

# **Program Management Information System of Alabama:**

***PromisAL***

## **Policies and Procedures**

**Version 1.0: October 12, 2007**

# Table of Contents

Table of Contents .....	2
Mission .....	5
Background .....	5
Introduction .....	5
I. Roles and Responsibilities.....	7
A. Governing Entity: Steering Committee .....	8
Policy: .....	8
Responsibilities: .....	8
B. Steering Committee Chair .....	10
Policy:.....	10
Responsibilities: .....	10
C. System Administrators.....	10
Policy:.....	10
Responsibilities: .....	10
D. Lead Agency of the State .....	11
Policy: .....	11
Responsibilities: .....	11
E. Continua of Care .....	12
Policy: .....	12
Responsibilities: .....	12
II. Implementation Policies and Procedures .....	14
A. Continuum of Care Participation Policy .....	15
Policy:.....	15
Procedure:.....	15
B. System Administrator Status Requirements .....	16
Policy: .....	16
Requirements: .....	16
C. PromisAL Hardware, Connectivity, and Security Requirements.....	17
Policy:.....	17
Requirements:.....	17
III. Operational Policies and Procedures .....	19
A. Continuum of Care Setup Procedures.....	20
Policy:.....	20
Procedure:.....	20
B. System Administrator Setup Procedures .....	21
Policy:.....	21
Procedure:.....	21
C. System Administrator Access Levels .....	22
Policy:.....	22
Procedure:.....	22
D. System Administrator Training Requirements .....	23
Policy: .....	23

Procedure:.....	23
E. PromisAL Data Collection Requirements.....	23
Policy: .....	23
Procedure:.....	23
F. Client Notification Policies and Procedures .....	25
Policy:.....	25
Procedure:.....	25
G. Inter-Continuum Data Sharing.....	28
Policy:.....	28
Procedure:.....	28
H. Sharing of Restricted Information through the Referral Process .....	28
Policy:.....	28
Procedure:.....	28
IV. Security Policies and Procedures.....	29
A. System Access Control.....	29
Policy:.....	29
Procedure:.....	29
B. Data Access Control Policies and Procedures .....	29
Policy:.....	29
Procedure:.....	29
C. Auditing Policies and Procedures.....	31
Policy: .....	31
Procedure:.....	31
V. Internal Operating Policies and Procedures.....	32
A. System Availability.....	32
Policy:.....	32
Procedure:.....	32
B. Software Technical Support Policies and Procedures .....	33
Policy: .....	33
Procedure:.....	33
VI. Data Ownership, Usage, and Release Policies and Procedures.....	34
A. Unduplication Policies and Procedures .....	34
Policy: .....	34
Procedure:.....	34
B. Data Quality Policies and Procedures .....	35
Policy: .....	35
Procedure:.....	35
C. Data Ownership Policies and Procedures .....	35
Policy: .....	35
Procedure:.....	35
D. PromisAL Data Uses and Disclosures Policies and Procedures .....	36
Policy: .....	36
Procedure:.....	36
E. Data Release Policies and Procedures .....	38
Policy: .....	38
Procedure:.....	38

VII. Acknowledgements .....39  
Appendix A: Continuum of Care Groups in Alabama.....40

## ***Mission***

*To advocate for the interests of the homeless and at risk populations of Alabama by serving them efficiently and effectively through recording, sharing, and analyzing data, while maintaining the highest level of integrity and confidentiality.*

## ***Background***

In 2001, Congress initiated a directive to the U.S. Department of Housing and Urban Development (HUD) to lead communities in developing an unduplicated count of the homeless population in America. This action was prompted by two factors: (1) cities such as Philadelphia were experiencing great success in using electronic data collection on their homeless population, and (2) national homelessness statistics were unreliable, thus skewing allocations of federal funding dollars.

In order to collect accurate data on homelessness and to be able to use this information to evaluate patterns of homeless program use and effectiveness, HUD challenged the communities to implement an information system; this would allow Congress, through HUD, to have a clearer picture of homelessness nationally, the first step in an initiative to solve the chronic homelessness problem. Subsequently, HUD required federally-funded public and nonprofit organizations to implement homeless management information systems. Homeless Management Information Systems (HMIS) are computerized data collection applications that facilitate the collection of information on homeless individuals and families using residential or other homeless assistance service agencies and store that data in centralized databases for different types of analyses.

Alabama realized that increased inter-agency communication would be a positive way to reduce homelessness and allocate resources more efficiently while fully complying with the HUD directive; therefore, several Continua of Care in Alabama chose to link their software to achieve the State of Alabama Multi-Implementation. This allows homeless data to be aggregated and presented at a national level to provide the information necessary to establish effective national policies to address homelessness.

## ***Introduction***

The Program Management Information System of Alabama (*PromisAL*) is a multi-implementation of HMIS that incorporates many areas of the State of Alabama. *PromisAL* is operated under a Steering Committee comprised of two representatives of each of the Continuum of Care groups across the State of Alabama (Appendix A: Continuum of Care Groups in Alabama).

Utilized software applications give homeless service providers throughout Alabama a means of tracking services and assessing service coverage and gaps. Software utilized

by *PromisAL* is an effective case management and data collection tool to aid the Continua in their efforts to prevent and end homelessness. Unduplicated counts of homeless persons and other aggregate, de-identified information can be generated and made available to policy makers, service providers, advocates, and consumer representatives. The Steering Committee is charged with balancing the unique interests and needs of all stakeholders involved: homeless and at risk men, women, and children; service providers; funders; policy makers; and healthcare providers. The following information outlines how this system is beneficial to each of the above stakeholders:

- **Social Workers/Case Managers, Homeless and At Risk Men, Women, and Children:** Social Workers/Case managers may document information about their clients in a way which will support the case management process. Case managers and clients will have access to on-line benefits, screening, and community resource information in order to learn about resources which will help clients find and keep permanent housing, or meet other goals clients have for themselves. Service coordination can be improved when information is shared among case management staff within one agency or, with appropriate client consent, with staff in other agencies who are serving the same clients.
- **Service Providers and Program Managers:** Program-level and agency-level information and reports will be accessible to agencies and program managers to provide a more complete understanding of clients' needs and outcomes, advocate for additional resources, complete grant applications, conduct evaluations of program services and staff performance, and report to fund providers. Minimally, the utilized software can generate the program portions of the HUD Annual Progress Report (APR), service-rendered reports, and bed night counts.
- **Policy Makers:** Because of the ease of extracting information from a computerized database, data may be analyzed in a timelier manner in order to support policy decisions that affect all stakeholders involved. Data elements can ultimately be used to identify risk factors for homelessness and effective prevention efforts against homelessness.
- **Healthcare Providers:** Through the use of HMIS, homeless and at risk persons can be referred to preventive or other appropriate healthcare services. This mitigates healthcare costs.
- **Taxpayers:** Because HMIS can record all client service transactions, a congregate listing of services received can aid in preventing service duplication and allow for more efficient usage of limited resources. This feature allows for greater coordination between agencies.

