Meeting Link:  https://us02web.zoom.us/j/83147801927
Meeting ID: 831 4780 1927
One tap mobile: +16699006833,,83147801927# US

Meetings are public. Homeless and formerly homeless Alameda County residents are especially encouraged to attend. Public Comment will be taken at the beginning of each meeting and is limited to 2 minutes per person. Click here to learn more about the public participation policy.

1. Welcome (C'Mone Falls, HUD CoC Chair) 2:00-2:10pm
2. HUD CoC Public Comment 2:10-2:20pm
3. Approval of Meeting Minutes, #6- 6.15.21 2:20-2:30pm
   Action Item
4. Homeless System Updates (All) 2:30-2:35pm
   Update
5. 2021 Notice of Funding Opportunity for COC (Chelsea and Homebase consultants) 2:35 – 3:20pm
   Action Items
   a. Overview of 2021 NOFA Application
   b. Strategic Direction
   c. Timeline
   d. 2021 Local Competition Review and Ranking Process
   e. NOFA Committee (approve alternate)
      i. Gloria Wroten currently serves on the System Coordination Committee since 2018.
   f. NOFA Appeal Board
      i. Ray Bonilla (Leadership Board)
      ii. NOFA Committee (Pending)
      iii. HUD CoC Board Member (Solicit volunteer)
6. Youth Action Board (Hannah/ Paul) 3:20- 3:30pm
   Update
   a. Youth Homelessness Demonstration Project Submission
   b. Application Part 2
7. Governance and Staffing Update (Chelsea) 3:30 – 3:40pm
   Update
8. Coordinated Entry Refresh (Colleen Budenholzer)  
   *Update*  
   3:40 - 3:45pm

9. Emergency Housing Vouchers Update  
   3:45 – 3:55

10. Announcements and Next Meeting/Agenda  
    3:55 - 4:00pm
    a. Next meeting, September 21st 2021 at 2:00pm to 4:00pm
HUD CoC Committee Minutes  
Tuesday, June 15, 2021  
2:00 p.m. - 4:30 p.m.

HUD CoC Members: C'Mone Falls (City of Oakland), Josh Jacobs (City of Berkeley), Riley Wilkerson (Alameda County Housing and Community Development), Marnelle Timson (Consumer Member), Tunisia Owens (Family Violence Law Center), Paulette Franklin (Alameda County Behavioral Health), Paul Berry (Youth Action Board), Lara Tannenbaum (City of Oakland), and Wendy Jackson (East Oakland Community Project).

Leadership Board Members: Kerry Abbott (Alameda County Health Care Services Agency, OHCC), Suzanne Warner (Alameda County Health Care Services Agency, OHCC), Andrea Ford (Alameda County Social Services Agency), Claudia Young (City of Livermore), Doug Biggs (Alameda Point Collaborative), Liz Varela (Building Futures with Women and Children), Jacqueline McCormick on behalf of Mayor Jesse Arreguin (City of Berkeley), Michelle Starratt (Alameda County Housing and Community Development Department), Moe Wright (BBI Construction), Peggy McQuaid (City of Albany), Susan Shelton, Suzanne Shenfil (City of Fremont) and Vivian Wan (Abode Services).

EveryOne Home Team: Chelsea Andrews (Executive Director), Katie Martin (Outreach Coordinator), Ja’Nai Aubry (Director of CoC Strategies), Dorcas Chang (Operations Coordinator) and Alexis Lozano (Data Analyst).

Members of The Public: Hannah Moore (All In Alameda County), Nic Ming (Social Impact Wheel), Beth Quirarte (Ruby’s Place), Heather MacDonald-Fine (Alameda County Health Systems), Ellen Morris (Eden Housing), Jared Savas (Supervisor Wilma Chan’s Office), Julie Christiansen (Oakland Housing Authority), and Laurie Flores (City of Fremont).

Absent: None.

1. Welcome (C'Mone Falls, HUD CoC Chair)
   a. HUD CoC Chair C'Mone F. (City of Oakland) welcomed the committee and attendees to the June meeting.

2. HUD CoC Public Comment
   a. Beth Q. (Ruby’s Place) made the announcement that Ruby’s Place is expanding their program to support transition aged youth and young victims of sex trafficking. Beth also spoke in support of having the proposed set-aside of the emergency housing vouchers for survivors of gender-based violence.
   b. There were no written public comments.

