments/revisions will be maintained.

- k) All access to, and editing of PPI data will be tracked by an automated audit trail, and will be monitored for violations use/disclosure limitations.
- 6) **Record Access and Correction:** Provisions will be maintained for the access to, and corrections of PPI records.
- a) Clients will be allowed to review their HMIS record within five (5) working days of a request to do so.
 - b) During a client review of their record, an Agency staff person must be available to explain any entries the client does not understand.
 - c) The client may request to have their record corrected so that information is up-to-date and accurate to ensure fairness in its use.
 - d) When a correction is requested by a client, the request will be documented and the staff will make a corrective entry if the request is valid.
 - e) A client may be denied access to their personal information for the following reasons:
 - i) the information was compiled in reasonable anticipation of litigation or comparable proceedings
 - ii) the information about another individual other than the Agency staff would be disclosed
 - iii) the information was obtained under a promise or confidentiality (other than a promise from a healthcare provider or homeless provider) and if the disclosure would reveal the source of the information, **or**
 - iv) disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.
 - f) 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.
 - g) 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, if they have been put at personal risk, or if they have been harmed.
 - h) Any client grievances relative to the HMIS will be processed and resolved according to the Agency's grievance policy.
 - i) A copy of any client grievance relative to HMIS data or other privacy/confidentiality issues, in addition to the Agency's response, will be forwarded to Housing First, Inc.
- 7) **Accountability:** Processes will be maintained to ensure that the privacy and confidentiality of client information is protected and that staff members are properly prepared and accountable to carry out Agency policies and procedures that govern the use of PPI data.
- a) Grievances may be initiated through the Agency grievance process for considering questions or complaints regarding privacy and security policies and practices.
 - b) All End Users of the HMIS must sign the AL-501 CoC End User License Agreement & Statement of Confidentiality, which specifies each staff person's obligations with regard to protecting the privacy of PPI, and indicates they have received a copy of the AL-501 CoC Privacy Notice to Clients and that they will comply with its guidelines.
 - c) All End Users of the HMIS must complete formal Privacy and Security Training.
 - d) A process will be maintained to document and verify completion of training requirements.
 - e) A process will be maintained to monitor and audit compliance with basic privacy requirements including, but not limited to, auditing clients entered against signed releases.
 - f) A copy of any staff grievances initiated relative to privacy, confidentiality, or HMIS data will be forwarded to Housing First, Inc.
- 8) **Limited Information Sharing:** The AL-501 CoC uses a limited data sharing model for those clients who wish to share their information within the HMIS. Clients are required to sign the AL-501 CoC Client Release of Information and Sharing Plan ("ROI" or "Sharing Plan"), which provides notice of how personal information is used within the HMIS, and requires client consent on how their personal information is shared and the Participating Agencies with which it is shared. A client may request a copy of the Sharing Plan to see a complete list of agencies with which information may be shared. Although the agencies who participate in the Sharing Plan may change from time to time, a client may always ask for the most recent copy of the Sharing Plan.

The limited sharing model outlined below, and offers three (3) different sharing options.

Limited Sharing Model:

1. **Option 1** - This option allows the most information sharing, and therefore the most coordination of services and the least duplication of efforts in order to serve a client. The information shared is as follows:
 - a. **Basic Information** – This information will be shared with Participating Agencies in Alabama and Florida. Basic Information includes the following: name, date of birth, social security number, program enrollments, case managers, military background (veteran status), and photo.
 - b. **Detailed Information** – This information will only be shared with local agencies in Mobile and Baldwin counties. Detailed Information is listed in the AL-501 CoC Sharing Plan, and includes the following: case plan(s), including goals, action steps, and case notes; communicable and venereal diseases (e.g. hepatitis, syphilis, gonorrhea, tuberculosis, HIV/AIDS); disability information, including chronic health condition(s), developmental, HIV/AIDS, physical and mental health; drug and/or alcohol abuse and treatment history; educational attainment; employment history; ethnicity; gender; health insurance (sources); household members; incidents and bans; income and non-cash benefits (amounts and sources); living situation, housing history, and circumstances of need; race; risk factors; services (requested and received) and referrals.
2. **Option 2** - Under this option, **only** the agencies a client specifies will see their Detailed Information, including their healthcare and drug treatment information.
3. **Option 3** - Under this option, information **will not** be shared, and the client **will not** be denied access to services because they choose not to share information.