## **I. Roles and Responsibilities**

## **A. Governing Entity: Steering Committee**

**Policy: The Steering Committee will approve all major *PromisAL* policy decisions before they become effective.**

### **Responsibilities:**

Steering Committee structure will have two seats for each Continuum of Care (CoC): one each for the Homeless Management Information System (HMIS) Administrator and the CoC Chair or designee. Each CoC has two votes. In addition to CoC seats the Steering Committee will have one voting advisory seat representing the Alabama Governor's Statewide Interagency Council on Homelessness (SICH) and one non-voting technical advisory seat. The Steering Committee can add non-voting advisory seats, as needed for additional partners and subject matter experts.

The Steering Committee's role is fundamentally advisory to the overall *PromisAL* project. The *PromisAL* Steering Committee will work with the System Administrators within each Continuum of Care to maintain minimum standards throughout the statewide implementation as published in the Program Management Information System of Alabama (*PromisAL*): Policies and Procedures. The Steering Committee will collaborate with the Alabama Governor's Statewide Interagency Council on Homelessness (SICH) in its role to end homelessness in Alabama. Specifically, the Steering Committee will assist the SICH by providing aggregate data, according to the Data Release Policies and Procedures, to guide future decision-making and policy suggestions to the Governor.

The *PromisAL* Steering Committee will meet at least quarterly, at which time issues surrounding HMIS and its Policies and Procedures can be raised for discussion and/or approval. Of the four annual meetings, at least two must be in person and the other two may take place as conference calls.

The Steering Committee shall designate a Policy Sub-Committee with a representative from each Continuum who is also a member of the Steering Committee. This sub-committee exists to help enforce the implementation of *PromisAL* policies. This committee shall review issues assigned by the Steering Committee Chair and shall make recommendations to the full Steering Committee for final decision.

The Steering Committee shall designate a Data Work Group comprised of all CoC System Administrators and technical representative(s) as needed. The Data Work Group shall review data-related issues as assigned by the Steering Committee Chair. The Data Work Group shall submit regular audit reports to the Steering Committee on HMIS System Administration activities.

Specific responsibilities of the Steering Committee will include but are not limited to:

- Determine the Policies and Procedures for *PromisAL* implementation.
- Ensure minimum data collection requirements, as defined in *E. PromisAL Data Collection Requirements*.
- Encourage statewide provider participation.
- Encourage CoCs to develop policies that facilitate consumer involvement.
- Ensure all CoCs have a privacy policy in place for *PromisAL* implementation that meets or exceeds minimum standards as defined in the Program Management Information System of Alabama (*PromisAL*): Policies and Procedures.
- Define criteria, standards, and parameters for the usage and release of all data collected as part of *PromisAL*.
- Determine the necessity of an HMIS software change.
- Document, approve, and review at least annually the above policies in the form of the “Program Management Information System of Alabama (*PromisAL*): Policies and Procedures”.
- Establish statewide mechanisms for monitoring compliance with the approved SOPs.
- Compile and analyze *PromisAL* data with other provider and community data sources.
- Resolve or make recommendations where conflicts of interest exist.
- Issue sanctions for violations that cannot or should not be handled at the CoC-level.
- Identify the two persons who shall act as System Administrators II from the CoC-selected System Administrators I.
- Manage Inter-Continuum Data Sharing.
- Distribute Cost Burden (fixed, variable, and one time) above and beyond that of the Lead Agency.

To the extent that an SOP is identified which conflicts with applicable state or federal laws, then the *PromisAL* Steering Committee will work with the appropriate entities to amend the policy in order to resolve the conflict. The *PromisAL* Steering Committee may also identify procedures that need to be amended based on the initial implementation and/or ongoing operation of the system. If the *PromisAL* Steering Committee, Policy Sub-Committee, or Data Work Group identifies procedures that need to be amended, the process will include:

- Any individual, organization or Steering Committee or Work Group can raise concerns or recommendations for revisions to a specific policy or procedure.
- The *PromisAL* Steering Committee will direct the concern to the Policy Sub-Committee or an ad-hoc sub-committee to explore the concern and to develop a recommendation for full Steering Committee consideration. While a single committee may be identified as the primary entity generally responsible for overseeing the policies and procedures, another committee may be designated as the lead to explore a specific concern or recommendation.

- Proposed revisions must be presented to and approved by the Steering Committee by a simple majority vote, either in person or electronically.
- After approval, a list of all revisions, the date revised, and a brief description of the revisions will be incorporated into the Table of Contents in the Policies and Procedures manual.

The *PromisAL* Steering Committee is also charged with guiding System Administrator compliance. Presentations of questionable audit findings shall be made to the Steering Committee, at which time the Steering Committee may issue sanctions to users who are found to be in violation of security protocols.

## ***B. Steering Committee Chair***

**Policy: The Steering Committee Chair shall direct the efforts of the Steering Committee.**

### **Responsibilities:**

The responsibilities of the Steering Committee Chair shall include:

- Calling and facilitating meetings;
- Designating committees; and
- Assigning committee duties and tasks.

## ***C. System Administrators***

**Policy: The System Administrators will be responsible for managing the day-to-day technical aspects of the software.**

### **Responsibilities:**

#### **System Administrators I:**

The *PromisAL* System Administrators are responsible for:

- Receiving full training specific to their utilized software;
- Communicating system availability, planned outages, and other *PromisAL* information to Agency Administrators;
- Assigning user IDs to new users based on the approved licensing structure, authorized agency requests, and documentation of user training;
- Managing user accounts and application access control, in conjunction with Agency Administrators;
- Managing data sharing and security settings, based on submission of executed Interagency and Inter-Continuum Data Sharing Agreements;

## **System Administrators II:**

In addition to all of the responsibilities listed above, System Administrators II shall also be responsible for:

- Making application level changes to setups and configurations;
- Modifying and creating high-level formulae for reporting purposes; and
- Communicating significant application issues and/or system requests to the vendor;

## **Data Work Group:**

The System Administrators, as the Data Work Group, will also be responsible for developing, managing, updating, and executing needed reports for the *PromisAL* Steering Committee.

Specifically, that responsibility includes:

- Designing State- and Continuum-level reports;
- Testing reports;
- Moving reports to production environment;
- Designing and managing report structure and library;
- Generating funding-related reports and data analysis for the State or the Continuum;
- Managing report access control;
- Deactivating/retiring reports, as needed
- Communicating significant application issues and/or system enhancement requests to the current vendor;

The System Administrators may assign the report generating duties to an ad-hoc member of the Data Work Group, as necessary.

## ***D. Lead Agency of the State***

**Policy: The Lead Agency of the State shall be designated by the Steering Committee to manage the financial and logistical responsibilities of *PromisAL*.**

### **Responsibilities:**

The Lead Agency is that agency which holds and maintains the contract with the *PromisAL* software vendor and maintains a Memorandum of Understanding between each Continuum of Care. Responsibilities are limited to ascertaining contractual obligations are fulfilled. These responsibilities include:

- Establishing a fee structure;
- Invoicing participants according to contractual obligations; and

- Ordering user licenses at the request of the System Administrators for each Continuum.

