Appendix I – Privacy Notice to Clients

The Homeless Management Information System (HMIS) was developed to meet a data collection requirement made by the United States Congress to the Department of Housing and Urban Development (HUD). Congress passed this requirement to get a more accurate count of individuals who are homeless and to identify the need for and use of different services by those individuals and families. Several CoCs in the Southeast share a single HMIS implementation. The CoC Lead Entity designates the HMIS Lead Agency for that CoC.

Many Agencies in this area use the HMIS to keep computerized case records. With client permission as indicated by a signed Release of Information, client information can be shared with other HMIS participating Agencies throughout the Implementation. The information entered by participating providers and shared with client consent includes basic identifying demographic data (e.g., name, birth date, and gender), the nature of the client's situation, and the services and referrals received from the participating Agency.

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

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

Confidentiality Rights

Each participating Agency is required to have a confidentiality policy that has been approved by its Board of Directors. The AL 502 Lead Agency must also have a Board Approved confidentiality policy. The AL 502 CoC Lead Agency operates the HMIS in accordance with HUD and HIPAA confidentiality regulations, including those covering programs that receive HUD funding for homeless services (Federal Register/Vol. 69, No. 146), and those covered under the HIPAA privacy and security rules which govern confidential health information such as the diagnosis, treatment, of a mental health disorder, a drug or alcohol disorder, and AIDS/HIV condition or a domestic violence situation. Other rules that may also apply include 42 CFR Part 2 governing drug and alcohol records.

The AL 502 CoC is restricted to using or disclosing personal information from the HMIS to the following circumstances:

- For functions related to payment or reimbursement for services.
- For functions related to helping Agencies operate the System.
- For functions related to the development of reports to better plan services.
- To carry out administrative functions including but not limited to legal, audit, personnel, planning, oversight and management functions;
- To develop databases used for research, where all identifying information has been removed.
- To support contractual research where privacy conditions are met with an approved Institutional Review Board (IRB), and only if the shared information includes no identifying information about the client.
- Where a disclosure is required by law and disclosure complies with, and is limited to, the requirements of the law. Instances, where this might occur, are during a medical emergency, to report a crime against the staff of the Agency, or to avert a serious threat to health or safety.

Your Information Rights

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

The AL 502 CoC may not disclose your personal protected information located within the HMIS except as required by law or to help the participating Agency/organization that collected/entered/updated the information operate the System.

The AL 502 CoC may not publish reports on client data that identifies specific Agencies or persons. Public reports otherwise published will be limited to the presentation of aggregated data that does not disclose personal identifying information.

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

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

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

Please feel free to contact us if you feel that your information rights have been violated. Please address your written communication to the CoC (HCCNWAL HMIS Lead - Community Action NW AL, 745 Thompson Street, Florence, Alabama 35630). Please include your contact information. We will respond in writing within 7 working days of the receipt of your letter.

How Your Information Will Be Kept Secure

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

- The computer program we use has the highest degree of security protection available.
- Only trained and authorized individuals will enter or view your personal information.
- Your name and other identifying information will not be contained in HMIS reports that are issued to local, state, or national Agencies.
- Employees receive training in privacy protection and agree to follow strict confidentiality standards before using the System.
- The server/database/software only allows authorized individuals access to the information. Only those who should see certain information will be allowed to see that information.
- The server/database will communicate using 128-bit encryption – an Internet technology intended to keep information private while it is transported back and forth across the Internet. Furthermore, identifying data stored on the server is also encrypted or coded so that it cannot be recognized.
- The server/database exists behind a firewall –a device meant to keep hackers/crackers/viruses/etc. away from the server.
- The main database will be kept physically secure, meaning only authorized personnel will have access to the server/database.

- System Administrators employed by the AL 502 Continuum-designated HMIS Lead Agency, Community Action Agency Northwest Alabama, support the daily operation of the database. Administration of the database is governed by agreements that limit the use of personal information to providing administrative support and generating reports using aggregated information. These agreements further ensure the confidentiality of your personal information.