9) Sharing of Information:

- a) At the Agency's or Continuum Designated HMIS Lead Agency's request, protections afforded to those with increased privacy risks (i.e. victims of domestic violence, dating violence, sexual assault, and stalking) include the following: setting closed visibility so that only the serving Agency may see the record, which requires the End User to notify the Continuum Designated HMIS Lead Agency's System Administrator within 24 hours of input of this information into the System to close the record; the right to have a record marked as inactive; the right to remove the record from the System.
- b) A completed ROI is needed before information is 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) The Sharing Plan informs the client about what is shared and the agencies with which it is shared.
- c) Clients will be informed about and understand the benefits, risks, and the available alternatives to sharing their information prior to signing an ROI, and their decision to sign or not sign shall be voluntary.
- d) Clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.
- e) All client ROI forms related to the HMIS will be placed in a file on the Agency's premises, and will be made available to Housing First for periodic audits.
- f) ROI forms will be retained for a period of seven (7) years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
- g) Outreach staff gathering information in the field, prior to execution of an ROI, must provide the client with the AL-501 CoC Outreach Privacy Notice (Appendix Q) and sign the AL-501 CoC Outreach Consent Certification (Appendix R), affirming receipt of the client's verbal consent before entering, updating, editing, printing, or disclosing their Basic Information. Basic Information includes the following: name, date of birth, social security number, program enrollments, case managers, military background (veteran status), and photo. Otherwise, limited visibility must be coordinated with Housing First, Inc. Detailed Information may not be entered into the HMIS prior to execution of the ROI.
 - i) 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.
 - j) Agencies who wish to share information with other Agencies participating in the PromisSE, outside of the AL-501 CoC, must sign interagency agreements describing the PromisSE privacy rules the agencies are required to follow. The agreement must also acknowledge the agencies are prohibited from making further disclosure of the information shared, unless it is expressly permitted by the written consent of the

- person to who it pertains or as otherwise permitted by law.
- k) 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.
 - l) 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 Continuum Designated HMIS Lead Agency’s System Administrator within 48 hours so that the client record can be “closed.”
- 10) **System Security:** System security provisions will apply to all Systems where PPI is stored, including Agency networks, desktops, laptops, mini-computers, mainframes and servers.
- a) **Password Access**
 - i) Only licensed end users who have completed Privacy and Security Training and passed the End User Certification Test will be given access to the HMIS through a username and password.
 - ii) Temporary/default passwords will be changed on first use.
 - iii) Access to the HMIS requires a username and password at least eight (8) characters long and using at least two (2) numbers and/or special characters.
 - iv) A username and password may not be stored or displayed in any publicly accessible location.
 - v) End Users must not be able to log on from more than location or workstation at a time.
 - vi) Individuals with usernames and passwords will not give this information to any other organization, governmental entity, business, or individual to access the HMIS.
 - b) **Virus Protection and Firewalls**
 - i) Commercial antivirus software is current and updates automatically.
 - ii) Virus protection will automatically scan files as they are accessed by End Users.
 - iii) Virus definitions will be updated regularly by the Agency.
 - iv) All computers accessing the HMIS are updated regularly and are protected by a firewall.
 - c) **Physical Access to Systems where HMIS Data is Stored**
 - 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 the computer is not in use.
 - iii) End Users must log out of the HMIS and their computer when leaving the workstation.
 - d) **Data Security**
 - i) HMIS data is prohibited from being downloaded onto Portable Storage Devices, including small plug-and-play devices such as USB drives, recordable discs, and external hard disks.
 - ii) Downloads for purposes of statistical analysis will exclude PPI whenever possible.
 - e) **Hard Copy Security**
 - i) Any paper or other hard copy containing PPI 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) Agency staff will supervise at all times any hard copies of data in a public area, which contain client identifying information generated by or for the HMIS. If the staff leaves the area, the hard copies must be secured in a place not accessible by the public.
 - iii) All written information pertaining to a username and password must not be stored or displayed in any publicly accessible location.
 - f) **Remote Access to the HMIS**
 - i) HMIS End Users are prohibited from accessing the HMIS from a computer that is available to the public, or through an internet connection that is not secure. Staff are not permitted to use public Wi-Fi to access the HMIS, including that provided by internet cafes, libraries, airports 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 PPI.
 - 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 Bowman Systems and are therefore not covered in 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. **Please see “Bowman Systems Securing Client Data” posted to www.hfal.org/services/hmis-department/policy-and-procedures/, detailing the software vendor’s data security standards.***

11) Privacy Policy Change History

Change History

This is Version 2 of our Privacy Policy, which is our first revision.

