North Alabama Coalition for the Homeless
Agency HMIS Privacy and Confidentiality Policy Guidelines

REASONS FOR POLICY:

1. To protect the privacy of agency clients
2. To comply with applicable laws and regulations
3. To insure 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 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) North Alabama Coalition for the Homeless HMIS Privacy Policy
   e) Agency Partnership Agreement(s).

NOTE: HIPAA statutes are more restrictive than the HMIS FR 4848-N-02 standards and in cases where both apply, HIPAA overrides the HMIS FR 4848-N-02 standards. In cases where an agency already has a confidentiality policy designed around the HIPAA standards, that policy can be (1) modified to include the HMIS data collection or (2) amended to create two sets of standards – one for clients covered under HIPAA and a second for those covered only under HMIS FR 4848-N-02.. Each Agency should indicate in its Privacy Notice which standards apply to its situation.

2) Use of Information PPI (protected personal 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, oversight and management functions;
   d) For creating de-personalized client identification to be used in 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 or the public;
   g) To report abuse, neglect, or domestic violence as required or allowed by law;
   h) Contractual research where privacy conditions are met (including a written agreement);
   i) To report criminal activity on agency premises; and/or

j) For law enforcement purposes in response to a properly authorized request for information from a properly authorized source.

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

NOTE: if a client refuses to release PPI, and such information is needed/required in order to provide services, the client's refusal may necessitate denial of service. An Agency may choose to make provisions for such denial of services In its policy.

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

a) PPI will be collected only for the purposes listed above.
b) Clients will be made aware that personal information is being collected and recorded.
c) A written sign will be posted in locations where PPI is collected. This written notice will read:

> "We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We collect only 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.

NOTE: Under HMIS FR 4848-N-02, agencies are permitted to require a client to express consent to collect PPI verbally or in writing; however, this is optional and not a requirement of the statute.

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

a) All PPI collected will be relevant to the purposes for which it is to be used.
b) 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.
c) Data will be entered in a consistent manner by authorized users.
d) Data will be entered in as close to real-time data entry as possible.
e) Measures will be developed to monitor data for accuracy and completeness and for the correction of errors.
    i) The agency runs reports and queries monthly to help identify incomplete or inaccurate information.
    ii) The agency monitors the correction of incomplete or inaccurate information.
    iii) By the 15th of the following month, all monitoring reports will reflect corrected data.
f) Data quality is subject to routine audit by System Administrators who have administrated responsibilities for the database.

NOTE: Refer to HMIS Data Quality Policy and Procedures for complete and detailed requirements.

5) **Privacy Notice, Purpose Specification and Use Limitations** The purposes for collecting PPI data, as well as it uses and disclosures, will be specified and limited.
   a) The purposes, uses, disclosures, policies, and practices relative to PPI data will be outlined in an agency Privacy Notice (copy attached).
   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 representatives, upon request and explained/interpreted as needed.
   d) Reasonable accommodations will be made with regards to the Privacy Notice for persons with disabilities and non-English speaking clients as required by law.
   e) PPI will be used and disclosed only as specified in the Privacy Notice and only for the purposes specified therein,
   f) Uses and disclosures not specified in the Privacy Notice can be made only with the consent of the client.
   g) The Privacy Notice will be posted on the agency web site where applicable.
   h) The Privacy Notice will reviewed and amended as needed.
   i) Amendments to or revisions of the Privacy Notice will address the retroactivity of any changes.
   j) Permanent documentation will be maintained of all Privacy Notice amendments/revisions.
   k) All access to and editing of PPI data will be tracked by an automated audit trail and will be monitored for violations use/disclosure limitations.

NOTE: Items above are required by HMIS FR 4848-N-02, and/or HMIS policy, but agencies can restrict and limit the use of PPI data further by requiring express client consent for various types of uses/disclosures and/or by putting restrictions or limits on various kinds of uses/disclosures.

6) **Record Access and Correction** Provisions will be maintained for the access to and corrections of PPI records.
   a) Clients will be allowed to review their HMIS records within 5 working days of making a request to do so.
   b) During a client's review of his/her records, an agency staff person must be available to explain any entries the client does not understand.
   c) The client may request to have his/her record corrected so that the information is up-to-date and accurate to ensure fairness in its use.
   d) When a correction is requested by a client, the request will be documented and the staff will make a corrective entry if the request is valid.
   e) A client may be denied access to his/her personal information for the following reasons:
      i) Information is compiled in reasonable anticipation of litigation or comparable proceedings;
      ii) Information about an individual other than the agency staff would be disclosed;
      iii) Information was obtained under a promise of confidentiality from a source other than this provider and disclosure would reveal the source of the information;
      iv) Disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.
   f) A client may be denied access to his/her personal information in cases 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 will be made a part of the client's record.

g) A grievance process may be initiated if a client feels that his/her confidentiality rights have been violated, if access has been denied to his/her personal records, or if the client has been harmed or put at personal risk.

