Oakland, Berkeley/Alameda County Continuum of Care

CA-502

Homeless Management Information System

Privacy Policy

Contents

Alameda County
Homeless Management Information System (HMIS)
Privacy Policy

STATEMENT OF PURPOSE:

To protect the privacy of agency clients

1. To comply with applicable laws and regulations

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:

Privacy Practices

1. Alameda County Housing & Community Development privacy practices will comply with all applicable laws governing Homeless Management Information System (HMIS) client privacy/confidentiality. Applicable standards include, but are not limited to the following:
   a. Federal Register Vol. 69. No. 146 (I IMIS FR 4848-N-02) - Federal statute governing HMIS information – Friday, July 30, 2004
   b. HIPAA - the Health Insurance Portability Act
   c. 42 CFR Part 2. - Federal statute governing drug and alcohol treatment
   d. Alameda County-wide Continuum of Care HMIS Policy and Procedures manual
   e. Alameda County-wide Continuum of Care HMIS partner agency sharing agreement(s)
   f. Violence Against Women Act

g. Family Violence Prevention and Services Act
h. Victims of Crime Act

Personally Identifiable Information

2. Use of Personally Identifiable Information (PII, personal 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 for 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
   j. For law enforcement purposes in response to a properly authorized request for information from a properly authorized source.

Data Sharing Practices

3. All routine data sharing practices with partnering agencies will be documented and governed by the CoC MOU Agreement.

Collection of Information

4. Information will be collected only by fair and lawful means with the knowledge or consent of the client.
   a. Client consent is assumed when all of the following take place:
      - Agencies post the Privacy Notice (see #6, below) at each intake desk (or comparable location) that explains the reasons for collecting HMIS information, and the uses and disclosures that are allowable
      - Agency staff discuss the contents of the notice with a client
      - The client agrees to provide personal information

- Agency staff complete a Staff Attestation form confirming they completed these steps and ensure that the form is retained in their organization's records.

b. Agencies may follow this Assumed Consent procedure if:
   - The data use or disclosure is listed in #2, above
   - The use or disclosure is listed in their CHO's privacy notice
   - Their organization instructs them to do so.

c. If the use or disclosure does not meet the requirements for the Assumed Consent procedure, or an organization wants staff to collect written consent, they should follow the Explicit Consent procedure:
   - Staff ask the client to sign the Release of Information (ROI) form indicating their consent to release their private information.
   - Staff then ensure that the completed form is uploaded into the agency's internal system.

d. Clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.

e. If a client chooses not to consent, staff will note "decline" in the HMIS and follow the agency's blind process (e.g., procedures that allow client data to be entered in the HMIS without a name and/or social security number).

f. Clients have the right to update or rescind their consent and levels of data sharing at any time. If a client requests to update their consent, staff informs the client that any changes will take effect as of the date the form is signed, and that any data or information shared before that time cannot be recalled.

g. Clients may request updates or revisions to their ROI during standard business hours.

Entering Non-Identifying Information

5. All people actively fleeing domestic violence will be entered into Clarity HMIS without the use of personally-identifying information (PII). For households in which the head of household is fleeing domestic violence, the profiles for other household members must also be de-identified.

   Please note domestic violence survivors may authorize their PII be recorded normally in HMIS after consenting to a Release of Information. However, an agency's primary concern must be the client's safety; profiles may remain de-

identified whenever necessary by following the HMIS De-identify Data Entry Guide. (See Appendix A)

Data Quality

6. Data Quality: PII data will be accurate, complete, timely, and relevant.
   a. All PII 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 seven 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.
      - Participating agencies will run reports and queries monthly to help identify incomplete or inaccurate information.
      - Agencies will monitor the correction of incomplete or inaccurate information.
   f. Data quality is subject to routine audit by the HMIS staff who have administrative responsibilities for the database.

Agency Standards

7. Each agency participating in the Alameda County CoC must decide whether to adopt the HMIS's standard Security Policy, Privacy Policy, Privacy Notice, and Procedure Manual. Alternatively, agencies may adapt them to include stricter protections, as necessary. HIPAA-covered entities will use HIPAA-oriented versions of these documents.

