****

**HOMELESS MANAGEMENT INFORMATION SYSTEM**

**PRIVACY PLAN**

**Introduction**

U.S. Department of Housing and Urban Development (HUD) set forth HMIS privacy standards in the Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice (Federal Register / Vol. 69, No. 146 on Friday, July 30, 2004). This Privacy Plan is intended to be consistent with these HUD standards.

All users, agencies and system administrators participating in HMIS must adhere to this Privacy Plan. In addition, this Privacy Plan is intended to support our mission to providing an effective and usable HMIS for client service and program use, reporting, and analysis.

The Memorandum of Agreement signed between the HMIS lead agency and each HMIS participating agency requires each HMIS participating agency to:

* Comply with all federal and state laws, rules and regulations that may apply to the use of ShareLink and the collection, use and disclosure of client information. NOTE: A CHO that is also a Covered Entity under HIPAA is not required to comply with the privacy or security standards in the Federal Register HMIS Data and Technical Standards Final Notice, dated July 20, 2004 if the CHO determines that a substantial portion of its homeless client data is protected health information as defined in the HIPAA rules;
* Comply with the operational policies and procedures contained in the ShareLink Homeless Management Information System Standard Operating Policies and Procedures guide;
* Adopt and implement a Privacy Policy that is in compliance with either the Federal Register HMIS privacy and security standards or the HIPAA rules as is applicable to AGENCY’s status and post this policy where HMIS is in use;
* Require all AGENCY ShareLink users to complete the Client Authorization Management training prior to being issued a ServicePoint User ID.
* Require all AGENCY ShareLink users to sign the ShareLink User Policy Responsibility Statement;
* Require AGENCY ShareLink Administrator to take action necessary to ensure that ShareLink User access is discontinued immediately upon the effective date that an AGENCY ShareLink user is no longer employed by the AGENCY or otherwise no longer authorized to be ShareLink user. Action will include at a minimum notifying the HMIS lead agency Administrator in writing of user right termination at least five business prior days to effective date or immediately upon termination of rights if prior notice is not available;
* Verify the accuracy and completeness of AGENCY resource information in ShareLink on at least an annual basis, and update as needed utilizing the AIRS Taxonomy codes;
* Cooperate with other agencies utilizing ShareLink in the coordination of care and case management for clients accessing services from multiple agencies for the mutual benefit of the client, the agencies, and the community;
* Obtain written authorization from the client using a client authorization for release of protected information form approved by ShareLink HMIS Policy Group before client information is used or disclosed for any purpose not allowed by the HIPAA rules, Federal Register HMIS privacy and security standards or other applicable laws;
* Retain original signed *ShareLink HMIS Client Authorization for Release of Protected Information* documentation at least six years from the date they cease to be in effect (from expiration or revocation).
* Safeguard information collected from clients or shared by other organizations as US Housing and Urban Development in Federal Register HMIS Data and Technical Standards Final Notice, dated July 20, 2004 or HIPAA Privacy rules as applicable.
* Authorize HMIS lead agency to create and share de-identified files and reports by using the methods defined in the HIPAA law, for itself and other methods as appropriate and as permitted by the HIPAA Privacy Rule;
* Authorize HMIS lead agency to create and share limited data sets as defined and limited by the HIPAA Privacy Rule.

The Memorandum of Agreement signed between the ShareLink HMIS Lead agency and each HMIS participating agency requires the ShareLink HMIS lead agency to:

* HMIS lead agency will adhere to the baseline security standards and requirements for system application and hardcopy security as outlined in the Federal Register/vol 69. No. 146/Friday July 30, 2004. (4.3.1.to 5.2.1) as amended in the March 2010 Data Standards.
* AGENCY retains ownership of the data that it enters into ShareLink. AGENCY may access this data online via ShareLink, or can obtain copies of data as extracted files by request from ShareLink HMIS Lead agency;
* AGENCY retains decision-making authority on items related to AGENCY operations and service delivery, including eligibility criteria for services and the means and mechanisms for providing services;
* Adopt and implement a Privacy Policy that is in compliance with either the Federal Register HMIS privacy and security standards or the HIPAA rules as is applicable to HMIS lead agency status;
* Provide ShareLink HMIS ServicePoint administration and user access ServicePoint software application.
* Provide initial training, on-going training and technical support to maintain the ShareLink HMIS system;
* Update the ShareLink Homeless Management Information Standard Operating Policies and Procedures guide as needed to meet current HMIS system requirements and maintain compliance with all federal and state laws, rules and regulations that may apply to the use of the ShareLink HMIS;
* Notify AGENCY in writing at least five business days prior to the effective date of changes to the ShareLink Homeless Management Information Standard Operating Policies and Procedures guide;
* Execute a ShareLink HMIS Memorandum of Agreement with all organizations using the ShareLink HMIS to prohibit the re-disclosure of individually identifiable information;
* Act as liaison between AGENCY and Bowman Systems;

HMIS users will receive training in Privacy Policies and acknowledge their responsibilities by signing the ShareLink HMIS User Policy and Responsibility Statement prior to being granted HMIS access. Each user will renew their Policy and Responsibility Statement yearly in order to maintain HMIS access.

The CoC, HMIS Committee, Agencies, and HMIS lead will share the responsibility of reviewing compliance with these standards at least annually. Any privacy policy compliance issue arising from review or from incident will be promptly addressed by the HMIS, Agency and HMIS Committee with CoC oversight.

Failure to comply with security policies can result in a user’s or agency’s access to HMIS being discontinued in accordance with HMIS Standard Operating Policies and Procedures.