7) **Accountability** Processes will be maintained to insure that the privacy and confidentiality of client information is protected and that staff is properly prepared and accountable to carry out agency policies and procedures that govern the use of PPI data.
   a) Grievances may be initiated through the agency grievance process for considering questions or complaints regarding privacy and security policies and practices. Each HMIS user must sign a Users Agreement that specifies staff's obligations with regard to protecting the privacy of PPI and indicates that he or she has received a copy of the agency's Privacy Notice and will comply with its guidelines.
   b) All HMIS users must sign a Users Agreement that specifies each staff person's obligations with regard to protecting the privacy of PPI and indicates that each one has received a copy of the agency's Privacy Notice and will comply with its guidelines.
   c) All users of the HMIS must complete formal privacy training.
   d) A process will be maintained to document and verify completion of training requirements.
   e) A process will be maintained to monitor and audit compliance with basic privacy requirements including, but not limited to, auditing clients entered against signed HMIS Releases.
   f) Regular user meetings will be held and issues concerning data security, client confidentiality, and information privacy will be discussed and solutions developed.

8) **Sharing of Information** Client data may be shared with partnering agencies only with client approval.
   a) All routine data sharing practices with partnering agencies will be documented and governed by an Agency Partnership Agreement.
   b) Agency defaults within the HMIS system will be set to "open" except for agencies serving high risk clients.
   c) A completed HMIS Client Release of Information (ROI) Form is required prior to any electronic information sharing.
      i) The HMIS release lists all HMIS partnering agencies to inform the client what information is to be shared and with whom it is to be shared.
      ii) The client accepts or rejects the sharing plan.
      iii) If the client rejects the sharing plan, staff will close the record and inform the System Administrator for client record duplication monitoring.
   d) Clients will be informed about and understand the benefits, risks, and available alternatives to sharing their information prior to signing an ROI, and their decision to sign or not sign shall be voluntary.
   e) Clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.
   f) All Client Authorization for ROI forms related to the HMIS will be placed in a file to be located on premises.
   g) HMIS-related Authorization for ROI forms will be retained for a period of 7 years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
   h) 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.

i) Restricted information, including progress notes and psychotherapy notes, about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence concerns shall not be shared with other participating Agencies without the client's written, informed consent as documented on the Agency-modified Authorization for Release of Confidential Form.
   i) Sharing of restricted information is not covered under the general HMIS Client ROI.
   ii) If a field that normally contains non-confidential information discloses confidential information, the following steps shall be taken.
      (1) The staff will complete an Authorization to release Confidential Information.
      (2) If the client refuses to authorize the release, the staff will close the Assessment/Screen by clicking the lock on the screen and removing any exceptions.

j) If a client has previously given permission to share information with multiple agencies beyond basic identifying information and non-restricted service transactions, and then chooses to revoke that permission with regard to one or more of these agencies, the affected agency/agencies will be contacted accordingly, and those portions of the record which are impacted by the revocation will be locked from further sharing.

k) All client ROI forms will include an expiration date, at which time a new ROI must be signed by the client.

9) System Security System security provisions will apply to all systems where PPI is stored, i.e., agency's networks, desktops, laptops, mini-computers, mainframes and servers.

a) Password Access**:**
   i) Only individuals who have completed Privacy and System Training may be given access to the HMIS through User IDs and Passwords.
   ii) Temporary/default passwords will be changed on first use.
   iii) Access to PPI requires a user name and password at least 8 characters long and using at least two numbers and two letters.
   iv) User Name and Password may not be stored or displayed in any publicly accessible location.
   v) Passwords must be changed routinely.
   vi) Users must not be able to log onto more than one workstation or location concurrently.
   vii) Individuals with User IDs and Passwords will not give nor share assigned User IDs and Passwords to access the HMIS with any other organization, governmental entity, business, or individual.

b) Virus Protection and Firewalls:
   i) Commercial virus protection software will be maintained by the agency to protect HMIS system from virus attack.
   ii) Virus protection will include automated scanning of files as they are accessed by users.
   iii) Virus Definitions will be updated regularly.
   iv) Each workstation will be protected by a firewall, either through a workstation firewall or a server firewall.

c) Physical Access to Systems Where HMIS Data is Stored
   i) Computers stationed in public places must be secured when workstations are not in use and when staff are not present.
   ii) After a brief period of system non-use, a password-protected screen saver will be activated.
   iii) During extended absences, staff must log off the computer

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 PPI 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) System Monitoring
   i) User access to the HMIS Live Web Site will be monitored using the Audit User Report feature of the HMIS software.

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

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

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 HMIS 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 or 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 Agency Participation Agreement and the User Agreement may be attachments to your Policy. In addition to customizing the sample policy provided above, the agency should describe:*
   a. *A plan for remote access if staff will be using the HMIS System outside of the office such as doing entry from home. Concerns addressed in this plan should include the privacy surrounding the off site entry*
   b. *Who will have what Access Levels on HMIS ServicePoint.*
   c. *How access to the room(s) where the System is being used will be controlled.*
   d. *Procedures for acquiring client consent.*
      i. *The Agency's Privacy Notice should be posted.*
      ii. *How the Privacy Notice will be explained (include the basic script – models provided by NACH for different levels of intervention).*
      iii. *How and when the HMIS Release will be introduced to clients.*
      iv. *A copy of the second Release required to share restricted information.*