Privacy Notice

8. The Privacy Notice (See Appendix A) is a consumer-friendly summary of the Privacy Policy that is meant to be easy for clients to understand and act upon. It outlines the purposes, uses, disclosures, policies, and practices relative to PII data.
   a. The agency Privacy Notice will comply with all applicable regulatory and contractual limitations.
   b. The agency Privacy Notice will be made available to agency clients, or their representative, upon request and explained/interpreted as needed.

c. Reasonable accommodations will be made with regards to the Privacy Notice for persons with disabilities and non-English speaking clients as required by law.
d. PII will be used and disclosed only as specified in the Privacy Notice, and only for the purposes specified therein.
e. Uses and disclosures not specified in the Privacy Notice can be made only with the consent of the client.
f. Participating agencies will post a written sign summarizing the HMIS and/or agency's privacy policy in all locations where intake occurs, either in offices or in the field. For example, outreach workers can tape the Privacy Notice/ Sign to the back of a clipboard.
    - Agencies that have adapted the CoC's Privacy Notice should post their revised notice.
    - Agencies may also post this language from HUD:

      We collect personal information directly from you for reasons that are discussed in our privacy notice. 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 only collect information that we consider to be appropriate.[1]

g. The Privacy Notice will be posted on the agency web site.
h. The Privacy Notice will be reviewed and amended as needed.
    - Amendments to or revisions of the Privacy Notice will address the retroactivity of any changes.
    - Permanent documentation will be maintained of all Privacy Notice amendments/revisions.

Provisions

9. Provisions will be made for clients to access and offer corrections to their PII records.
    a. Clients will be allowed to review their HMIS record within five business days of a request to do so.

[1] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.1 pg. 45929

b. During a client review of their record, an agency staff person must be available to explain any entries the client does not understand.
c. The client may request to have their record corrected so that information is up-to date and accurate to ensure fairness in its use.
d. When a correction is requested by a client, staff will document the request and the staff will make a corrective entry if the request is valid.
e. A client may be denied access to their personal information for the following reasons:
    - Information is compiled in reasonable anticipation of litigation or comparable proceedings
    - Information about another individual other than the agency staff would be disclosed
    - Information was obtained under a promise of confidentiality other than a promise from this provider and disclosure would reveal the source of the information
    - The disclosure of information which would be reasonably likely to endanger the life or physical safety of any individual.
f. A client may be denied access to their personal information in the case 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 be made a part of the client's record.
g. A grievance process may be initiated if a client feels that their confidentiality rights have been violated, if access has been denied to their personal records, or if they have been put at personal risk, or harmed (see # 10, below)

Accountability processes

10. Accountability processes will be maintained to protect the privacy and confidentiality of client information, and to ensure that agency staff is properly prepared to carry out policies and procedure that govern the use of PII data.
    a. All users of the HMIS system must sign User Agreements that specifies each staff persons' obligations to protect the privacy of PII, indicates that they have received a copy of the agency's Privacy Notice and that they will comply with its guidelines.
    b. All staff, interns, volunteers, or associates collecting PII intended for, or viewing data generated by, the HMIS must successfully complete CoC-sponsored privacy and security certification training.

c. A process will be maintained to document and verify completion of training requirements.
d. Regular user meetings will be held and issues concerning data security, client confidentiality, and information privacy will be discussed and solutions will be developed.

System security provisions

11. System security provisions will apply to all systems where PII is stored: agency networks, desktops, laptops, mini-computers, mainframes and servers. a. Password Access:
    - Only individuals who have completed Privacy and Security Certification and Software Training may be given access to the HMIS system. ○ Temporary default passwords will be changed on first use.
    - Access to PII requires a username and password at least 8 characters long and using at least one number and one letter.
    - Passwords will not use or include the user's name or the vendor name and will not consist entirely of any word found in the common dictionary or any of the above words spelled backwards.
    - Usernames and passwords may not be stored or displayed in any publicly accessible location.
    - Passwords must be changed routinely.
    - Users must not be able to log onto more than one workstation or location at a time.
    - Users will not give or share assigned HMIS usernames and passwords any other person, organization, governmental entity, or business.

    b. Virus Protection and Firewalls:
    - Commercial anti-virus protection software will be maintained to protect all agency network systems and workstations from virus attack.
    - Virus protection will include automated scanning of files as they are accessed by users.
    - Virus definitions will be updated regularly.
    - All workstations 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:
    - Computers stationed in public places must be secured when workstations are not in use and staff is not present.