## ***E. Continua of Care***

**Policy: Each Continuum of Care shall be responsible for developing and implementing policies and procedures for their HMIS, according to the HUD Data and Technical Standards Final Notice and the Program Management Information System (*PromisAL*): Policies and Procedures.**

### **Responsibilities:**

Each Continuum of Care that hosts an HMIS must develop and implement HMIS Policies and Procedures. These Policies and Procedures may go beyond those of the Program Management Information System of Alabama (*PromisAL*): Policies and Procedures, but they must include all topical areas that are covered therein. Continuum of Care Policies and Procedures must include the following:

- Local Roles and Responsibilities
- Implementation Policies and Procedures
  - Participation Policy
  - Initial Participation Requirements
  - Agency Information Security Protocol
  - Hardware, Connectivity, and Security Protocol
  - User Implementation Requirements
- Operational Policies and Procedures
  - Agency Setup Procedure
  - User Setup Procedure
  - User Access Levels
  - User Training Requirements
  - Client Setup Procedure
  - Client Notification Policy and Procedure
  - Data Collection Requirements and Timeframe for Entry
  - Interagency Data Sharing
  - Inter-Continuum Data Sharing
  - Sharing of Restricted Information in the Referral Process
- Security Policies and Procedures
  - System Access and Control
  - Data Access and Control
  - Auditing
- Data Ownership, Usage, and Release Policies and Procedures
  - Unduplication
  - Data Quality
  - Data Ownership
  - Data Uses and Disclosures

- Data Release

In addition to establishing Policies and Procedures, each Continuum must have at least one person to act as the System Administrator/HMIS Coordinator for that Continuum. This person shall hold the highest HMIS authority, in conjunction with the Continuum Agency/Organization, at the Continuum-level. This person shall also be expected to attend and participate in the quarterly *PromisAL* Steering Committee Meetings and to serve as a member of the Data Work Group of said committee.

## **II. Implementation Policies and Procedures**

## ***A. Continuum of Care Participation Policy***

**Policy: HUD requires that any Continuum of Care wishing to apply for or currently receiving HUD monies must participate in HMIS.**

### **Procedure:**

Beginning with the 2003 CoC and ESG grants, HUD requires all recipients of McKinney-Vento and homeless HOPWA grants to participate in the local HMIS. McKinney-Vento grants include Emergency Shelter Grants and Supportive Housing Program, Section 8 Moderate Rehabilitation SRO, Shelter Plus Care grants. This policy is consistent with the Congressional Direction for communities to provide data to HUD on the extent and nature of homelessness and the effectiveness of its service delivery system in preventing and ending homelessness. The *PromisAL* and its operating policies and procedures are structured to comply with the HUD Data and Technical Standards Final Notice. Recognizing that agencies may be further regulated by HIPAA and other Federal, State, and local laws, the Continuum may negotiate its procedures and/or execute appropriate business agreements with partner agencies so they are in compliance with applicable laws.

### **Participation Requirements:**

#### **Mandatory Participation:**

All agencies funded by HUD through the Continuum grant process must meet the Minimum Participation Standards of *PromisAL*, as defined by this Policy. Participating Continua of Care are required to comply with all applicable Policies and Procedures and must agree to execute and comply with a *PromisAL* Continuum Participation Agreement.

#### **Voluntary Participation:**

Only HUD-funded agencies are required to meet Minimum Participation Standards. However, HUD mandates that 75% of all beds in a Continuum, regardless of funding streams, will be covered in HMIS. Therefore, Continua of Care must strongly encourage non HUD-funded agencies to implement *PromisAL* with their homeless and at risk programs. While the Continuum cannot require non HUD-funded providers to participate in *PromisAL*, they will be expected to work closely with those agencies to articulate the benefits of the HMIS and to strongly encourage their participation in order to achieve a comprehensive and accurate understanding of homelessness in the State of Alabama.

### **Minimum Participation Standards:**

- Collecting the universal data elements, as defined in *E. PromisAL Data Collection Requirements*, for all programs operated by the agencies primarily serving persons who are homeless, formerly homeless, or at risk persons with agencies receiving ESG or HOPWA monies;
- Collecting program-specific data elements, as defined in *Data Collection Requirements*, for all clients served by the program funded by the aforementioned funding streams; and
- Entering client-level data into *PromisAL* within the CoC-established timeframe of client interaction, as defined by a CoC-generated Agency Participation Agreement. Data entry within 24 hours of client interaction is highly recommended.

Entered data will be used by the Data Work Group of the Steering Committee for analytical and administrative purposes including the preparation of reports to funders. A client has the right to refuse to have his or her data entered into the *PromisAL* database. The client's individual choice regarding participation will not affect his or her rights to services.

### ***B. System Administrator Status Requirements***

**Policy: The Continuum of Care selected *PromisAL* user who requires legitimate System Administrator access to the software will be granted such access upon completion of required training and execution of a *PromisAL* System Administrator Agreement or a CoC System Administrator Agreement.**

#### **Requirements:**

#### **Eligible System Administrators:**

The System Administrator II of the Continuum of Care which houses the Lead Agency shall authorize use of *PromisAL* to users who need access to the system for system administration, report writing, data analysis and report generation, or other essential activities associated with carrying out administrative responsibilities at the Continuum level.

System Administrator types and areas of access are defined in *C. System Administrator Access Levels*.

#### **System Administrator Requirements:**

Prior to being granted a username and a password, users must:

- Execute a *PromisAL* System Administrator Agreement or equivalent CoC System Administrator Agreement; and

- Successfully complete all *PromisAL* software application training required for the System Administrator user level. (Training requirements are documented in D. System Administrator Training Requirements.)

*PromisAL* System Administrators must be aware of the sensitivity of client-level data and take appropriate measures to prevent unauthorized disclosures. System Administrators are responsible for protecting institutional information to which they have access and for reporting security violations to the appropriate authority. System Administrators must comply with all policies and standards described in the Program Management Information System of Alabama (*PromisAL*): Policies and Procedures. They are accountable for their actions and for any actions undertaken with their usernames and passwords.

### **Compliance Guidance:**

All potential violations of any security protocols will be investigated by the *PromisAL* System Administrators Peer Review Group. Any System Administrator found to be in violation of the security protocols will be sanctioned according to the procedure delineated in C. Auditing Policies and Procedures. The choice of actions taken would depend on the frequency, prior training, severity of violation, and intent. Actions taken may include, but are not limited to:

- Presentation of Peer Review Group findings to Steering Committee;
- Suspension of system privileges; or
- Revocation of system privileges.