- 1. Version 1 - June 2014. Initial Policy**
- 2. Version 2 – September 2016. Updated. – Updated “Compliance” section; renamed “Use of Information” section “Uses and Disclosures of Information,” and revised it to correspond with the uses and disclosures in the AL-501 CoC Privacy Notice to Clients; added “Limited Information Sharing” section to reflect amendments to the ROI and the addition of the Sharing Plan, and added the verbal consent exception for outreach workers; in the “Sharing of Information” section, deleted reference to the default setting of open in HMIS for record sharing between Agencies, added the verbal consent exception for outreach workers, and amended the requirement for additional interagency agreements to be executed only when Agencies wish to share client data with other Agencies within the HMIS outside of the AL-501 CoC vs. the requirement for an interagency agreement to share locked data addressed through the Sharing Plan and Participation Agreement; renamed “Stored Data Security and Disposal” section “Data Security” and added a policy prohibiting HMIS data from being downloaded onto Portable Storage Devices, and deleted any policies allowing or prescribing guidelines for the download of HMIS data onto data storage mediums, and added the website address to locate Bowman System’s data security standards.**

Effective Date: The AL-501 CoC Privacy Policy governs the privacy of information received on or after January 1, 2017. Information received or entered prior to the effective date is governed under the preceding Privacy Policy.

Universal Data Elements

HMIS Universal Data Elements are elements required to be collected by all projects using the software as an HMIS. Projects funded by any one or more of the federal partners must collect the Universal Data Elements as are projects that are not funded by any federal partner (e.g. missions) but are entering data as part of the Continuum of Care's HMIS implementation.

Universal Data Elements enable the HMIS the ability to record unique, unduplicated client records, establish participation in a project within a date range, and identify clients who meet time criteria for chronic homelessness.

The Universal Data Elements include:

- 3.1 Name
- 3.2 Social Security Number
- 3.3 Date of Birth
- 3.4 Race
- 3.5 Ethnicity
- 3.6 Gender
- 3.7 Veteran Status
- 3.8 Disabling Condition
- 3.917 Living Situation
- 3.10 Project Entry Date
- 3.11 Project Exit Date
- 3.12 Destination
- 3.13 Personal ID
- 3.14 Household ID
- 3.15 Relationship to Head of Household
- 3.16 Client Location

For more information and a full description of the Universal Data Elements, please reference the 2014 HUD Data Standards: Data Manual, Version 5.1.

APPENDIX L

Program Management Information System of the Southeast PromisSE

Participation Agreement Between One Roof and

(Name of Continuum Designated HMIS Lead Agency)

This agreement is entered into on _____(dd/mm/yy) between One Roof, designated as PromisSE's HMIS Lead 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 for being homeless.

II. One Roof Responsibilities

1. One Roof, as PromisSE's HMIS Lead Agency, will offer initial training for the HMIS Coordinator of each local 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 HMIS Lead Agencies electronically at least two weeks in advance, barring extenuating circumstances.
2. One Roof, as PromisSE's HMIS Lead Agency, will provide PromisSE software support and technical assistance (i.e., general trouble-shooting and assistance with standard report generation) to the HMIS Coordinator of each local 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.
3. One Roof will establish a fee structure for financing the software utilized by PromisSE, including an administrative fee.
4. One Roof will invoice participants in a timely manner.

Updated 7/18/14

APPENDIX L

5. One Roof will order user licenses at the request of the HMIS Coordinator of each local HMIS Lead Agency.

III. HMIS Lead Agency's Responsibilities

1. The 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 Lead Agency, within 48 hours of any changes in this designation.
2. The 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.
3. The HMIS Lead Agency agrees to designate and provide training for a Continuum System Administrator responsible for administering the PromisSE within the Continuum.
4. The 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 Policy and Procedure Manual and any Federal standards that supersede the Policies and Procedures.
5. The 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.
6. The HMIS Lead Agency agrees to make end user license and reporting license requests through One Roof.
7. The HMIS Lead Agency agrees to make Bowman requests through One Roof.

IV. Custody of Data

1. The HMIS Lead Agency and One Roof understand that the 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).
2. 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.
3. 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 Lead Agency by the PromisSE Steering Committee for continuing administration, and all PromisSE Continuums will be informed in a timely manner.
4. In the event that the 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

1. One Roof makes no warranties, expressed or implied. The 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 HMIS Lead Agency or another party arising from participation in the PromisSE; or arising from any acts, omissions, neglect, or fault of the HMIS Lead Agency or its agents, employees, licensees, or clients; or arising from the HMIS Lead Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This HMIS Lead Agency will also hold One Roof harmless for loss or damage

Updated 7/18/14

APPENDIX L

resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by the chosen software vendor for PromisSE by the HMIS Lead Agency'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 HMIS Lead Agency for damages, losses, or injuries to the 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 HMIS Lead Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of One Roof.

2. It is the responsibility of the HMIS Lead Agency to ensure that each participating Agency within the Continuum maintain compliance with all PromisSE Policies and Procedures in addition to any required by Federal standards.

