# Santa Barbara County HMIS Data Privacy Plan

### Continuum of Care:

CA-603 Santa Maria/Santa Barbara County

### HMIS Lead Agency:

County of Santa Barbara
Community Services Department
Housing and Community Development Division
105 E. Anapamu St., Room 105
Santa Barbara, CA 93101
Telephone: (805) 568-3520
Fax: (805) 560-1091

## Contents

## 1. Introduction

This document indicates the techniques and procedures that will be used to protect the privacy of clients and other people who contribute information to the Homeless Management Information System (HMIS) for the Santa Maria/Santa Barbara County Continuum of Care.

As described in the March 2010 HMIS Data Standards Revised Notice, an HMIS is an electronic data collection system that stores historical, person-level information about persons who access the homeless services system in a Continuum of Care. HMIS is a valuable resource because of its capacity to integrate and unduplicate data from all homeless assistance and homeless prevention programs in a Continuum of Care. Aggregate HMIS data can be used to understand the size, characteristics and needs of the homeless population at the local, state and national levels. The HMIS Data and Technical Standards are issued by the U.S. Department of Housing and Urban Development (HUD).

The following HUD HMIS Standards were referenced in the creation of this document:

- 2004 HMIS Data and Technical Standards Final Notice
- Guidance on HPRP Subgrantee Data Collection and Reporting for Victim Service Providers
- 2011 HMIS Requirements Proposed Rule
- 2017 HMIS Data Standards Revised Notice

The roles and responsibilities described in this document will primarily be fulfilled by the Continuum of Care, the HMIS Lead Agency, and HMIS Partner Agencies (referred to by HUD as Contributing Homeless Organizations or CHOs).

A Continuum of Care is a group composed of representatives of organizations, including nonprofit providers of homeless services, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, veterans service providers, mental health agencies, hospitals, universities, affordable housing developers and law enforcement, that serve homeless and formerly homeless persons and that carry out the responsibilities delegated to a Continuum of Care under HUD's regulations for a particular community. A Continuum of Care is ultimately responsible for oversight and guidance of HMIS. A Continuum of Care is also responsible for oversight of the security of the data and any public use of the data.

The Director of the Community Services Department, or his/her designee, is the authorizing agent for all agreements made between HMIS Partner Agencies and the HMIS Lead Agency. In all HMIS governance decisions, the Continuum of Care will balance the interests and needs of all HMIS stakeholders, including homeless men, women and children, service providers, and policy makers.

The HMIS Lead Agency provides day-to-day management of system participation, operations and security. In Santa Barbara County, the role of HMIS Lead Agency is currently filled by the Housing and Community Development Division of the Community Services Department of the County of Santa Barbara.

An HMIS Partner Agency is an entity that has agreed to uphold these Policies and Procedures by executing a Memorandum of Understanding with the County of Santa Barbara. Some HMIS Partner Agencies may be obligated to comply with the Health Insurance Portability and Accountability Act ("HIPPA"), and/or with 42 CFR Part 2, regarding the confidentiality of substance use disorder patient records. Where possible, these agencies should comply with HIPAA, with 42 CFR Part 2, and with this Privacy Plan. If it is not possible to reconcile all of the applicable rules, then agencies should comply with the more stringent regulations. Agencies and programs are responsible for ensuring HIPAA and 42 CFR Part 2 compliance.

## 2. Revision History

This Privacy Plan shall be reviewed and, if necessary, revised at least annually by the Continuum of Care. See Section 6.6 of the Administrative Policies and Procedures for more detail on changes of this and other documents.

| Date | Author | Description |
|---|---|---|
| 11/30/2013 | Community Technology Alliance (www.CTAgroup.org) | Full revision referencing all HUD standards and 2011 HEARTH HMIS Proposed Rule |
| 4/14/2014 | County of Santa Barbara Community Services Department | Revisions referencing designations |
| 10/20/2017 | HomeBase | Technical revisions based on best practices in other communities. Privacy Plan split off from general Policies and Procedures, and established as stand-alone document. |

# 3. Privacy Policies

## 3.1 Obtaining Informed Consent

- Client data may only be entered or imported into HMIS if the client has provided informed consent, as demonstrated by a signed HMIS Client Informed Consent and Release of Information Authorization form.
- Each Partner Agency must attempt to reach each client at least once per year in order to have the client re-sign a new copy of the HMIS Release of Information form. If the client does not sign the form for three consecutive years, then the client must be assumed to have withdrawn consent to share the client's sensitive personal information. All information about that client (except for basic identifying information such as name, appearance, date of birth, contact information, and last known locations) must then be removed from HMIS and/or anonymized so that it can no longer be connected with the client.
- A client shall have the right to receive a copy of all HMIS data relating to him/her upon written request.
- The burden rests with the Partner Agency End User or intake counselor to inform the client about the purpose and function of HMIS data before asking for consent. As part of informed consent, a privacy notice must be posted in the intake area explaining the reasons for collecting the data, the client's rights with regard to data collection, and any potential future uses of the data. An example of such a sign may be found in the HMIS web portal resource library.
- Partner Agency End Users must obtain a new signed ROI and enter it into HMIS if the client's original release has expired.
- Upon written request to the HMIS Lead Agency, a client shall be given a print-out of all data relating to him/her within 10 working days.
- Consent for the sharing of all information except for name, date of birth, contact information, and last known location will expire three years after a client gives informed consent. Case workers will attempt to renew the client's informed consent once per year.