## ***C. PromisAL Hardware, Connectivity, and Security Requirements***

**Policy: Any computer that interfaces with *PromisAL* must meet the minimum vendor hardware and connectivity specifications and the security specifications, according to HUD.**

### **Requirements:**

#### **Computer System Requirements for HMIS:**

Every Continuum of Care must maintain the appropriate hardware and connectivity according to the software vendor specifications.

#### **Security Specifications:**

All workstations directly accessing *PromisAL* and any workstation that is on a network that has a workstation(s) directly accessing *PromisAL* must have:

- Operating System updates. Operating system updates must be downloaded and applied automatically or on a regular basis.

- Firewall protection (in addition to or other than Windows Firewall).
- Virus protection software.
- Anti-spyware software.
- PC, LCD, or Laptop Privacy Screen (**This level of security is suggested but optional.**).

**Certain internet security software is available at reduced rates for non-profit organizations to download at <http://www.techsoup.org>.**

Other products available may come at a cost or for free. Be aware that many free versions are for personal (not business) use only. Norton®, F-Secure®, and ZoneAlarm® offer suites that have all-in-one security and have received high ratings from Consumer Reports (September 2006, pp 20-29).

### **III. Operational Policies and Procedures**

## ***A. Continuum of Care Setup Procedures***

**Policy: The *PromisAL* System Administrator may set up a new Continuum of Care account, based on the following procedure.**

### **Procedure:**

Prior to setting up a new Continuum of Care within the *PromisAL* database, the Chair or the Director of the proposed CoC must complete the required implementation requirements outlined in II. Implementation Policies and Procedures.

The System Administrator of the CoC in which the Lead Agency is housed shall:

- Verify that the required documentation has been correctly executed and submitted, including:
  - Certification of Initial Implementation Requirements;
  - Executed Continuum of Care Participation Agreement;
  - Designation of System Administrator; and
  - Payment of all *PromisAL*-related fees.
- Request and receive approval from the vendor and the Lead Agency to set up a new CoC.
- Setup a profile for the new Continuum within *PromisAL* authorizing software use.

### Data Migration from former system:

A CoC joining *PromisAL* may have already initiated HMIS data collection and have data they would like to integrate into *PromisAL*. Data Migration from existing systems shall take place under the following circumstances:

- The Lead Agency shall initiate contact with the *PromisAL* software vendor
- The System Administrator from the new CoC shall negotiate pricing with the vendor based on the amount and format of data to be moved.
- Issues experienced by the System Administrator during these negotiations or processes should be raised with the System Administrators II for further discussion or action.
- If costs should exceed the limit of what a Continuum can afford so that they may join the Statewide Implementation, a vote will go to the Steering Committee to decide if funds shall be allocated from other Continua to assist the new Continuum's efforts.

## ***B. System Administrator Setup Procedures***

**Policy:** The *PromisAL* System Administrator may create a new System Administrator User ID for eligible individuals based on the following procedure.

### **Procedure:**

In order for a Continuum of Care to authorize System Administration rights for a new user, the Continuum Chair or Director (or an authorized designee) must:

- Authorize the creation of a user account for the specified individual by completing a *PromisAL* System Administrator Request Form, included in the CoC Participation Packet.

The proposed *PromisAL* System Administrator must:

- Attend applicable training as described by D. System Administrator Training Requirements.
- Execute a *PromisAL* System Administrator User Agreement.

The System Administrator for the CoC in which the Lead Agency is housed must:

- Review HMIS records about potential System Administrator to ensure that the individual does not have previous policy and procedure violations that would prohibit access to *PromisAL*, as determined by the *PromisAL* System Administrators in conjunction with the *PromisAL* Steering Committee.
- Verify that the required documentation (*PromisAL* System Administrator Agreement has been correctly executed and submitted).
- Verify that required training has been successfully completed.
- Approve the new user request electronically by assigning a user ID and a temporary password.

The CoC Chair or Director (or authorized designee) is responsible for immediately notifying a *PromisAL* System Administrator II regarding terminating user access if that CoC's System Administrator leaves employment with the agency, or otherwise no longer needs access to *PromisAL*, following the procedures outlined in B. Data Access Control Policies and Procedures.

The CoC Chair or Director is also responsible for ensuring that the System Administrator understands and complies with all applicable Program Management Information System of Alabama (*PromisAL*): Policies and Procedures.

**C. System Administrator Access Levels**

**Policy: Each PromisAL user must be assigned a designated user access level that controls the level and type of access the individual has within the system.**

**Procedure:**

All PromisAL System Administrators must be assigned a designated access level that controls the level and type of access that System Administrator has within the system. A model of least-privilege is used: no user will be given more than the least amount of privilege needed to perform his or her particular duties.

**System Administration II:**

The System Administrator II will have access to system-wide data in order to accomplish his or her system administration and reporting responsibilities. The System Administrator II is not bound by his or her Continuum of Care and can view and extract client-level data from any provider. This does not imply that any System Administrator II should view data outside of his or her own CoC without appropriate authorization.

**System Administrator I:**

The System Administrator I may perform all system maintenance and reporting tasks within the defined limits of his or her own Continuum. For assistance with tasks that require shadowing a user within his or her CoC, the System Administrator I should notify a System Administrator II, who has the shadowing capability.

All system-level users will sign confidentiality agreements and execute a PromisAL System Administrator Agreement. Occasionally, a vendor customer service representative may be granted access to data to manage and test application development and administration functions or to correct a problem within the system.

Area / Access Level	ResourcePoint	Edit All Provider Profile Screens	Edit System-wide news	Edit Agency News	View or Edit Client Profile	ShelterPoint	Service Transactions	Assessments	Case Plans	Default Reports	Custom Reports	Edit User Information	Create or Delete Users	Shadow Mode	Merge Clients	Duplicate Client Report
System Administrator I	X	X	X	X	X	X	X	X	X	X	X	X	X			
System Administrator II	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

## ***D. System Administrator Training Requirements***

**Policy: *PromisAL* System Administrators must successfully complete the training required for their user access levels.**

### **Procedure:**

Prior to gaining access to the *PromisAL* application, users must successfully complete the following training:

- System Administrator training (provided by a vendor representative or other appointed System Administrator)

In addition to completing application training, System Administrators must understand Data Quality and Computer Ethics and be prepared to train end users within their respective continua on these topics.

## ***E. PromisAL Data Collection Requirements***

**Policy: All Participating Agencies that provide service for homeless and at risk persons are encouraged, and in some cases required, to collect data for some or all clients served by their programs, as specified by these procedures.**

### **Procedure:**

#### **Universal Data Elements:**

Each Continuum is responsible for ensuring that a minimum set of data elements, referred to as the Universal Data Elements, will be collected and/or verified from all clients of HUD-funded agencies to be entered into the HMIS system.