- After a short period of time, a password protected screen saver will be activated while the computer is temporarily not in use.
- For extended absence from a workstation, staff must log off the computer.

d. Stored Data Security and Disposal:
   - All HMIS data downloaded onto a data storage medium must be maintained and stored in a secure location, not accessible to non-licensed users of the HMIS system.
   - Data containing PII will not be downloaded to any remote access site at any time for any reason, nor transmitted outside the physical agency by any means whatsoever.
   - Data stored on a portable medium will be secured when not in use and will never be taken off site at any time for any reason.
   - Data downloaded for purposes of statistical analysis will exclude PII whenever possible.
   - HMIS data downloaded onto a data storage medium must be disposed of by reformatting twice, as opposed to erasing or deleting. This includes hard drives.

e. System Monitoring: All access to and editing of PII data will be tracked by the HMIS' automated audit trail and will be monitored for violations use/disclosure limitations.

f. Hard Copy Security:
   - Any paper/hard copy reports, data entry forms, or signed consent containing PII that is either generated by or for the HMIS will be secured.
   - At all times in a public area, agency staff will supervise hard copy documents with identifying information generated by or for the HMIS. If the staff leaves the area, the hard copy must be secured in areas not accessible by the public.
   - All written information pertaining usernames and passwords must not be stored or displayed in any publicly accessible location.

g. Access to the HMIS system is allowed only from authorized agency locations.

Grievance Policy

12. The purpose of the Grievance Policy is to allow clients to express concerns and have correction implemented. Clients will contact the participating agency with which they have an HMIS-data-related grievance within seven days of the incident and

submit their complaint in writing. The participating agency shall assist the client in the navigating the grievance procedure.

a. Any client grievances relative to the HMIS system will be processed/resolved according to the provider agency's grievance policy.
b. Participating agencies will report all HMIS-related client grievances to the HMIS Lead Agency Senior Manager (or designee) and CoC staff, along with a description of their response.
c. If clients are unsatisfied with the resolution of their grievance at the agency level, they may request mediation at the CoC level. System, agency, or client level issues may be brought before the CoC Committee for review. The Committee's grievance subcommittee will hear the complaint; their decision is final.
d. All actions and resolutions will be in writing.

APPENDIX A

PRIVACY NOTICE

De-identify Data Entry Guide

CA-502 Oakland, Berkeley/Alameda County CoC

Privacy Notice

For organizations in the Oakland-Berkeley-Alameda County Continuum of Care

When you meet with a member of our organization or get services from us, you consent to allow us to collect, use, and share information about you for certain reasons. We have a responsibility to protect your information and privacy.

This Privacy Notice summarizes our Privacy Policy. The Privacy Notice and Policy can be found online at www.achmis.org or you can ask a staff member for a copy.

What information do we collect?

We collect information that can be used to identify you, such as:

- Your name, address, date of birth.
- Contact information.
- Identification numbers.
- Photos or videos.
- Information about services you received.

Why do we collect and share your information?

We collect, use, or share your information to:

- Provide or coordinate services.
- Collect payments.
- Run the organization.
- Create data that can't identify you.
- Support research.
- Follow local, state, and federal laws.
- Follow court orders, respond to threats, and ensure public safety.

We will ask for your written or verbal consent to use or share your information for any purpose not listed above, or if the law requires it.

What other steps do we take to protect your privacy?

In addition to following local, state, and federal laws, we will:

- Assist you if you need help or translation, as required by law.
- Explain and share this Privacy Notice and the Privacy Policy. This Notice summarizes the Policy.
- Only collect the information we need.
- Have a plan for keeping information in good order and deleting old data.
- Share the least amount of information needed to complete a task.
- Allow you to review and correct your information and explain if your request is denied.
- Have a plan and train staff to handle questions, complaints, or a data breach.

The Privacy Policy can be changed at any time. Changes can apply to information that has already been collected.

For a list of organizations that are part of the Oakland-Berkeley-Alameda County Continuum of Care, please visit www.achmis.org or ask a staff member for a copy.

