

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 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."

- 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.**

APPENDIX J

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.

APPENDIX K

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 Start Date
- 3.11 Project Exit Date
- 3.12 Destination
- 3.15 Relationship to Head of Household
- 3.16 Client Location
- 3.20 Housing Move-in Date

For more information and a full description of the Universal Data Elements, please reference the 2017 HMIS Data Standards: Data Manual, Version 1.3



Homeless Definition

CRITERIA FOR DEFINING HOMELESS	Category 1	Literally Homeless	(1) Individual or family who lacks a fixed, regular, and adequate nighttime residence, meaning: <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	(2) Individual or family who will imminently lose their primary nighttime residence, provided that: <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	(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: <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	(4) Any individual or family who: <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