3. Approval of Meeting Minutes, #5 - 5.18.21
   a. Paulette F. made a motion to approve the May meeting minutes. Josh J. seconded.
      i. C'Mone=Yes  
      ii. Josh=Yes  
      iii. Riley=Yes  
      iv. Marnelle=Yes  
      v. Tunisia=Abstain  
      vi. Paulette=Yes
   1. Motion passed.

4. Homeless System Updates (All)
a. Lake Merritt Lodge is now open and will operate through September. The hotel is a
similar model to other Project Roomkey/ Safer Ground hotels.

5. **Youth Action Board Update (Hannah/Paul)**
   a. The Youth Action Board is hosting two focus groups for the Youth Homelessness
      Demonstration Project (YHDP) to gather youth wisdom. The first is this Thursday at
      Covenant House from 1:00-2:30pm. The second is next Thursday, June 24th at REACH
      Ashland Youth Center from 3:00-4:30pm. Youth that participate will be compensated with
      a gift card, pizza and water. There are also plans to hold a virtual focus group. And later,
      All In will be hosting a writing workshop to pull together a support letter from young
      people as required in the YHDP application.

6. **Youth Homelessness Demonstration Project (Ja’Nai)**
   a. Staff provided an overview of the YHDP application. The application lead will be the
      Office of Homeless Care and Coordination with support from EveryOne Home, All In
      Alameda County, City of Oakland, the Collaborative Applicant (HCD) and a consultant
      funded by a new grant.

1. **Governance Update (Chelsea)**
   b. Staff requested the committee’s thoughts and suggestions on the size and composition of
      the new CoC Standards, Compliance and Funding Committee. The new committee will
      have many of the current responsibilities of the HUD CoC Committee. The committee
      expressed the desire to:
      i. Ensure the benchmarks for people with lived experience of homelessness are
         met
      ii. Ensure the benchmarks for Black, Indigenous, and People of Color are met
      iii. Have representation from the cities and the Alameda County Housing and
           Community Development Department (HCD)

7. **2021 CoC NOFA** (Note that the Leadership Board is welcome to participate in this discussion
   item)
   a. General Update (Riley W.)
      i. Last year, Alameda County HCD identified Homebase as the consultant for the
         2020 CoC NOFA. They were the only applicant to respond to a Request for
         Proposal. However, HUD allowed for waivers for all CoC-funded projects to allow
         for non-competitive renewal in 2020. As a result, there was not a competitive
         local process to manage in 2020. Therefore, HCD is moving ahead to contract
         with HomeBase for this year.
      ii. Staff anticipates that the NOFA will be released in the next few weeks given that
          the Grant Inventory Worksheet (GIW) was submitted last Friday. HUD uses the
          GIW to determine the projects that are eligible for renewal. They then do an
          assessment nationally to determine the amount of funding available for renewing
          and new projects.
   b. NOFA Committee (Ja’Nai)
      i. Staff provided an overview on the roles and responsibilities of the committee and
         the conflict-of-interest policy. The proposed roster includes people that have
         previously served along with three new members. The new members submitted
         applications in the fall of 2019, and they were screened by the Nominating
         Committee and interviewed by EveryOne Home staff.
      ii. C’Mone F. made a motion to approve the 2021 NOFA Committee roster. Tunisia
          O. seconded.
         1. C’Mone = Yes
         2. Josh = Yes
         3. Riley = Yes
         4. Marnelle = Yes
         5. Paul = Yes
         6. Lara = Yes
         7. Tunisia = Yes
         8. Paulette = Yes
         a. The motion passed.
   c. Strategic Direction (Ja’Nai)
      i. The committee reviewed the strategic direction from 2019. Members discussed:
1. How COVID-19 may have impacted the ability for projects to spend down and therefore the involuntary reallocation policy may not be appropriate. The language can be softened or eliminated in this round since spending was not a priority for projects.

2. Projects should include in their application how they incorporate consumer voices and integrate racial equity. Information can be gathered this round to determine where projects are at, and then it can be scored in the next round.

ii. C'Mone F. made a motion to have the following modifications to the strategic direction: 1) Prioritize projects that show a commitment to racial equity and lift up the voices of people with lived experience (new projects scored/ renewals are not scored this year but will be in the future), 2) Remove the involuntary reallocation policy and instead encourage voluntary reallocation and 3) Discourage the use of bonus points for any component when building the application. Lara T. seconded.