Universal Data Elements include:

- First, Middle, Last Name, and Suffix
- Social Security Number and Data Quality
- Date of Birth or estimated Date of Birth (age)
- Ethnicity and Race
- Gender
- Veteran Status
- Disabling Condition
- Length of Current Episode of Homelessness
- Number of Previous Episodes of Homelessness
- Residence Type Prior to Program Entry and Length of Stay
- Zip Code of Last Permanent Residence and Data Quality
- Program Entry and Exit Dates
- Household Affiliation for the purposes of this Program Entry

HUD-funded Agencies must report client-level data for the Universal Data Elements using the required response categories detailed in Exhibit 3: Required Response Categories for Universal Data Elements of the HUD Data and Technical Standards Final Notice.

### **Program-Specific Data Elements:**

All Participating Agencies are also responsible for ensuring that the following assessment data elements, referred to as Program-Specific Data Elements, are collected from each client served. It is highly recommended that these Program-Specific Data Elements be entered into *PromisAL* within 24 hours of collecting the information. The Program-Specific Data Elements are located throughout the *PromisAL* application.

Program-Specific Data Elements include:

- Causes of Homelessness (Program Entry)
- Income Sources and Amounts (Program Entry and Exit)
- Sources of Non-Cash Benefits (Program Entry and Exit)
- Presence of Disability (Program Entry)
- History of Domestic Violence and Timeframe (Program Entry)
- Services Received (Throughout Program Enrollment)
- Referrals Provided (Throughout Program Enrollment)
- Destination upon Leaving (Program Exit)
- Reasons for Leaving (Program Exit)
- Program Outcomes (Throughout Program Enrollment or at Program Exit)

HUD-funded Agencies must provide client-level data for the Program-Specific Data Elements using the required response categories detailed in Exhibit 4: Required Response Categories for Program-Specific Data Elements of the HUD Data and Technical Standards Final Notice.

Individual Continua of Care reserve the right to increase the minimum required data elements through their grant contract processes independent of this SOP.

### **Domestic Violence, Unaccompanied Youth, and Anonymous HMIS Data Collection Requirements:**

HUD-funded Agencies in Participating Continua who provide services for Victims of Domestic Violence and Unaccompanied Youth must adhere to federal regulations regarding the transmission of data for these special populations.

*Note that this section should not be considered final, and may be revised as a result of the specific discussions at the Federal, State and Local level..*

Agencies that work with clients who wish to remain anonymous shall collect the Universal and Program-Specific data elements as defined above. They shall, however, enter Anonymous Client-level Data into *PromisAL*.

Anonymous Client-level Data are defined as individual client records that contain no personal client identifying information, in whole or in part, or any information that may be used to construct a person's identity. No one beyond the originating agency will have access to any client's personal identifying information through *PromisAL*.

Client personal identifying information is defined as the following data fields:

- Name(s) or Aliases
- Social Security Number
- Date of Birth
- Unique Identifying Characteristics
- Zip Code of Residence Prior to Program Entry
- Emergency Contact Information
- Any other data fields that may be used to leverage the identity of any individual client.

\*A unique client identifier shall be automatically assigned to each anonymous client by the *PromisAL*. The unique client identifier shall not contain any masked client personal identifying information. The unique client identifier shall not contain, in whole or in part, any client personal identifying information as listed in the above fields. The unique client identifier provides an unduplicated internal count of clients served by the Agency, and provides the Continuum the means of conducting longitudinal analysis of services provided to each client.

## ***F. Client Notification Policies and Procedures***

**Policy: Participating Agencies shall use the required client notification and/or consent procedure prior to entering any client-level data into *PromisAL*.**

### **Procedure:**

All verbal and written client notification and consent must include a statement that no client will be denied services for refusal to consent. Participating Agencies may either use the standard *PromisAL* Privacy and Confidentiality Policy Guidelines developed by the Steering Committee or incorporate the content of the *PromisAL* documents into the Agency's own documentation. All written consent forms must be stored in a client's case management file for record keeping and auditing purposes.

Agencies must make reasonable accommodations for persons with disabilities throughout the data collection process. This may include but is not limited to, providing qualified sign language interpreters, readers or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability.

Agencies that are recipients of federal assistance shall provide required information in languages other than English that are common in the community, if speakers of these

languages are found in significant numbers and come into frequent contact with the program.

### **Definitions and Descriptions of Client Notifications and Consent Procedures:**

#### **Client Notice:**

A written notice of the assumed functions of the *PromisAL* must be posted and given to each client so he or she is aware of the potential uses of his or her information and where it is stored. To fulfill this requirement, the agency may either adopt the *PromisAL* Privacy and Confidentiality Policy Guidelines or may develop a Privacy Notice that is equivalent to or more stringent than the *PromisAL* Privacy and Confidentiality Policy Guidelines. If the agency has a website, the adopted Privacy and Confidentiality Policy Guidelines or equivalent privacy notice must also be posted on the website.

Consent is required to have the client's information entered into *PromisAL*. As part of the notification process, clients must be informed of their right to designate their client record as anonymous and their right to refuse to have their information entered into *PromisAL*. Clients also have the right to view a copy of their records upon request.

#### **Client Refusal:**

After learning about *PromisAL*, if a client does not wish to have his/her information entered into the system, the service provider is procedurally and legally barred and prohibited from entering such information into the system. The client's individual choice regarding participation will not affect his or her rights to services.

#### **Anonymous Client:**

A client may choose to be entered into the system anonymously. For anonymous client data entry, refer to E. *PromisAL* Data Collection Requirements.

#### **Closed Client Record:**

After learning about *PromisAL*, if a client does not wish to have his/her Primary Identifiers accessible to all *PromisAL* users, the originating *PromisAL* user should close that client's record (see vendor documentation for instructions on closing a client's record). A client's record may be closed completely or closed with exceptions. Closing a client's record will hide all of the client's information from all other users of the system, excluding the System Administrators. Closing a client's record "with exceptions" hides the client's information from all users except those that are in agencies or programs that are listed as exceptions. This closed client record will allow the agency to access the client's information for agency purposes, while protecting the client's rights to privacy. However, users should be aware that closing records should be reserved for extreme circumstances as they may lead to duplications within the system.

### Deletion of Client Records:

A client has the right to request the deletion of his or her record from the system. At that time, a written request should be submitted to the originating agency. The originating agency should then notify its System Administrator. After reviewing that client's file, the System Administrator will notify the vendor so that they may permanently delete the client record. All other agencies that have had HMIS-recorded contact will be notified of that client's deletion by the System Administrator.

### Written Client Consent for Interagency and Inter-Continuum Data Sharing:

Clients will be notified through the *PromisAL* Privacy and Confidentiality Policy Guidelines that certain agencies participating in *PromisAL* will be able to view their Personal Identifying Information. At any given time, a list of the agencies participating in Interagency and Inter-Continuum Data Sharing will be available. Written client consent to share Personal Identifying Information with other Participating Agencies will be obtained as part of the client's signed and dated Release of Information (ROI).