VI. Terms and Conditions

- 1. The HMIS Lead Agency shall not transfer or assign any rights or obligations under the Participation Agreement without the written consent of One Roof.
- 2. 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 breeches 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.
- 3. 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
 1704 5th Ave N
 Birmingham, AL 35203

 (205)254-8833
 One Roof Telephone Number

 One Roof Representative Printed Name

 One Roof Representative Title

 One Roof Representative Signature

 Date (mm/dd/yy)

 HMIS Lead Agency Name

 HMIS Lead Agency Address

 HMIS Lead Agency City, State ZIP

 HMIS Lead Agency Telephone Number

 HMIS Lead Agency Rep. Printed Name

 HMIS Lead Representative Title

 HMIS Lead Representative Signature

 Date (mm/dd/yy)

APPENDIX L

**Program Management Information System of Alabama
HMIS Lead Agency
One Roof
ASSURANCE**

_____ (Name of 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 HMIS Lead Agency's Board Approved Confidentiality Policy.
- The 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 HMIS Lead Agency PromisSE Policy and Procedure Manual.
- The HMIS Lead Agency's Conflict of Interest Policy.
- The HMIS Lead Agency's Whistleblower Policy.

By: _____

Title: _____

Signature: _____

Date: _____

APPENDIX M

AL-501 CoC System Administrator Agreement

Name: _____

Agency Name: _____

A Continuum Designated HMIS Lead Agency (Housing First, Inc.) must designate and staff one HMIS System Administrator. The System Administrator’s requirements and responsibilities within the AL-501 Continuum of Care (CoC) include, but are not limited to, the following:

- Completing, at minimum, System Administrator training.
- Ensuring all End Users have a signed AL-501 CoC End User License Agreement & Statement of Confidentiality on file.
- Ensuring all Agency Administrators have a signed AL-501 CoC Agency Administrator Agreement on file.
- Ensuring all Security Officers have a signed AL-501 CoC Security Officer Agreement on file.
- Ensuring all End Users complete the annual End User Certification Test, to include Privacy and Security Training.
- Ensuring all End Users complete workflow training and related updates, and have documentation of the training.
- Ensuring the Participating Agencies are in compliance with the Data Security Standards detailed in the AL-501 CoC HMIS Policies and Procedures.
- Ensuring the Participating Agencies are in compliance with the AL-501 CoC HMIS Operating Policies and Procedures.
- Ensuring all the Participating Agencies’ End Users have successfully cleared a criminal background check, evidenced by the receipt of the AL-501 CoC HMIS Criminal Background Check Certification forms from the Agency Administrator, prior to gaining access to the HMIS.

The original AL-501 CoC System Administrator Agreement shall be kept on file at the Housing First, Inc., and all subsequent Agreements shall be kept on file at Housing First for a minimum of five (5) years.

One Roof makes no warranties, expressed or implied. The Housing First, Inc., at all times, will indemnify and hold the One Roof harmless from any damages, liabilities, claims, and expenses that may be claimed against Housing First; or for injuries or damages to Housing First 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 Housing First's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. Housing First will also hold One Roof harmless for loss or damage resulting in the loss of data due to delays, nondeliveries, mis-deliveries, or service interruption caused by Bowman Systems, by Housing First or other Participating Agencies’ negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. One Roof shall not be liable to Housing First for damages, losses, or injuries to Housing First or another party other than if such is the result of gross negligence or willful misconduct of One Roof. One Roof agrees to hold Housing First harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of OneRoof.

The AL-501 CoC System Administrator Agreement is in effect for a period of one (1) year from the date of signing. Failure to comply with the provisions of this Agreement is grounds for termination or suspension of your ServicePoint license and access to ServicePoint. Your signature below indicates your agreement to comply with the AL-501 CoC System Administrator Agreement.

Employee Printed Name

Agency Official Printed Name

Employee Signature

Agency Official Signature

Date (mm/dd/yy)

Date (mm/dd/yy)

Updated 9/2016

APPENDIX N

AL-501 CoC System Security Officer Agreement

Name: _____

Agency Name: _____

A Continuum Designated HMIS Lead Agency (Housing First, Inc.) must assign a System Security Officer. The Security Officer requirements and responsibilities within the AL-501 Continuum of Care (CoC) include, but are not limited to, the following:

- Ensuring the Continuum Designated HMIS Lead Agency's computers connected to the HMIS are automatically updated on a regular basis, have current antivirus software, and firewall protection.
- Ensuring all End Users complete annual Privacy and Security Training. Training must be provided by the Continuum Designated HMIS Lead Agency and based on the Privacy and Security Plan detailed in the AL-501 CoC HMIS Operating Policies and Procedures.
- Conducting an annual security review of the Continuum Designated HMIS Lead Agency that includes reviewing compliance with the Privacy and Security Plan. The System Security Officer must document the findings of the review on the AL-501 CoC Privacy and Security Checklist (Appendix E), which must be submitted to the PromisSE HMIS Lead Agency's System Administrator no later than December 31st of each year.
- Notifying the PromisSE HMIS Lead Agency's System Administrator when a System Administrator leaves the organization or when revision of a System Administrator's access level is needed because of changes to job responsibilities. The notification must be made within 24 hours of the change.
- Reporting any security or privacy incidents to the Continuum Designated HMIS Lead Agency's System Administrator. The System Administrator investigates the incident, including running applicable audit reports. If the System Administrator and System Security Officer determine that a breach has occurred and/or the End Users involved violated privacy or security guidelines, the System Administrator will report the breach to the chair of the AL-501 CoC Board of Directors and the CEO of Housing First. A Corrective Action Plan will be implemented, which must include supervision and retraining of the offending party, at minimum. It may also include the removal of HMIS End User licenses, client notification, and/or appropriate legal action. The Continuum Designated HMIS Lead Agency may request, or independently order, an updated criminal background check on any End User suspected of violating one or more of the standards or requirements outlined in the AL-501 CoC HMIS Operating Policies and Procedures and the AL-501 CoC End User License Agreement & Statement of Confidentiality.

The original AL-501 CoC System Security Officer Agreement shall be kept on file at the Continuum Designated HMIS Lead Agency, and all subsequent Agreements shall be kept on file for a minimum of five (5) years.

One Roof makes no warranties, expressed or implied. The Housing First, Inc., at all times, will indemnify and hold the One Roof harmless from any damages, liabilities, claims, and expenses that may be claimed against Housing First; or for injuries or damages to Housing First 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 Housing First's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. Housing First will also hold One Roof harmless for loss or damage resulting in the loss of data due to delays, nondeliveries, mis-deliveries, or service interruption caused by Bowman Systems, by Housing First or other Participating Agencies' negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. One Roof shall not be liable to Housing First for damages, losses, or injuries to Housing First or another party other than if such is the result of gross negligence or willful misconduct of One Roof. One Roof agrees to hold Housing First harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of OneRoof.

The AL-501 CoC System Security Officer Agreement is in effect for a period of one (1) year from the date of signing. System Security Officers are required to complete the End User Certification Test and document compliance monitoring annually, at which time a new agreement will be provided. Failure to comply with the provisions of this Agreement is grounds for termination or suspension of your

Updated 9/2016

APPENDIX N

ServicePoint license and access to ServicePoint. Failure to comply with the provisions of this Agreement may additionally result in termination or suspension of the AL-501 CoC Participation Agreement. Your signature below indicates your agreement to comply with the AL-501 CoC System Security Officer Agreement.

Employee Printed Name

Agency Official Printed Name

Employee Signature

Agency Official Signature

Date (mm/dd/yy)

Date (mm/dd/yy)

APPENDIX O

AL-501 CoC Agency Audit Checklist

- ___ Completed and submitted the AL-501 CoC HMIS Operating Policies and Procedures Compliance Checklist (Appendix D)
- ___ Completed annual AL-501 CoC Privacy and Security Checklist (Appendix E)
- ___ All End Users have executed the AL-501 CoC End User License Agreement & Statement of Confidentiality (Appendix F).
- ___ AL-501 CoC Public Notice (Appendix H) is posted and visible to clients
- ___ AL-501 CoC Privacy Notice to Clients (Appendix I) is available to clients
- ___ AL-501 AL-501 CoC Privacy Policy (Appendix J) has been adopted, outlining the privacy and security standards for use of the HMIS.
- ___ AL-501 CoC Privacy Policy includes a remote access plan
- ___ Hard copy data is secure
- ___ HMIS workstations are password protected
- ___ HMIS workstations have time scheduled locked settings
- ___ Client data is entered into the HMIS within 48 hours of collection
- ___ End Users have received a copy of the HUD Data Elements (Appendix K)
- ___ End Users have been trained on the HUD definition of homelessness and understand the priority of homelessness documentation.
- ___ Agency has a process to ensure client names are spelled properly and the DOB is accurate
- ___ End Users update client information as required by program type through Interim Updates and Annual Assessments (as applicable).
- ___ Agency Administrators or assigned End Users are running monthly data quality reports and making corrective action according to the data quality requirements in the AL-501 CoC HMIS Operating Policies and Procedures.
- ___ All End Users participate in initial HMIS training, and successfully complete the annual Privacy and Security Training and End User Certification Test (90% score or better).
- ___ All Agency Administrators with an ART license have had at least ART 101 training

By signing below, you certify the Agency is in compliance with the aforementioned requirements. Failure to report compliance concerns or findings to the Continuum Designated Lead Agency's System Administrator is grounds for revocation of your System Security Officer status, and termination or suspension of your ServicePoint license and access to the System. Failure to report compliance concerns or findings to the Continuum Designated Lead Agency's System Administrator may additionally result in termination or suspension of the Agency's AL-501 CoC Participation Agreement.