   1. C'Mone=Yes
   2. Josh=Yes
   3. Riley=Yes
   4. Marnelle=Yes
   5. Paul=Yes
   6. Lara=Yes
   7. Tunisia=Yes
   8. Paulette=Yes
   9. Wendy=Yes
   a. The motion passed.

8. Emergency Housing Vouchers (Ja'Nai)
   a. The committee is being asked to determine prioritization and targeting for the emergency housing vouchers and authorize the HUD CoC and Leadership Board chairs to sign the EHV Memorandum of Understanding on behalf of the Continuum of Care (MOU) between the CoC and four recipient PHA’s on the HUD CoC Committee’s behalf.
   b. The System Coordination Committee voted and recommended that Project Roomkey residents be prioritized for the vouchers and then to set aside vouchers for communities that are underrepresented in Project Roomkey, including fleeing Domestic Violence/GBV survivors and Transition Aged Youth.
   c. The committee discussed that there may be populations left out of this targeting, including those currently in Rapid Rehousing and unable to take on the rent after subsidies end, and those currently residing in the FEMA trailers.
   d. C'Mone F. made a motion to target the vouchers as recommended by the System Coordination Committee and authorization for the HUD CoC Committee and Leadership Board Chairs to review/sign final MOU on behalf of the CoC. Lara T. seconded.

   1. C'Mone=Yes
   2. Josh=Yes
   3. Riley=Yes
   4. Marnelle=Yes
   5. Paul=Yes
   6. Lara=Yes
   7. Tunisia=Yes
   8. Paulette=Yes
   9. Wendy=Yes
   a. The motion passed.

9. Announcements and Next Meeting/Agenda
   a. Next Meeting: August 17, 2021 from 2:00-4:30 p.m.
   b. An emergency meeting to take action on the CoC NOFA may be scheduled in July.

Notes submitted by: Alexis Lozano
Reviewed by: Ja’Nai Aubry
Privacy Policy

All Continuums of Care are responsible for the oversight and operation of a Homeless Management Information System. The Oakland-Berkeley-Alameda County (CA-502) CoC recognizes its responsibility to safeguard the privacy of information collected about people experiencing homelessness. At the same time, the CA-502 CoC affirms its support for sharing HMIS data to facilitate and enhance care coordination, reimbursement for services, homeless system planning, and public knowledge of homelessness. This Policy describes standards for the privacy of personal information collected and stored in the Homeless Management Information System (HMIS) and elsewhere within the CA-502 CoC network. The standards seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. This Privacy Policy (hereinafter referred to as “Policy”) is based on principles of fair information practices recognized by the information privacy and technology communities.

This Policy defines the privacy standards that will be required of any organization within the CA-502 CoC (such as a homeless assistance provider, health care organizations offering housing services or HMIS software company) that records, uses, or processes personally identifiable information (PII) on clients at-risk of or experiencing homelessness for the CA-502 CoC HMIS. Organizations must also comply with federal, state, and local laws that require additional confidentiality protections, where applicable.

This Policy recognizes the broad diversity of organizations that participate in the CA-502 CoC HMIS, and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some organizations (e.g., such as those serving victims of domestic violence, runaway youth or persons with substance use disorder) must implement higher levels of privacy standards because of the nature of the clients they serve and / or service provisions. Others (e.g., large emergency shelters) may find higher standards overly burdensome or impractical. At a minimum, however, all organizations must meet the privacy standards described in this Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for organizations with additional needs or capacities.

The following sections discuss the CA-502 CoC HMIS privacy standards in close alignment with the federal HUD HMIS Privacy and Security Standards.

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
1 Definitions and Scope

1.1. Definitions

- **Homeless Management Information System (HMIS):** A local information technology system used to collect client-level data and data on the provision of housing and services to homeless individuals and families and persons at risk of homelessness.

- **Coordinated Entry:** A process developed to ensure that all people experiencing a housing crisis have fair and equal access and are quickly identified, assessed for, referred, and connected to housing and assistance based on their strengths and needs. In the CA-502 CoC, the HMIS is used to support coordinated entry.