### Written Client Release of Information for Sharing of Restricted Information through the Referral Process:

At any point during the case management process, an agency staff member can initiate a referral to another agency. *PromisAL* provides functionality to automate the referral and to provide users at the recipient agency with access to a specified portion of the originating agency's client record as part of the referral. In order to provide access to client data with a referral, the originating agency must receive a secondary client Release of Information (ROI) that specifically indicates the name of the recipient agency, the purpose for sharing, the specific data categories that are being shared, the expiration of the consent, and whether or not the originating agency has permission to receive information back from the referral agency on the outcome of the referral. Any client data can potentially be sent through the referral process based on client release. To fulfill this requirement, the agency may develop an internal form that contains the fields identified above.

### **Applicability:**

In all cases, the Participating Agency shall uphold Federal and State Confidentiality regulations to protect client records and privacy. If an agency is covered by more stringent regulations, the more stringent regulations prevail.

### **Privacy Compliance and Grievance Policy:**

Agencies must establish a regular process of training users on this policy, regularly auditing that that policy is being followed by agency staff (including employees, volunteers, affiliates, contractors and associates), and receiving and reviewing complaints about potential violations of the policy.

### ***G. Inter-Continuum Data Sharing***

**Policy: The PromisAL Steering Committee allows data sharing among agencies upon signing of appropriate MOU by Participating Continua.**

**Procedure:**

#### **Written Agreement:**

Continua wishing to share information electronically through *PromisAL* are required to establish a data sharing network in writing by jointly executing the appropriate Memorandum of Understanding (MOU), as provided by the *PromisAL* Steering Committee.

#### **Role of Continuum Chair or Director:**

The Continuum Chair or Director is responsible for ensuring that all users within his or her continuum abide by all the policies stated in the Program Management Information System of Alabama (*PromisAL*): Policies and Procedures as well as those in the appropriate MOU(s). Chairs or Directors for Continua wishing to participate in the data-sharing network must sign the appropriate MOU(s).

#### **Client Authorization:**

Case Managers from agencies in continua that have a valid MOU may only share client information if the client authorizes that sharing with a valid Client Consent Form (Release of Information).

Continua are strongly encouraged to share (at a minimum):

- Personal Identifiers (Name, Social Security Number, Date of Birth, Gender)
- HUD Universal Data Elements
- Service Transactions

### ***H. Sharing of Restricted Information through the Referral Process***

**Policy: Agencies will be able to share client information beyond those elements supported by the Data Sharing MOU with appropriate written client consent.**

**Procedure:**

Any client information stored in the client record of an originating agency may be shared with another Participating Agency in another continuum based on a second written client Release of Information (ROI) that allows for the sharing of restricted information that specifically indicates the recipient agency, purpose for sharing, the specific data categories that are being shared, the expiration of the consent, and whether or not the originating agency has permission to receive information back from the referral agency on the outcome of the referral.

## **IV. Security Policies and Procedures**

### ***A. System Access Control***

**Policy: *PromisAL* must be reasonably secured from access by unauthorized users.**

**Procedure:**

#### **Central Server Access Controls:**

The central server for *PromisAL* is housed with the current vendor. It will take all appropriate measures to control unauthorized access to client data.

The vendor will determine the physical access controls appropriate for the environment housing the central *PromisAL* server based on its security policies, standards, and guidelines. All those granted access to an area or to data are responsible for their actions. Additionally, if an individual gives access to another person, the authorizing individual is responsible for the other person's activities.

#### **Workstation Access Controls:**

Agency Administrators, in conjunction with their System Administrator, will determine the physical access controls appropriate for their organizational setting based on the Program Management Information System of Alabama (*PromisAL*): Policies and Procedures. Each agency workstation should meet appropriate and current security protection, as specified in C. *PromisAL* Hardware, Connectivity, and Security Requirements.

### ***B. Data Access Control Policies and Procedures***

**Policy: *PromisAL* must be reasonably secured to protect data from access by unauthorized users.**

**Procedure:**

## **User Accounts:**

System Administrators must follow the procedures documented in II. Implementation Policies and Procedures for user account set-up, including appropriate training and establishment of appropriate user access level. It is the responsibility of the System Administrator's supervisor to notify the System Administrator for the Continuum which houses the Lead Agency immediately when that System Administrator no longer requires access to *PromisAL*.

Users should only be logged into *PromisAL* from one workstation at any given time.

## **User Passwords:**

Each user must have a unique identification code (user ID). Each user's identity will be authenticated using a user password. Passwords are the individual's responsibility. Users are prohibited from sharing passwords. Sanctions will be imposed on the user and/or agency if account sharing occurs.

Passwords should not be written down. Users should not have passwords saved on a personal computer for easier log on.

## **Temporary Suspension of User Access to Database Resources:**

### **System Inactivity:**

Users must logoff from *PromisAL* and the workstation if they leave their workstation. Inactivity time-out thresholds have been implemented by the vendor to protect *PromisAL* information. Therefore, if a user is logged onto a workstation, and the period of inactivity on the workstation exceeds the 30-minute inactivity time period, the user will be automatically logged off of the system.

### **For Cause Temporary Suspension:**

If any user is being reviewed for possible violations, his or her password may be temporarily suspended.

## **Electronic Data Controls:**

### **Continuum Policies Restricting Access to Data:**

The Participating Continua must establish internal access to data protocols based on the HUD Data and Technical Standards Final Notice.

### **Raw Data:**

Some users will be granted access to the functionality to download and to save the client-level data onto their local computers. Once this information has been downloaded from the *PromisAL* database in raw format to an Agency's computer, this data then becomes the responsibility of the agency.

#### Ability to Export Continuum-Specific Data from *PromisAL*:

Participating Agencies will have the ability to export a copy of their own data for internal analysis and use. Agencies are responsible for the security of this information.

#### Hardcopy and Digital Data Controls:

Printer versions (hardcopy) of confidential data should not be copied or left unattended and open to compromise. Media containing *PromisAL* client-identified data may not be shared with any person or agency other than the owner of the data for any reason not disclosed within the Client Notice.

Continuum policies, consistent with applicable state and federal laws, should be established regarding appropriate locations for storage, transmission, use and disposal of *PromisAL*-generated hardcopy or digital data. *PromisAL* data may be transported by authorized employees using methods deemed appropriate by the participating agency that meet the above standard. Reasonable care should be used, and media should be secured when left unattended. Magnetic media containing *PromisAL* data which is released and/or disposed of from the participating organization should first be processed to destroy any data residing on that media. Degaussing and overwriting are acceptable methods of destroying data. *PromisAL* information in hardcopy format should be disposed of properly. This may include mechanical shredding.

### ***C. Auditing Policies and Procedures***

**Policy: The System Administrators will monitor system access that could potentially reveal a violation of security protocols.**

**Procedure:**

#### Access Monitoring Plan:

The *PromisAL* software application maintains an audit trail that tracks user log-in attempts, for a minimum of six months. The *PromisAL* application also maintains an audit trail that tracks the deletions to client records (including the actual assessment entry, date deleted, and username) for a minimum of six months and a record of deleted client records (case number, intake information, data deleted, and username) for a minimum of one year. The *PromisAL* application is designed to record transactional

data on all other client information for historical and audit purposes. Each entry shall also reflect the user that created the entry and the date and name of the user that made the most recent modification. *PromisAL*-selected software is designed to automatically fulfill these obligations.