Benefits of HMIS and Agency Information Sharing

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

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

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

Risks in Sharing Information

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

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

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

Appendix J – Partner Agency Privacy Policy

Reasons for Policy:

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: Agency privacy practices will comply with all applicable laws governing the HMIS client privacy/confidentiality. Applicable standards include, but are not limited to the following:
   a. Federal Register Vol. 69, No. 146 (HMIS FR 4848-N-02) - Federal statute governing HMIS information.
   b. HIPAA - the Health Insurance Portability Act.
   c. 42 CFR Part 2. - Federal statute governing drug and alcohol treatment.
   d. CoC HMIS Policy and Procedures
   e. NOTE: HIPAA statutes are more restrictive than the HMIS FR 4848-N-02 standards and in cases where both apply, HIPAA over-rides the HMIS FR 4848-N-02 standards. In cases where an Agency already has a confidentiality policy designed around the HIPAA standards, that policy can be modified to include the HMIS data collection or can be amended to create one set of standards for clients covered under HIPAA, and a second set of standards for those covered only under HMIS FR 4848-N-02. Agencies should indicate in their Privacy Notice which standards apply to their situation.
2. Use of Information: PII (personally identifiable information - information which can be used to identify a specific client) can be used only for the following purposes:
   a. To provide or coordinate services to a client.
   b. For functions related to payment or reimbursement for services.
   c. To carry out administrative functions such as legal, audit, personnel, planning, oversightand management functions.
   d. For creating de-personalized client identification for unduplicated counting.
   e. Where disclosure is required by law.
   f. To prevent or lessen a serious and imminent threat to the health or safety of an individual orthe public.
   g. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, includingthe target of the threat.
   h. To report abuse, neglect, domestic violence, or any other crime of a predatory nature as requiredor allowed by law.
   i. Contractual research where privacy conditions are met (including a written agreement).
   j. To report criminal activity on Agency premises.
   k. NOTE: HMIS FR 4848-N-02 standards list items a-d above as allowable reasons for disclosing PII but make provisions for additional uses to meet individual Agency obligations. In some cases, theseuses (e-I above) have additional conditions, and HMIS FR 4848-N-02 4.1.3 should be consulted if anyof

these optional items are to be included in an Agency's policy. It also states, "except for first party access to information and required disclosures for oversight and compliance auditing, all uses and disclosures are permissive and not mandatory."

3. Collection and Notification: Information will be collected only by fair and lawful means with the knowledge or consent of the client.
   a. PII will be collected only for the purposes listed above.
   b. Clients will be made aware that personal information is being collected and recorded.
   c. A written sign will be posted in locations where PII is collected. This written notice will read:
      "We collect personal information directly from you for reasons that are discussed in ourprivacy 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."
   d. This sign will be explained in cases where the client is unable to read and/or understand it.
   e. NOTE: Under HMIS FR 4848-N-02, Agencies are permitted to require a client to express consent to collect PII verbally or in writing, however, this is optional and not a requirement of the statute.

4. Data Quality: PII data will be accurate, complete, timely, and relevant.
   a. All PII 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.
   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 PII data, as well as its uses and disclosures, will be specified and limited.
   a. The purposes, uses, disclosures, policies, and practices relative to PII data will be outlined in an Agency Privacy Notice.
   b. The Agency Privacy Notice will comply with all applicable regulatory and contractual limitations.
   c. The Agency 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. PII 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 PII data will be tracked by an automated audit trail and will be monitored for violations use/disclosure limitations.
NOTE: Items above are required by HMIS FR 4848-N-02, and/or AL-501 HMIS policy, but Agencies can restrict and limit the use of PII data further by requiring express client consent for various types of uses/disclosures, and/or by putting restriction or limits on various kinds of uses/disclosures.

6. Record Access and Correction: Provisions will be maintained for the access to, and corrections of, PII records.
   a. Clients will be allowed to review their HMIS record within 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 client requests a correction, 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. Information is compiled in reasonable anticipation of litigation or comparable proceedings.
      ii. Information about another individual other than the Agency staff would be disclosed; and/or
      iii. Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.
   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, or if they have been put at personal risk, or harmed.
   h. Any client grievances relative to the HMIS will be processed and resolved according to Agency grievance policy.
   i. A copy of any client grievance relative to the HMIS data or other privacy/confidentiality issues and Agency response are forwarded to the CoC.