Updated 9/30/22

Alameda County HMIS:

Consent Refused Data Entry Guide

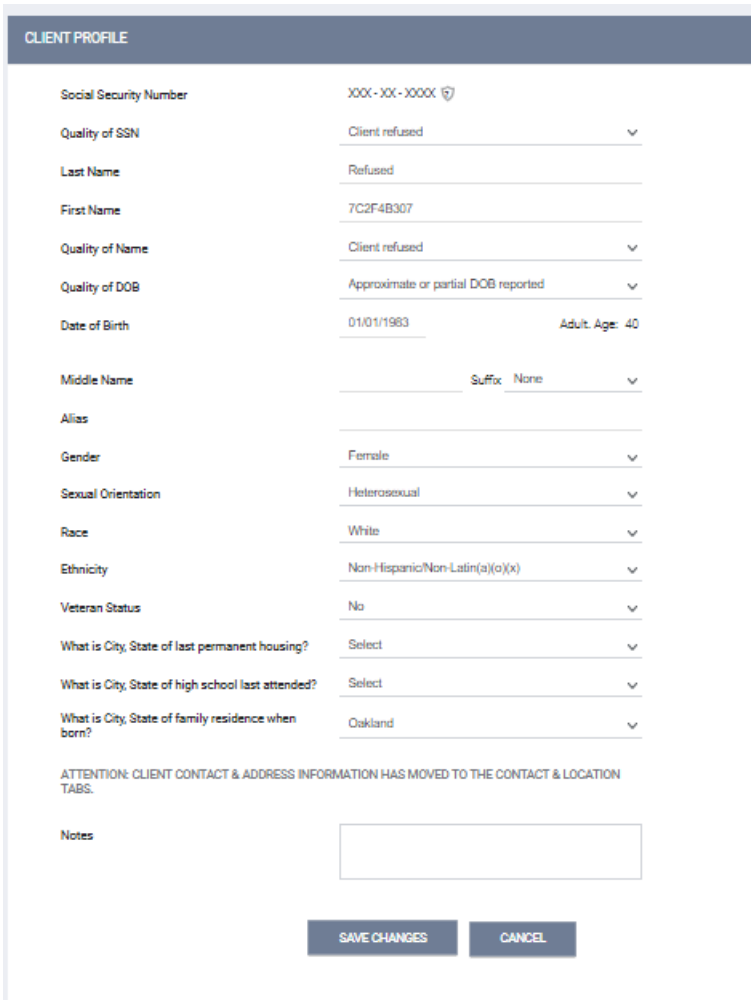
Clients are not required to provide written consent to have any personal information stored in HMIS. Personal information includes not just names, exact dates of birth, and partial or full social security numbers, but also information that may not be identifying in and of itself, but when combined with other non-identifying information, may unintentionally lead to the identification of that person.

The de-identified data entry protocol should be followed as described below. If one member of a household refuses consent, de-identified data entry protocol should be used for all members even if others are willing to consent.

NOTE: Providers should not enter identifying information into HMIS for clients who are: 1)receiving services from domestic violence agencies; 2) currently fleeing or in danger from a domestic violence, dating violence, sexual assault or stalking situation; or 3) under 13 with no parent or guardian available to consent to enter the minor's information in HMIS.

De-identifying a New Data Entry Protocol:

1. From the search screen, click "Add Client"
2. Enter '000-00-0000' for Social Security, select "Client Refused" for Quality of SSN
3. Enter "Refused" for last name
4. Temporarily enter "Refused" for first name, select "Client Refused" for Quality of Name
5. For the Date of Birth, enter 01/01/___ and the year the client was Born, select "Approximate or partial DOB reported" for Quality of DOB
6. Leave Middle Name and Suffix blank
7. Enter Gender, Race, Ethnicity and Veteran status with real data
8. Select Save
9. Edit First Name: copy the UII for First Name.
10. Profile will look like this:



If a client profile exists and it now needs to be de-identified, follow the steps listed above and contact the Help Desk if help is needed to de-identified the record.

As service provider working with a de-identified client record, please: Retain the Clarity unique identifier and any other identifying information (such as name, date of birth, SSN, etc…) you will need in order to identify and update the client's record in Clarity throughout the course of serving them.

Retain this information in a manner that meets agency, HUD, and ACHMIS security requirements.

Updated June 2023