The System Administrators must review System Administrator audit records at least quarterly for evidence of violations of system misuse. Audits may include reviews of user viewing, editing, and deleting client records. System Administrators will be required to submit monthly reports regarding *PromisAL* activities to their respective Continuum Chairs or Directors, accounting for any inconsistencies.

All users and custodians are obligated to report suspected instances of noncompliance and/or security violations to the appropriate Continuum Chair or Director or the Steering Committee Chair.

### **Compliance Guidance:**

All potential violations of any security protocols will be investigated by the *PromisAL* System Administrators Peer Review Group. Any System Administrator found to be in violation of the security protocols will be sanctioned according to the procedure delineated in C. Auditing Policies and Procedures. The choice of actions taken would depend on the frequency, prior training, severity of violation, intent, etc. Actions taken may include, but are not limited to:

- Presentation of Peer Review Group findings to Steering Committee;
- Suspension of system privileges; or
- Revocation of system privileges.

All *PromisAL* sanctions will be imposed by the Steering Committee. Sanctions can be appealed to a group comprised of the Steering Committee and any necessary ad hoc members.

## **V. Internal Operating Policies and Procedures**

### ***A. System Availability***

**Policy:** The *PromisAL* application will be consistently available to users and users will be promptly informed of any interruption to service.

**Procedure:**

*These guidelines are provided as a reference; however, the official document for system operation is held by the PromisAL vendor.*

### **Hours of System Operation:**

The present *PromisAL* vendor allows 24-hour access. Scheduled maintenance of *PromisAL* will inconvenience as few users as possible.

### **Planned Interruption to Service:**

The System Administrator for the Continuum in which the Lead Agency is housed will identify times for planned security patches and upgrades in coordination with the vendor. System users will be notified in advance on the vendor's application and by email from their respective System Administrators. An explanation of the need for the interruption, expected duration, and benefits or consequences will be provided.

### **Unplanned Interruption to Service:**

Users will be notified as to appropriate procedures.

## ***B. Software Technical Support Policies and Procedures***

**Policy: *PromisAL* System Administrators will offer standard software application technical support services to all Participating Agencies and users.**

### **Procedure:**

#### **Technical Support Resolution Procedure – Use of the *PromisAL* Application:**

As unanticipated technical support questions arise on the use of the *PromisAL* application, users should follow the procedure below to resolve their questions:

- Refer to training materials.
- If question is still unresolved, direct the technical support question to the Agency Administrator.
- If the question is still unresolved, the Agency Administrator can further direct the question to the appropriate System Administrator.
- If the question is still unresolved, a System Administrator II can further direct the question to the vendor's customer service representative for resolution.

#### **Technical Support Resolution Procedure – Access to the *PromisAL* Application or Database:**

If a user experiences an unplanned interruption to *PromisAL* operation, users should follow the procedure below to notify their respective System Administrators and/or understand the status of operations:

- Contact the Agency Administrator, who should immediately check the status of the Agency's Internet Service Provider.

- If the system outage is unrelated to the agency's internet connectivity, the Agency Administrator should contact the System Administrator to immediately report the interruption.
- The Agency Administrator should communicate the results of the status update to all agency users who may attempt to use *PromisAL* during the period of interruption.

### **Report Generation:**

System Administrators will be a resource to agency staff as they develop reports but will only be available to provide a limited, reasonable level of support to each agency.

### **Programming-Related Service Requests:**

If a user encounters programming issues within the *PromisAL* application that need to be addressed, the user should identify the error or make a suggested improvement to the Agency Administrator. The Agency Administrator should notify the System Administrator, identifying the specific nature of the issue or recommended improvement along with the immediacy of the request.

Service requests will be reviewed by the System Administrator for further action. Requests to fix programming errors or "bugs" will be prioritized and forwarded to the vendor, as appropriate.

## **VI. Data Ownership, Usage, and Release Policies and Procedures**

### ***A. Unduplication Policies and Procedures***

**Policy: *PromisAL* System Administrators II will employ various methodologies to achieve an unduplicated client database and to accommodate the unique situations of different provider types.**

#### **Procedure:**

The *PromisAL* application will use the following data elements to create unduplicated client records:

- Name (First, Middle Initial, Last, Suffix)
- Date of Birth (actual or estimated)
- Gender
- Race and Ethnicity
- Social Security Number (full or partial)

In order to achieve unduplication it is recommended that the end user performs the client search using minimal data elements entered in *PromisAL*. Based on the results, the user will be asked to select a matching record if the other identifying fields match correctly. If the user is unsure of a match (either because some data elements differ or because of blank information), the user should ask the client for more information and/or create a new client record. If the difference between the information of client to be put in the system and the one already in the system is minimal, like a letter in one part of the name is different or only the gender is different, it is recommended that the user enter the client's information under that profile, making appropriate changes to incorrect information. If the difference is too great or if the user is unsure if it is the same client, the user should create a new client profile.

If there appears to be a potential duplicate in the system, the user should notify his or her respective System Administrator, who will then take the appropriate steps to rectify the issue.

System Administrators II have the ability to run a default report to detect duplicated clients. An appointed System Administrator II will generate this report at least every six months. When duplicates are detected, the appointed System Administrator II should use duplicate files to create a single client record.

## ***B. Data Quality Policies and Procedures***

**Policy: All data entered into *PromisAL* and/or used by the System Administrators or the Steering Committee for analytical or reporting purposes must meet the data quality standards.**

### **Procedure:**

In order to ensure data quality, accurate and relevant data will be entered in a timely manner. Users will complete the required data elements, according to E. *PromisAL* Data Collection Requirements. The following procedures will be conducted to be sure that the data in the *PromisAL* are appropriate:

- Identifiers will be removed from data that is not in current use after 7 years from date of creation or last edit unless other requirements mandate longer retention.
- Data quality is subject to routine audit by the System Administrators who have administrative responsibilities for the database.

## ***C. Data Ownership Policies and Procedures***

**Policy: All data is governed by the owner(s) of the data with regard to data use and disclosure.**

### **Procedure:**

The client ultimately retains ownership of any identifiable client-level information that is stored within *PromisAL*. If the client consents to share data, the client, or agency on behalf of the client, has the right to later revoke permission to share his/her data without affecting his/her rights to service.

Identifiable client-level data may only be stored and accessed within *PromisAL* in accordance with the client notification and consent documents.

In cases where agencies and clients agree to share identifiable client-level data, this information may only be shared in accordance with client notification and consent documents, G. Inter-Continuum Data Sharing, and H. Sharing of Restricted Information through the Referral Process.