- **Personally Identifiable Information (PII):** Any information maintained by or for a Covered Homeless Organization about a client at-risk of or experiencing homelessness that: (1) identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

Set forth below is a non-exclusive list of information that may constitute PII on its own or in combination with other information:

- Full name
- Home address
- Business Contact Information
- Personal email address
- Social security number
- Passport number
- Driver’s license number
- Certificate number
- Credit card numbers
- Date of birth
- Telephone number
- Log in details
- Personnel number
- Vehicle identifier or serial number
- Photograph or video identifiable to an individual
- Biometric information
- Medical information
- Criminal history
- Other information related to an individual that may directly or indirectly identify that individual (e.g., salary, performance rating, purchase history, call history, etc.) [3]

- **Covered Homeless Organization (CHO):** Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, discloses or processes PII on clients at-risk of or experiencing homelessness for an HMIS. This definition includes both organizations that have direct access to the CA-502 CoC HMIS,

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to [jessica@hanserdhealth.com](mailto:jessica@hanserdhealth.com) and [SWarner@acgov.org](mailto:SWarner@acgov.org).
as well as those formally partnering organizations who do not but do record, use, or process PII of target population clients.

- **Recording**: Activities internal to any given CHO that involve creating a hard copy or electronic record of data that includes PII.
- **Uses**: Activities internal to any given CHO that involves interaction with PII.
- **Disclosures**: Activities in which a CHO shares PII externally with other entities.
- **Compelled Disclosures**: Activities in which a CHO is legally compelled by law to share PII.
- **Processing**: Any operation or set of operations performed on PII, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission, and destruction of the information.
- **Permitted Uses and Disclosures**: The uses and disclosures of PII that are allowed by this Policy, in alignment with the federal HUD HMIS Privacy Standards. [1]

### 1.2 Applying this Policy

This Policy applies to any homeless assistance organization that records, uses, or processes personally identifiable information (PII) for the CA-502 CoC HMIS. A provider that meets this definition is referred to as a covered homeless organization (CHO). All PII maintained by a CHO in print or electronic formats is subject to these standards.

Any CHO that is covered under the Health Insurance Portability and Accountability Act (HIPAA) is not required to comply with this Policy if the CHO determines that a substantial portion of its PII about clients at-risk of or experiencing homelessness is protected health information as defined in the HIPAA rules. Exempting HIPAA-covered entities from this Policy avoids all possible conflicts between the two sets of rules.

This Policy gives precedence to the HIPAA privacy and security rules because:

1. The HIPAA rules are more finely attuned to the requirements of the health care system;
2. The HIPAA rules provide important privacy and security protections for protected health information; and
3. Requiring a homeless provider to comply with or reconcile two sets of rules would be an unreasonable burden.

It is possible that part of a homeless organization’s operations may be covered by this Policy while another part is covered by the HIPAA standards. A CHO that, because of organizational structure, legal requirement, or other reason, maintains personal information about a client at-risk of or experiencing homelessness that does not fall under this Policy (e.g., the information is subject to the HIPAA health privacy rule) must describe that information in its privacy notice

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
and explain the reason the information is not covered. The purpose of the disclosure requirement is to avoid giving the impression that all personal information will be protected under this Policy if other standards or if no standards apply. [2]

2 Allowable HMIS Uses and Disclosures of Personally Identifiable Information (PII)

Clients will provide written or verbal consent for any uses and disclosures defined in this section.

2.1 Permitted Uses and Disclosures

Per the 2004 HMIS Data and Technical Standards, HUD permits the following uses and disclosures of PII without participant consent, provided that the uses and disclosures are listed in the Privacy Notice. If any of these uses and disclosures are not listed in the Privacy Notice, written consent is required:

1. To provide or coordinate services for an individual or household
2. For functions related to payment or reimbursement for such resources and services;
3. To carry out administrative functions, including but not limited to legal, audit, personnel, oversight, contractual obligations and management functions; or
4. For creating deidentified PII.

CHOs, like other institutions that maintain personal information about individuals, have obligations that may transcend the privacy interests of clients. The following additional uses and disclosures recognize those obligations to use or share personal information by balancing competing interests in a responsible and limited way. Under this Policy, these additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with this Policy). However, nothing in this Policy modifies an obligation under applicable law to use or disclose personal information.

