H.M.I.S. Privacy Notice

This Notice applies to all SLO County HMIS-Participating Providers and addresses how information about clients may be used and disclosed at Providers as well as client rights over their information. This Notice may be amended at any time, and amendments may affect information obtained before the date of the amendment.

A. HMIS DATA COLLECTION & PURPOSE

A Homeless Management Information System (HMIS) is a local information technology system used to collect data on the housing and services provided to homeless individuals and families and persons at risk of homelessness. Providers participating in an HMIS are required to collect universal data elements from all clients, including Personally Identifying Information, demographic characteristics, and residential history. This information is critical for providers and communities to better understand the extent and nature of homelessness at a local level, evaluate program effectiveness, and improve future housing and service provision. Some providers are also required by their funders to obtain certain additional information to assess services, to determine eligibility, and to monitor outcomes. Most federally-funded homeless service providers are required to participate and record the clients they serve in an HMIS.

This agency is an HMIS-participating homeless service provider ("HMIS Provider"), meaning we collect and enter information about the persons we serve in the private and secure the CountyHMIS (HMIS) database, the local HMIS for this community. There are firm policies and procedures in place to protect against unauthorized disclosure of any personal information collected, and this information is critical to obtain an accurate picture of the homeless population we serve and for this agency to continue to offer you the service(s) you are accessing today. We only collect information deemed appropriate and necessary for program operation or information that is required by law or by the organizations that fund this program. We do not need your consent to enter a record of your visit into the HMIS, but you may refuse to have your personal identifying information within this record and still be eligible to receive services.

If you have any concerns or questions about the information provided above, please speak to an intake worker.

B. PERMITTED DATA USES AND DISCLOSURES

HMIS is designed to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data, including Personally Identifying Information (PII is any information that can be used to identify a particular individual, including a client's name, Social Security Number, and Date of Birth). Once collected, we (as an HMIS Provider) have obligations about how these data may be used and disclosed (usesare internal activities for which providers interact with client PII; disclosures occur when providers share PII with an external entity). HMIS Providers are limited to the following circumstances for the use and disclosure of HMIS PII:

HUD required:
(1) Client access to their information; and
(2) Disclosures for oversight of compliance with HMIS privacy and security standards.
HUD permitted:
(3) To provide or coordinate services to an individual;
(4) For functions related to payment or reimbursement for services;
(5) To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions;
(6) For creating de-identified reporting from PII;
(7) Uses and disclosures required by law;
(8) Uses and disclosures to avert a serious threat to health or safety;
(9) Uses and disclosures about victims of abuse, neglect or domestic violence;
(10) Uses and disclosures for research purposes; and
(11) Uses and disclosures for law enforcement purposes.
A client must provide prior written consent for any other use or disclosure of HMIS PII.
HMIS Providers must also ensure that any use or disclosure does not violate other applicable local, state, or federal laws. Therefore, some HMIS Providers may have more restrictive privacy policies, often dependent upon funding source or the nature of projects. Specific, per-project information regarding data use and disclosure can be obtained upon request.

C. CLIENT CONTROL OVER DATA
HMIS recognizes every independent legal adult (person over 17 years of age) as the owner of all information about themselves, and any parent, legal guardian, or legal power of attorney as the designated owner of all information about any household members under their guardianship (all minors and any incapacitated/disabled adults). By seeking assistance from this HMIS Provider and consenting to your personal information being entered into a record within the HMIS, you transfer governance responsibility over your HMIS record to us, and we are responsible for handling your record in accordance with HMIS privacy policies and any applicable federal, state, or local requirements.

You retain ownership of your information within your HMIS record, and as owner you have the following rights, in general:
» Refusal: to refuse to answer a question you do not feel comfortable with and not have it recorded within HMIS;
» Access/Correction: to request and view a copy of your project information record within HMIS from your provider, including those who have accessed and/or edited your record, and to request corrections to that record;
» Grievance: to ask questions of or submit grievances to your provider regarding privacy and security policies and practices;

» Anonymized Record: to request that your provider anonymize your personal data record within HMIS; and
» Optional Data Sharing: to choose if your information is shared outside of HMIS with researchers and other providers, and to make this decision at each project you receive services from. (Please note that if you decide NOT to data share, it does not prohibit the project from entering your data into HMIS – it prohibits the sharing of your data as outlined on the consent form).

HMIS Providers reserve the following exceptions to the above: (1) Provider Right to Deny Review: if information is compiled in reasonable anticipation of litigation or comparable proceedings; if information about another individual other than the participating provider staff would be disclosed; if information was obtained under a promise of confidentiality other than a promise from this provider and disclosure would reveal the sources of the information; or if the disclosure of information would be reasonably likely to endanger the physical safety of any individual; and (2) Provider Right to Deny Access/Correction: in response to repeated or harassing requests.

D. RESPONSIBILITY TO PROTECT DATA

The County of San Luis Obispo Department of Social Services is the System Administrator of HMIS. HMIS uses Bell Data Technology's software application and database, which is maintained in compliance with all federal standards set forth in the Health Insurance Portability and Accountability Act (HIPAA) and its subsequent legislation – the standards required to protect medical records –as well as U.S. Department of Housing and Urban Development HMIS standards.

The County HMIS staff take the protection of client confidentiality and privacy seriously. The following security measures, among others, are in place to ensure that your information is protected:
» System Security: HMIS data is encrypted and securely transmitted from Providers to the HMIS database, extensive procedures are in place to prevent unauthorized access, and the entire HMIS system and database is protected at the highest level of security for health data;
» Access: Only CountyHMIS staff and staff at providers may receive authorization to access HMIS, and authorization requires comprehensive initial training and annual privacy and security training thereafter;
» Confidentiality Agreements: Every HMIS Provider and every person authorized to read or enter information into HMIS signs an agreement every year that includes: (1) commitments to maintain the confidentiality of all HMIS information; (2) commitments to comply with all security measures in compliance with federal HMIS requirements and any applicable federal, state, or local laws; and (3) penalties for violation of the agreement;

» Monitoring: Annual monitoring is conducted for HMIS providers to ensure compliance with privacy and security policies; and
» Reporting: Published HMIS reports are comprised of aggregate data only, and never contain any client-level or identifying (PII) data.

IMPORTANT INFORMATION FOR ALL CLIENTS – PLEASE READ

If you do not understand any of the information within this form, you may ask your intake worker for further explanation or an alternate Format. You may keep the first 2 pages of this form (containing the HMIS Privacy Notice) for your records. You may request a copy of any participating provider or HMIS policies from your intake worker.