In the event that a Participating Agency withdraws from *PromisAL*, the agency will retain ownership of the identifiable client-level data that has been entered into the system. The System Administrators shall make reasonable accommodations to assist that agency in exporting their data in a format that is usable in an alternative database. In this circumstance, any agency-entered client-level data must be de-identified in order to remain in the *PromisAL* database. This de-identified information shall remain available to the Continuum and to the Steering Committee for analytical purposes. For the purposes of de-identification, the vendor's identification number shall not be considered an identifying data element.

#### ***D. PromisAL Data Uses and Disclosures Policies and Procedures***

**Policy: All parties that have access to *PromisAL* data will follow the data disclosure policies and procedures to guide the use and disclosure of client information stored in or generated by *PromisAL*.**

#### **Procedure:**

Each Participating Continuum must adopt the standard Privacy Notice or incorporate the standard notice into a pre-existing privacy notice that is equivalent to or more stringent than that established by the *PromisAL* Steering Committee. Every agency must post and explain the notice to each client and have a copy available at the client's request. If an agency maintains a public website, the agency must post the most current version of its privacy notice on the website.

An agency's Privacy Notice must:

- Specify all potential uses and disclosures of client personal information.
- Specify the purpose for collecting the information.
- Specify the time period for which the data will be retained at the agency and the method for disposing of it or removing identifiers from personal information that is not in current use 7 years after it was created or last changed.
- State the process and applicability of amendments, and commit to documenting all privacy notice amendments.

- Offer reasonable accommodations for persons with disabilities and/or language barriers throughout the data collection process.
- Allow the individual the right to inspect and to have a copy of their client record and offer to explain any information that the individual may not understand.
- Specify a procedure for accepting and considering questions or complaints about the privacy and security policies and practices.

### **State Steering Committee-Approved Uses and Disclosures:**

*PromisAL* client data may be used or disclosed for (1) case management, (2) administrative, (3) billing, (4) analytical purposes, and (5) other purposes as required by law. Uses involve sharing parts of client information with persons within an agency. Disclosures involve sharing parts of client information with persons or organizations outside of an agency.

- **Case Management Uses and Disclosures:** Agencies may use or disclose client information for case management purposes associated with providing or coordinating services. Data will be shared with other agencies upon the signing of the appropriate Memoranda of Understanding. Sharing of data beyond those covered by the Memoranda of Understanding would require a secondary Release of Information in order to disclose restricted information.
- **Administrative Uses and Disclosures:** Agencies may use client information internally to carry out administrative functions, including but not limited to audit, personnel oversight, and management functions.
- **Billing Uses and Disclosures:** These include functions related to payment or reimbursement for services (e.g., Medicaid billing). An example might include generating aggregate reports for the people and organizations that fund an agency. A client's personal information may be disclosed for billing or reimbursement purposes, if required by the payor/billing agency.
- **Analytical Uses and Disclosures:** Agencies may use client information for internal analysis. An example would be analyzing client outcomes to evaluate program effectiveness. Agencies will disclose portions of a client's information without the personal identifiers for analytical purposes related to analyzing client data, including but not limited to understanding trends in homelessness and needs of persons who are homeless.
- **Other Purposes as Required by Law:** Agencies may disclose client-level data, for example, in response to a subpoena.

## ***E. Data Release Policies and Procedures***

**Policy:** All *PromisAL* stakeholders will follow the data release policies and procedures to guide the release of client information stored in or generated by *PromisAL*.

**Procedure:**

### **Transmission and Storage of Data:**

All data must be classified and treated according to one of the following definitions. All of these data classifications are controlled by the data release criteria defined below.

- **Confidential Data:** Confidential data is information that identifies clients contained within the database. Examples include Social Security number, address, or any other information that can be leveraged to identify a client. Specific identifiable data elements are described in E. *PromisAL* Data Collection Requirements. Confidential data requires appropriate security and protection at all times as described in B. Data Access Control Policies and Procedures.
- **Internal Data:** Internal data is any information that is scheduled, but not yet approved, for publication. Examples include draft reports, fragments of data sets or data without context, accessible only to internal employees. No auditing is required. No special requirements surround destruction of these data. These data must be stored securely and can be transmitted via internal or first class mail.
- **Public Data:** Public data is any information that is published according to Data Release policies. Additional security controls are not required.

### **Data Release Criteria:**

*PromisAL* client data will only be released in aggregate or anonymous client-level data formats for purposes beyond those specified in E. Data Release Policies and Procedures, according to the criteria specified below.

- **Client-Identified Data Release Criteria:** No identifiable client data will be released to any person, agency, or organization that is not the owner of said data for any purpose other than those specified in D. *PromisAL* Data Uses and Disclosures Policies and Procedures without written permission from the owner.
- **Aggregate Data Release Criteria:** All data must be anonymous, either by removal of all identifiers and/or all information that could be used to infer an individual or household's identity. Aggregate data must represent sixty percent (60%) of the clients in that universe (program, agency, subpopulation, geographic area, etc.), unless otherwise required for the Congressional AHAR.

Only Participating Agencies can authorize release of aggregate data or program-specific information beyond the standard reports compiled by the continua agencies for funding purposes. There will be full access to aggregate data for all Participating Agencies. Parameters of the aggregate data (e.g., where the data comes from, what it includes and what it does not include) will be presented to each requestor of aggregate data. Released aggregate data will be made available in the form of an aggregate report. Special care should be taken when there are fewer than eight (8) clients in an aggregate report.

- **Anonymous Client-Level Data Release Criteria:** All data must be anonymous, either by removal of all identifiers and/or all information that could be used to infer an individual or household's identity. Program-specific information will not be released without the written consent of the agency's CEO or Executive Director. Parameters of the data (e.g., where the data comes from, what it includes, and what it does not include) will be presented to each requestor of data.

### **Data Release Process:**

Beyond individual agency reports or continuum reports on its funded programs, the *PromisAL* Steering Committee must approve the release of data for public.

## **VII. Acknowledgements**

In the process of creating the Program Management Information System of Alabama (*PromisAL*): Policies and Procedures, several documents were used as models and templates. These sources include the "Chicago Enterprise Case Management System: Standard Operating Procedures for the ECM-HMIS Implementation", "Wisconsin ServicePoint: Standard Operating Procedures", "Michigan Statewide Homeless Management Information System", and "State of Massachusetts: Outline of Standard Operating Procedures (SOPs) Manual". Special thanks to the Department of Housing and Urban Development for providing Technical Assistance on this project.

## **Appendix A: Continuum of Care Groups in Alabama**

Alabama Rural Coalition for the Homeless (ARCH)  
Community Homelessness Assessment Linkage and Networking Group (CHALENG of Tuscaloosa)  
Homeless Care Council of Northwest Alabama (HCCNWAL)  
Homeless Coalition of Northeast Alabama (HCNEA)  
Housing First, Inc of Mobile and Baldwin Counties  
Metropolitan Birmingham Services for the Homeless (MBSH)  
Mid-Alabama Coalition for the Homeless (MACH)  
North Alabama Coalition for the Homeless (NACH)