2.2 Additional Permissions

Per the 2004 HMIS Data and Technical Standards, HUD also permits the following uses and disclosures of PII without participant consent, provided that these additional uses and

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
disclosures are listed in the Privacy Notice. If any of these uses and disclosures are not listed in a CHO’s Privacy Notice, written consent is required:

2.2.1 Uses and disclosures required by law

A CHO may use or disclose PII when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law. For example, information may need to be disclosed to the Department of Health and Human Services to make sure that a client’s rights have not been violated.

2.2.2 Uses and disclosures to avert a serious threat to health or safety

A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PII if:

1. The CHO, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
2. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

2.2.3 Uses and disclosures about victims of abuse, neglect or domestic violence

A CHO may disclose PII about an individual whom the CHO reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority (including a social service or protective services organization) authorized by law to receive reports of abuse, neglect or domestic violence under the following circumstances:

1. Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law; or
2. If the individual agrees to the disclosure; or
3. To the extent that the disclosure is expressly authorized by statute or regulation; and the CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PII for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
A CHO that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if:

1. The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
2. The CHO would be informing a personal representative (such as a family member or friend), and the CHO reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the CHO, in the exercise of professional judgment.

2.2.4 Uses and disclosures for academic research purposes.

A CHO may use or disclose PII for internal quality improvement or evaluation conducted by an individual or institution that has a formal relationship with the CHO if the analysis is conducted either:

- By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the CHO;
- By an institution for use in a research project conducted under a written research agreement approved in writing by the CoC Board.

A written research agreement must:

1. Establish rules and limitations for the processing and security of PII in the course of the research;
2. Provide for the return or proper disposal of all PII at the conclusion of the research;
3. Restrict additional use or disclosure of PII, except where required by law; and
4. Require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

A written data sharing agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board, or other applicable human subjects protection institution.

Any research / evaluation on the nature and patterns of homelessness (at the CA-502 CoC-wide level) that uses PII HMIS data will take place only on the basis of specific agreements between researchers and the entity that administers the HMIS. These agreements must be approved by

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
the CA-502 CoC Board and must reflect adequate standards for the protection of confidentiality of data.

2.2.5 Disclosures for law enforcement purposes

A CHO may, consistent with applicable law and standards of ethical conduct, disclose PII for a law enforcement purpose to a law enforcement official under any of the following circumstances:

- In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
- If the CHO believes in good faith that PII disclosure is necessary to report specified types of criminal conduct to law enforcement in order to seek remediation. This policy allows for the disclosure of PII to report crimes that cause harm to the CHO’s assets, personnel, participants served, or other members of the public. Examples of criminal conduct covered include: assault or bodily harm of any type, harassment, credible threats of violence, theft, destruction of property, and manufacture/production or distribution of controlled substances on CHO premises. It is not intended to cover minor infractions such as personal possession or use of controlled substances, unless covered elsewhere in this policy (i.e. Section 2.3.2).
- If the official is an authorized federal official seeking PII for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought. [4]

3 Privacy Requirements and Responsibilities

All CHO’s involved with the CA-502 CoC HMIS must comply with the privacy requirements described here with respect to:

1. Data collection limitations;
2. Data quality;
3. Purpose and use limitations;
4. Openness;
5. Access and correction; and
6. Accountability.

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
A CHO must comply with federal, state, and local laws that require additional confidentiality protections. All additional protections must be described in the CHO’s privacy notice. A CHO must comply with all privacy protections in this Notice and with all additional privacy protections included in its privacy notice, where applicable.

A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PII. When PII is shared between organizations, responsibilities for privacy may reasonably be allocated between the organizations. Organizations sharing a common data storage medium and PII may adopt differing privacy policies as they deem appropriate, administratively feasible, and consistent with this Policy, which allows for the de-duplication of clients at-risk of or experiencing homelessness at the CoC level.[5] Those differing privacy policies may mean that one CHO has a more rigorous privacy standard, but each policy must, at minimum, meet and not contradict the privacy standards set forth herein. In addition, CHO's must maintain documentation regarding changes to their privacy policies.