## 3.2 Limited Collection of Client Data

- Client data can be collected for HMIS only when it complies with **both** all CoC-wide privacy policies **and** with the policies, procedures and confidentiality rules of the program that is collecting the data.
- Victim service providers may **not** directly enter or provide client-level data to HMIS. Instead, a victim service provider, which is defined as a private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault or stalking, must use a comparable database that collects client-level data over time and generates unduplicated aggregate reports based on the data. Legal service providers may also elect to use a comparable database if it is necessary to protect attorney-client privileges.
- If a Partner Agency wishes to import data into HMIS that is not collected directly from a client or provider (e.g., an import of older data or data from other systems), the Partner Agency must first obtain express permission from the HMIS Lead. Even after permission is received, it is the responsibility of the Partner Agency to protect the privacy of any persons described by any imported data.
- Data may be collected and entered into HMIS only when that data is expected to be useful for organizing, providing, or evaluating the delivery of housing or housing-related services. Partner Agencies may not use the HMIS Client Consent Form to cover the collection of data that is irrelevant to homelessness. Partner Agencies may not use HMIS to store data that is irrelevant to homelessness.

## 3.3 Limited Access to Client Data

- Except as ordered by a Court or as needed to respond to a specific medical emergency, personally identifiable data from HMIS may only be shared when **all** of the following conditions are met:
    - the recipient of the data is either a regular staff member working for the HMIS Lead, or an authorized Technical Administrator and/or End User at an HMIS Partner Agency, and
    - the sharing agency has secured informed consent authorizing such sharing, as demonstrated by a signed HMIS Client Informed Consent and Release of Information Authorization form, and
    - The Client Informed Consent and Release of Information Authorization is still valid (i.e., it has not yet expired, nor has it been revoked).
- Other non-HMIS inter-agency agreements do not cover the sharing of HMIS data. Sharing of client data may be limited by program specific confidentiality rules.
- Data used for research or policy evaluation will be shared only after the data has been thoroughly de-identified. This includes both removing names and contact info, and removing descriptions or combinations of characteristics that could be used to identify a person.

### *Physical Safeguards*

In order to protect client privacy, it is important that the following physical safeguards be put in place by each agency's Technical Administrator. For the purpose of this section, authorized persons will be considered only those individuals who have completed Privacy and Security training within the past 12 months.

1. Computer Location – Computer must be in a secure location where only authorized persons have access. Computer must not be accessible to clients, the public, or casual volunteers.
2. Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.
3. PC Access (visual) — Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or other unauthorized Partner Agency staff members or volunteers and utilize visibility filters to protect client privacy.
4. Unique Passwords -- User IDs are individual and passwords are confidential. No individual should ever use or allow use of a User ID that is not assigned to that individual, and user-specified passwords should never be shared or communicated in any format.

## 3.4 Resistance to Outside Disclosures

- If an outside entity, such as a Court or law enforcement authority, attempts to access client-specific data, the outside entity will be politely but firmly instructed that the data is confidential and cannot be released without (i) a valid warrant, or (ii) the client's express consent. The client and/or the client's social worker will then be informed of the attempted access so that the client can take any appropriate steps to resist any further attempts by outside parties to access the client's private information.
- No client-specific data will be released or shared outside of the Partner Agencies unless the client gives specific written permission or unless withholding that information would be illegal. Note that services may NOT be denied if client refuses to sign Client Informed Consent and Release of Information Authorization or declines to state any information.
- Aggregate data that does not contain any client-specific identifying data may be shared with internal and external agents without specific permission. This policy should be made clear to clients as part of the Informed Consent procedure.
- A log of all external releases or disclosures of PPI, including dates, agencies, persons, and other details, must be maintained by the HMIS Lead Agency for 7 years and made available to the client upon written request to the HMIS Lead Agency and within 10 working days.

- If a client signs an ROI, but chooses not to share information with other Partner Agencies, End Users' data collection and data entry practices should follow the workflow and specific data entry guidelines established in the HMIS End User Manual to prevent sharing of client assessment information.

### 3.5 Long-Term Data Storage and Disposal

1. The Continuum of Care will adopt a plan to dispose of (or remove identifiers from) client data 7 years after it was created or last changed. Once adopted, that plan will be incorporated into these Policies and Procedures.

## 4. Forms Control

All forms required by these Policies and Procedures are available in on the HMIS web portal. Completed forms must be filed as described in the chart below and maintained for 7 years.

#### Filing of Completed Forms

| Form ID # | Form title | Responsibility for maintaining file of signed forms |
|---|---|---|
| 1MOU-20171020 | Memorandum of Understanding | HMIS Lead Agency |
| 1CC-20171020 | Compliance Certification Checklist | HMIS Lead Agency |
| 1EU-20171020 | HMIS End User Agreement | Partner Agency Technical Administrator |
| 1PN-20171020 | Privacy Notice | N/A |
| 1ROI-20171020 | Client Informed Consent and Release of Information Authorization | Partner Agency End User |
| 1SI-20171020 | Standardized Intake | N/A |

Form ID Syntax: Version Number + Form Code – YYYYMMDD of last revision