System Security Officer Name

System Security Officer Signature

Date

AL-501 CoC HMIS Contract Agreement Policy

HMIS Contract Agreement

The Continuum Designated HMIS Lead Agency will execute the AL-501 CoC HMIS Contract Agreement with each Participating Agency within the AL-501 CoC, outlining the rights and responsibilities of each party. The contract term operates on the Continuum Designated HMIS Lead Agency's fiscal year (October 1 – September 30). Additional services must be formally requested by the Agency. The cost of the additional services will be billed to the Agency on the statement immediately following the request.

HMIS Fee Schedule

The HMIS Fee Schedule (see Attachment B of the AL-501 CoC HMIS Contract Agreement) provides a detailed itemization of the amount of the HMIS Contract Agreement, and is designed to ensure high quality HMIS customer service, technical assistance, and data management through equitable cost sharing amongst participating Agencies. The HMIS Fee Schedule may be amended as needed by the Continuum Designated HMIS Lead Agency. Changes must be reviewed and approved by the CoC Board of Directors prior to public distribution and implementation.

Payments

Agencies may choose to pay on a monthly or an annual basis. If a new Agency joins the HMIS, or if an existing Agency implements a new project within the contract year, the HMIS contract amount will be prorated. The Continuum Designated HMIS Lead Agency expects payment at the time it is due. Statements will be submitted to the Agency by the 15th of each month. Payment is due upon receipt, and is considered late after a grace period of 30 days from date of issue. Payments must be issued on a company check and made payable to the Continuum Designated HMIS Lead Agency. At the close of the grace period, the Continuum Designated HMIS Lead Agency reserves the right to suspend the accounts of all End Users associated with the Agency until full payment is received.

Contract Termination

Both parties reserve the right to terminate the HMIS Contract Agreement. The terminating party must submit in writing a notice of termination no less than 30 days prior to the intended termination date. The terminating Agency is responsible for payment through the 30-day notice, and subject to a termination fee equal to two (2) months of the HMIS contract amount or payment of the contract in full, whichever is the lesser amount. Refunds to Agencies paying annually will be made after the notice period. Should the Continuum Designated HMIS Lead Agency wish to terminate the HMIS Contract Agreement, the request will be brought before the CoC Board of Directors for review to determine the validity of the request and subsequent fees. Should the violation include a breach of the AL-501 CoC HMIS Operating Policies and Procedures, the Continuum Designated HMIS Lead Agency reserves the right to collect or withhold the full balance of the HMIS contract amount after termination.

Project Defunding

If the HMIS Contract Agreement includes a federally funded subrecipient project that is defunded, and the Agency wishes to terminate the project within the HMIS, the Continuum Designated HMIS Lead Agency must be notified in writing prior to the project's date of closure. A termination fee will not be assessed. If the annual contract amount was paid in full, the Agency will be reimbursed the prorated contract amount for the defunded project within 30 days from the date of the project's closure.

Hardship Clause

The Continuum Designated HMIS Lead Agency understands unforeseen events may arise that impede an Agency's ability to meet the financial obligation of the contract. Should such an event occur, the Agency must inform the Continuum Designated HMIS Lead Agency by written notice 15 days prior to the close of the grace period. The Continuum Designated HMIS Lead Agency will present the case to the CoC Board of Directors, the body responsible for determining whether the circumstances meet the basic requirements of the Hardship Clause. If accepted, reasonable accommodations will be determined on an individual basis.

AL-501 CoC Outreach Privacy Notice

Our homeless outreach team collects information about the people experiencing homelessness in our community. When we meet with you, we will ask you information about yourself and your family, and we will put the information into a computer system called PromisSE (or "HMIS"). The information that we collect allows us to work with other agencies to help you, to coordinate your case management, to create de-identified reports about homelessness in our community, and to reduce the number of times that you have to re-tell your story or re-give your information.

We may be required to collect some personal information by law or by organizations that give us money to operate our homelessness assistance programs. 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. A copy of our Privacy Notice to Clients and our Privacy Policy, which describe our full privacy practices, are available to you upon request.

You have the right to ask us not to enter your information into HMIS, and we will never deny you services because you did not share your information. Our outreach team will only enter your basic information into HMIS if you give us verbal consent. Basic Information includes the following: name, date of birth, social security number, program enrollments, case manager(s), military background (veteran status), and photo.

APPENDIX R

AL-501 CoC Outreach Consent Certification

Client Name

Date

I affirm that I gave the above referenced client a copy of the AL-501 CoC Outreach Privacy Notice, and after I explained its contents to the client, the client gave verbal consent to enter his or her Basic Information into the PromisSE or HMIS. Basic Information includes the following: name, date of birth, social security number, program enrollments, case manager(s), military background (veteran status), and photo.