3.1 Data Collection Limitation

A CHO may collect PII only when appropriate to the purposes for which the information is obtained or when required by law. A CHO must collect PII by lawful and fair means and, where appropriate, with the knowledge of the individual.

A CHO must post a sign at each intake desk (comparable location) or available on a clipboard in the field that explains generally the reasons for collecting this information and how to obtain a copy of the Privacy Policy. Staff must also verbally explain this information during enrollment and obtain written or verbal consent.

3.2 Data Quality

PII collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PII should be accurate, complete, and timely, as defined by the CA-502 Data Quality Monitoring Plan. A CHO must develop and implement a plan to dispose of, or remove identifiers from, PII that is not in current use seven years after the PII was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention). [8]

3.3 Purpose Specification and Use Limitation

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
A CHO may use or disclose PII only if the use or disclosure is allowed by this Policy. A CHO may assume consent for all uses and disclosures specified in this Policy and for uses and disclosures determined by the CHO to be compatible with those specified in this Policy. This Policy limits the disclosure of PII to the minimum necessary to accomplish the purpose of the disclosure. Uses and disclosures not specified in this Notice can be made only with the consent of the client or when required by law.

A CHO processing PII for the purposes of the CA-502 CoC HMIS will agree to additional restrictions on the use or disclosure of the client’s PII by obtaining oral or written individual consent using the CA-502 CoC Information Sharing Authorization - Housing (ISA-H) form.

A CHO processing PII for the purposes of the CA-502 CoC HMIS will agree to additional restrictions on the use or disclosure of the client’s PII at the request of the client, where it is reasonable to do so. This can include, but is not limited to, the following additional restrictions:

1. Entering client PII into the HMIS so that it is not shared with any other CHO; or
2. Using de-identified client information when coordinating services through the HMIS.

A CHO, in the exercise of professional judgment, will communicate with a client who has requested additional restrictions, when it is reasonable to agree to these and alternatives in situations where it is not reasonable. [9]

### 3.4 Openness

A CHO must adhere to this Policy and describe its policy and practices for the processing of PII and must provide a copy of this Policy to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its Policy on the web page. A CHO must post the CA-502 Consumer Notice stating the availability of its Policy to any individual who requests a copy.

This Policy may be amended at any time and amendments may affect PII obtained by a CHO before the date of the change. An amendment to this Policy regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

CHOs are obligated to provide reasonable accommodations for persons with disabilities throughout the data collection process. This may include but is not limited to, providing qualified sign language interpreters, readers or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability. See 24 CFR 8.6; 28 CFR 36.303. Note: This obligation does not apply to CHOs who do not receive federal financial assistance and who

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
are also exempt from the requirements of Title III of the Americans with Disabilities Act because they qualify as “religious entities” under that Act.

In addition, CHO's that are recipients of federal financial assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the program. See HUD Limited English Proficiency Recipient Guidance published on December 18, 2003 (68 FR 70968). [10]

### 3.5 Access and Correction

In general, a CHO must allow an individual to inspect and to have a copy of any PII about the individual. A CHO must offer to explain any information that the individual may not understand. A CHO must consider any request by an individual for correction of inaccurate or incomplete PII pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

A CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PII:

1. Information compiled in reasonable anticipation of litigation or comparable proceedings;

2. Information about another individual (other than a health care or homeless provider);

3. Information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or

4. Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual. A CHO can reject repeated or harassing requests for access or correction.

A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the PII about the individual. [11]

### 3.6 Accountability

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and Swarner@acgov.org.
A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign annually a confidentiality agreement that acknowledges receipt of a copy of this Policy and that pledges to comply with this Policy. [12]

In the event of an unlawful privacy or security breach, CHO(s) are required to notify the HMIS team within three business days following the CA-502 CoC Incident Reporting form and process. The HMIS team will respond within 3 business days of receiving the notification. The incident may be escalated to the HMIS Oversight Committee. A written response or corrective action plan will be provided. Corrective actions may include notifying the consumer, downgrading system access, terminating user privileges, and disciplinary actions up to and including termination.

4 Special Considerations

This section addresses special considerations that prohibit data sharing without a written consent.

4.1 Runaway and Homeless Youth (RHY) or Emancipated Minors

For RHY grantees, data can only be shared if written consent is obtained from the parent or legal guardian of a youth who is under age 18, or with written consent from a youth who is emancipated.