7. Accountability: Processes will be maintained to ensure that the privacy and confidentiality of client information is protected, and staff is properly prepared and accountable to carry out Agency policies and procedure that govern the use of PII data.
   a. Grievances may be initiated through the Agency grievance process for considering questions or complaints regarding privacy and security policies and practices. All End Users of the HMIS must sign an End Users Agreement that specifies each staff person's obligations with regard to protecting the privacy of PII and indicates that they have received a copy of the Agency's Privacy Notice and that they will comply with its guidelines.
   b. All System End Users must complete formal Privacy Training.
   c. A process will be maintained to document and verify completion of training requirements.
   d. A process will be maintained to monitor and audit compliance with basic privacy requirements including, but not limited to, auditing clients entered against signed HMIS Releases.
   e. A copy of any staff grievances initiated relative to privacy, confidentiality, or HMIS data will be forwarded to the CoC.

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

a. Agency defaults within the System will be set to "open" unless otherwise requested by the Agency.
b. A completed PromisSE HMIS Client Release of Information (ROI) Form is needed before information may be shared electronically. If the client refuses to have their information shared, their information is still entered into the HMIS but "closed" so that only that Agency and the System Administrators have access.
    i. PromisSE HMIS release informs the client about what is shared and with whom it is shared.
c. Clients will be informed about and understand the benefits, risks, and available alternatives to sharing their information prior to consenting to the ROI, and their decision to consent shall be voluntary.
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 to be located on premises and will be made available to the CoC for periodic audits. ROI granted via verbal consent will be noted as "Verbal Consent in the ROI section of HMIS.
f. PromisSE ROI forms will be retained for a period of 7 years, while they are active, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised. ROI forms can be retained electronically in HMIS and discarded immediately after.
g. 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.
h. Client information, including progress notes and psychotherapy notes, about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence entered by Agencies with "closed" visibility shall not be shared with other participating Agencies without the client's written, informed consent. Sharing of "closed" information must also be planned and documented through a fully executed agreement between Agencies, as documented through an inter-Agency "closed" data sharing agreement.
    i. Sharing of "closed" information is not covered under the general PromisSE ROI.
    ii. Once the client has provided written consent, and the involved PromisSE Member Agencies have executed a sharing of "closed" information agreement for an individual client or household, a copy of those documents must be sent to the local System Administrator (SA), along with a ticket outlining the information to be shared and the receiving Agency. The SA will then "open" that information only to the Receiving Agency.
i. 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.
j. 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 record can be "closed".

9. System Security: The System security provisions will apply to all Systems where PII is stored: Agency networks, desktops, laptops, minicomputers, mainframes, and servers.
    a. Password Access:
        i. Only individuals who have completed Privacy and basic System training may be given access to the System through End User IDs and Passwords.
        ii. Temporary/default passwords will be changed on first use.
        iii. Access to PII requires an End Username and password at least 8 characters long and using at least two numbers and/or special characters.
        iv. End User Name and password may not be stored or displayed in any publicly accessible location
        v. End Users must not be able to log onto more than one workstation or location at a time.

vi. Individuals with End User IDs and Passwords will not give or share assigned End User ID and Passwords to access the System with any other organization, governmental entity, business, or individual.

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

c. Physical access to computers and other devices where System data is stored and/or accessible.
   i. Computers stationed in public places must be secured when workstations are not in use and staff are not present.
   ii. After a short period of time, a password protected screen saver will be activated during the time that the System is temporarily not in use.
   iii. Staff must log out of the System when leaving the workstation.

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

e. Hard Copy Security:
   i. i) Any paper or other hard copy containing PII that is either generated by or for the HMIS, including, but not limited to reports, data entry forms and signed consent forms will be secured.
   ii. ii) Agency staff will supervise at all times a hard copy with identifying information generated by or for the HMIS when the hard copy is in a public area. If the staff leaves the area, the hard copy must be secured in areas not accessible by the public.
   iii. iii) All written information pertaining to the End Username and password must not be stored or displayed in any publicly accessible location.

f. Remote Access to the HMIS:

   i. All HMIS End Users are prohibited from using a computer that is available to the public or from accessing the System from a public location through an internet connection that is not secured. End Users are not allowed to use Internet Cafes, Libraries, Airport Wi-Fi or other non-secure internet connections.
   ii. Staff must use remote laptops or desktops that meet the same security requirements as those office HMIS workstations.
   iii. Downloads from the HMIS may not include client PII.
   iv. Remote System access should be limited to situations in which it is imperative that the End User access the System outside of the normal office setting.
   v. Remote System access should reflect the requirements of job responsibilities.

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

Procedures:

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

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