Employee Printed Name

Employee Signature

Date

AL-501 CoC HMIS Criminal Background Check Certification

The Program Management Information System of the Southeast (“PromisSE” or “HMIS”) 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. As such, an Agency’s employees, volunteers, staff and any persons requesting access to the PromisSE must comply with the AL-501 CoC End User License Agreement & Statement of Confidentiality and the requirements set forth in the AL-501 CoC HMIS Operating Policies & Procedures, including the successful clearance of a criminal background check, which must be certified by the Agency Administrator to the Continuum Designated HMIS Lead Agency’s (Housing First) System Administrator on the said form before access is granted to the HMIS.

It is duly noted Housing First may request, or independently order, an updated criminal background check on any end user suspected of violating one or more of the standards or requirements outlined in the AL-501 CoC HMIS Operating Policies and Procedures and the AL-501 CoC End User License Agreement & Statement of Confidentiality.

Prospective HMIS End User Name

Date

I affirm the Prospective HMIS End User referenced above successfully cleared his or her criminal background check completed on _____, which means the said individual hasn’t been convicted of a crime involving deception, or a felony involving violence or the threat of violence against another person within the last seven (7) years.

Agency Administrator Printed Name

Agency Administrator Signature

Date

AL-501 CoC HMIS Privacy Statement

Your privacy is very important to us. This privacy statement describes the privacy policy of the AL-501 Homeless Coalition of the Alabama Gulf Coast Continuum of Care (“AL-501 CoC”) regarding your personal protected information (information which can be used to identify a specific client or “PPI”) residing in PromisSE, and explains what PPI is collected, why it is collected, and how it is used and disclosed. PromisSE is a Homeless Management Information System (“HMIS” or “System”), which is a computer system that the U.S. Department of Housing and Urban Development (“HUD”) requires us to use for homeless assistance programs. The HMIS is used collect client data and data on the provision of housing and services to homeless individuals, families, and persons at risk of homelessness. The information that we collect allows us to work with other Agencies to help you, coordinate your case management, and to reduce the number of times you have to re-tell your story or repeat information.

Confidentiality Rights

The HMIS is operated by the AL-501 CoC’s Continuum Designated HMIS Lead Agency (Housing First, Inc.) in accordance with HUD confidentiality regulations, including those covering programs that receive HUD funding for homeless services (Federal Register/Vol. 69, No. 146). Agencies covered under the Health Insurance Portability and Accountability Act (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, must notify Housing First’s System Administrator of their HIPAA status to allow Housing First to handle their client data in compliance with HIPAA. Other rules that may also apply include 42 CFR Part 2 governing drug and alcohol records.

Why We Collect Information

We collect Personal Protected Information directly from you for reasons discussed in the AL-501 CoC Privacy Notice to Clients. We may also collect information about you from other Agencies if you have given the Agency written consent to share your information. We may be required to collect some personal information by law or by organizations that give us money to operate our programs. Additional personal information that we collect is important to run our programs, to improve the services for homeless persons, and to better understand the needs of homeless persons. The collection and use of PPI is guided by strict standards of confidentiality. We only collect PPI when appropriate, by lawful and fair means, and with the your knowledge or consent. Our Privacy Notice is posted on our website at www.hfal.org/services/hmis-department/policy-and-procedures/. A copy of our Privacy Notice is available to you upon request.

How We Use and Disclose Information

Protected Personal Information can only be used for the following purposes:

- a. To **provide or coordinate services** for you;
- b. for functions related to **payment or reimbursement for services**;
- c. to **carry out administrative functions** such as legal, audits, personnel, oversight, and management functions;
- d. to **create de-identified (anonymous) information** that can be used for reporting, research, and statistical purposes without identifying clients;
- e. for **contractual research purposes** where privacy conditions are met (including a written agreement);
- f. **when required by law** to the extent that use or disclosure complies with and is limited to the requirements of the law;
- g. to **avert a serious threat to health or safety** if:
 - i. we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, **and**
 - ii. the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat;
- h. to comply with **government reporting obligations** for the HMIS and for oversight of compliance with HMIS requirements;
- i. to **report criminal activity** on Agency premises.

Limited Information Sharing

We require you to sign the AL-501 CoC Client Release of Information and Sharing Plan (“ROI” or “Sharing Plan”), which provides notice of how your personal information is used within the HMIS, and requires your consent on how your personal information is shared and the Participating Agencies with which it is shared. Please request a copy of the Sharing Plan to see a complete list of agencies with which you may share information. Although the agencies who participate in the Sharing Plan may change from time to time, you may always ask for the most recent copy of the Sharing Plan from this Agency.