The RHY rule states the following regarding data sharing: Pursuant to the Act, no records containing the identity of individual youth served by a Runaway and Homeless Youth grantee may be disclosed except:

1. For Basic Center Program grants, records maintained on individual youth shall not be disclosed without the informed consent of the youth and parent or legal guardian to anyone other than another organization compiling statistical records, or a government organization involved in the disposition of criminal charges against the youth;
2. For Transitional Living Programs, records maintained on individual youth shall not be disclosed without the informed written consent of the youth to anyone other than an organization compiling statistical records;

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
3. Research, evaluation, and statistical reports funded by grants provided under section 343 of the Act are allowed to be based on individual youth data, but only if such data are de-identified in ways that preclude disclosing information on identifiable youth;

4. Youth served by a Runaway and Homeless Youth grantees shall have the right to review their records; to correct a record or file a statement of disagreement; and to be apprised of the individuals who have reviewed their records;

5. The Department of Health and Human Services (HHS) policies regarding confidential information and experimentation and treatment shall not apply if HHS finds that state law is more protective of the rights of youth;

6. Procedures shall be established for the training of RHY program staff in the protection of these rights and for the secure storage of records. 45 CFR § 1351.21.

4.2 Victim Service Providers

VAWA Section 3, regulations prohibit Victim Service Providers from sharing personally identifying information about victims without informed, written, reasonably time-limited consent. VAWA also prohibits Victim Service Providers from disclosing individual information without written consent. Victim Service Providers are agencies receiving federal funds to serve survivors. Funding requirements prohibit Victim Service Providers from requiring a signed consent as a condition of service. Additionally, Victim Service Providers cannot share PII to comply with Federal, Tribal, or State reporting, evaluation, or data collection requirements.

These provisions do allow survivors to make a request that their personal confidential information be shared by a victim service provider for a specific purpose by completing a (1) time-limited, (2) informed, and (3) written or verbal consent. The consent (specific and time-limited) must be for services requested by the survivor and they must be fully informed of all possible consequences of disclosure, as well as alternative ways to meet their needs without having to consent to release of confidential information. [13]


Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.


[8] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.2 pg. 45929-45930

[9] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.3 pg. 45930

[10] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.4 pg. 45930


[12] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.6 pg. 45931


Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
Security Policy

All Continuums of Care are responsible for the oversight and operation of a Homeless Management Information System. The Oakland-Berkeley-Alameda County (CA-502 CoC) recognizes its responsibility to safeguard the security of information collected about people experiencing homelessness. At the same time, the CoC affirms its support for sharing HMIS data to facilitate and enhance care coordination, reimbursement for services, homeless system planning, and public knowledge of homelessness. This Policy describes standards for the security of personal information collected and stored in the Oakland-Berkeley-Alameda County Continuum of Care (CA-502 CoC) Homeless Management Information System (HMIS), and elsewhere within the CA-502 CoC network. The standards seek to ensure the security of personal information. This HMIS Security Policy (hereinafter referred to as “Policy”) is based on principles of fair information practices recognized by the information security and technology communities.

This Policy defines the security standards that will be required of any organization within the CA-502 CoC CoC that records, uses, or processes personally identifiable information (PII) on clients at-risk of or experiencing homelessness for the CA-502 CoC HMIS. Organizations must also comply with federal, state, and local laws that require additional security protections, where applicable.

This Policy recognizes the broad diversity of organizations that participate in the CA-502 CoC HMIS and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some organizations (e.g., such as those serving victims of domestic violence) may choose to implement higher levels of security standards because of the nature of the clients they serve and / or service provision. Others (e.g., large emergency shelters) may find higher standards overly burdensome or impractical. At a minimum, however, all organizations must meet the security standards described in this Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for organizations with additional needs or capacities.

The following sections discuss the CA-502 CoC HMIS and the CA-502 CoC CES security standards in close alignment with the federal HUD HMIS Privacy and Security Standards.

1 HMIS SECURITY DEFINITIONS

- **Homeless Management Information System (HMIS):** A local information technology system used to collect client-level data and data on the provision of housing and services to homeless individuals and families and persons at risk of homelessness.