The Limited Sharing Model we use is as follows, and offers three (3) sharing options:

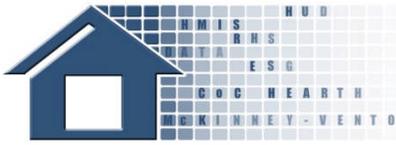
1. **Option 1** - This option allows the most information sharing, and therefore the most coordination of services and the least duplication of efforts in order to serve you. The information below will be shared as follows:
 - a. **Basic Information** – This information will be shared with Participating Agencies in Alabama and Florida. Your Basic Information includes the following: your name, date of birth, social security number, program enrollments, case manager(s), military background (veteran status), and photo.
 - b. **Detailed Information** – This information will only be shared with local agencies in Mobile and Baldwin counties. Please ask for a copy of the Sharing Plan to see a complete list of these agencies. Your Detailed Information is listed in the AL-501 CoC Sharing Plan, and includes the following: case plan(s), including goals, action steps, and case notes; communicable and venereal diseases (e.g. hepatitis, syphilis, gonorrhea, tuberculosis, HIV/AIDS); disability information, including chronic health condition(s), developmental, HIV/AIDS, physical and mental health; drug and/or alcohol abuse and treatment history; educational attainment; employment history; ethnicity; gender; health insurance (sources); household members; incidents and bans; income and non-cash benefits (amounts and sources); living situation, housing history, and circumstances of need; race; risk factors; services (requested and received) and referrals.
2. **Option 2** - Under this option, **only** the agencies that you specify will be able to see your Detailed Information, including your healthcare and drug treatment information.
3. **Option 3** - Under this option, your information **will not** be shared, and you **will not** be denied access to services because you choose not to share your information.

A client's Basic Information (name, date of birth, social security number, program enrollments, case manager(s), military background/veteran status, and photo) collected in the field by outreach workers may be entered into the HMIS prior to the execution of a signed ROI. However, the outreach worker must provide the client with the AL-501 CoC Outreach Privacy Notice (Appendix Q) and sign the AL-501 CoC Outreach Consent Certification (Appendix R), affirming receipt of the client's verbal consent before entering, updating, editing, printing, or disclosing their Basic Information. Otherwise, limited visibility must be coordinated with Housing First. Detailed Information may not be entered into the HMIS prior to execution of the ROI.

Your Information Rights

1. All requests for personal information located within the HMIS need to be made to the Agency or organization that collected and entered or updated your information.
2. We may not disclose your Personal Protected Information located within the HMIS except as required by law, or to help the Participating Agency that collected/entered/updated the information operate the System.
3. We may not publish reports on your 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 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 Administrator(s) operating the HMIS database may see your information.



Homeless Definition

CRITERIA FOR DEFINING HOMELESS	Category 1	Literally Homeless	<p>(1) Individual or family who lacks a fixed, regular, and adequate nighttime residence, meaning:</p> <ul style="list-style-type: none"> (i) Has a primary nighttime residence that is a public or private place not meant for human habitation; (ii) Is living in a publicly or privately operated shelter designated to provide temporary living arrangements (including congregate shelters, transitional housing, and hotels and motels paid for by charitable organizations or by federal, state and local government programs); <u>or</u> (iii) Is exiting an institution where (s)he has resided for 90 days or less <u>and</u> who resided in an emergency shelter or place not meant for human habitation immediately before entering that institution
	Category 2	Imminent Risk of Homelessness	<p>(2) Individual or family who will imminently lose their primary nighttime residence, provided that:</p> <ul style="list-style-type: none"> (i) Residence will be lost within 14 days of the date of application for homeless assistance; (ii) No subsequent residence has been identified; <u>and</u> (iii) The individual or family lacks the resources or support networks needed to obtain other permanent housing
	Category 3	Homeless under other Federal statutes	<p>(3) Unaccompanied youth under 25 years of age, or families with children and youth, who do not otherwise qualify as homeless under this definition, but who:</p> <ul style="list-style-type: none"> (i) Are defined as homeless under the other listed federal statutes; (ii) Have not had a lease, ownership interest, or occupancy agreement in permanent housing during the 60 days prior to the homeless assistance application; (iii) Have experienced persistent instability as measured by two moves or more during in the preceding 60 days; <u>and</u> (iv) Can be expected to continue in such status for an extended period of time due to special needs or barriers
	Category 4	Fleeing/ Attempting to Flee DV	<p>(4) Any individual or family who:</p> <ul style="list-style-type: none"> (i) Is fleeing, or is attempting to flee, domestic violence; (ii) Has no other residence; <u>and</u> (iii) Lacks the resources or support networks to obtain other permanent housing