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhcsolutions.com and copy SWarner@acgov.org.
Security Policy

- **Coordinated Entry**: A process developed to ensure that all people experiencing a housing crisis have fair and equal access and are quickly identified, assessed for, referred, and connected to housing and assistance based on their strengths and needs. In the CA-502 CoC CoC, the HMIS is used to support coordinated entry.

- **Personally Identifiable Information (PII)**: Any information maintained by or for a Covered Homeless Organization about a client at-risk of or experiencing homelessness that: (1) identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

Set forth below is a non-exclusive list of information that may constitute PII on its own or in combination with other information:

- Full name
- Home address
- Business Contact Information
- Personal email address
- Social security number
- Passport number
- Driver's license number
- Certificate number
- Credit card numbers
- Date of birth
- Telephone number
- Log in details
- Personnel number
- Vehicle identifier or serial number
- Photograph or video identifiable to an individual
- Biometric information
- Medical information
- Criminal history
- Other information related to an individual that may directly or indirectly identify that individual (e.g., salary, performance rating, purchase history, call history, etc.)

- **Covered Homeless Organization (CHO)**: Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, discloses or processes PII on clients at-risk of or experiencing homelessness for an HMIS. This definition includes both organizations that have direct access to the CA-502 CoC CoC HMIS as well as those organizations who do not but do record, use, or process PII of target population clients.

- **Recording**: Activities internal to any given CHO that involve creating a hard copy or electronic record of data that includes PII.

- **Uses**: Activities internal to any given CHO that involves interaction with PII.

- **Disclosures**: Activities in which a CHO shares PII externally with other entities.

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhcsolutions.com and copy SWarner@acgov.org.
Security Policy

- **Processing:** Any operation or set of operations performed on PII, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission, and destruction of the information.

## 2 System Security

### 2.1 Applicability

A CHO must apply system security provisions to all the systems where PII is stored, including, but not limited to, a CHO’s networks, desktops, laptops, mini-computers, mainframes, and servers.

### 2.2 User Authentication

Each user accessing a machine that contains CA-502 CoC HMIS and / or CoC data must have a unique username and password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

- Using at least one number and one letter or symbol;
- Not using, or including, the username, the HMIS name, or the HMIS vendor’s name; and / or
- Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location. Individual users must not log on to more than one workstation at a time, or log on to the network at more than one location at a time.

### 2.3 Virus Protection

A CHO must protect the CA-502 CoC HMIS and any electronic device used to store PII by using available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the CA-502 CoC HMIS application is used and / or where PII is stored. A CHO must regularly update virus definitions from the software vendor.

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhcsolutions.com and copy SWarner@acgov.org.
Security Policy

2.4 FIREWALLS

A CHO must protect the CA-502 CoC HMIS and any electronic device used to store PII from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, so long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization.

For example, a laptop, which can be used to access the CA-502 CoC HMIS inside or outside the CHO, must be equipped with its own firewall.

2.5 PUBLIC ACCESS

The CA-502 CoC HMIS and any electronic device used to store PII that use public forums for data collection or reporting must be secured to allow only connections from previously approved computers and systems through Public Key Infrastructure (PKI) certificates, or extranets that limit access based on the Internet Provider (IP) address, or similar means. A public forum includes systems with public access to any part of the computer through the Internet, modems, bulletin boards, public kiosks or similar arenas.

2.6 PHYSICAL ACCESS TO SYSTEMS WITH ACCESS TO HMIS DATA

A CHO must, at all times, staff computers stationed in public areas that are used to collect and store CA-502 CoC HMIS data. When workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password-protected screensaver when the workstation is temporarily not in use. Password-protected screensavers are a standard feature with most operating systems and the amount of time can be regulated by a CHO. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system and shut down the computer.

2.7 DISASTER PROTECTION AND RECOVERY

The CA-502 CoC HMIS data is copied on a regular basis to another medium (e.g., tape) and stored in a secure off-site location where the required security standards apply. The CHO that stores the data in a central server stores that central server in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors or equivalent modern

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhcsolutions.com and copy SWarner@acgov.org.
Security Policy

technology is used to protect systems used for collecting and storing all the CA-502 CoC HMIS data.

2.8 DISPOSAL

In order to delete all CA-502 CoC HMIS data from a data storage medium (e.g. computer, phone, USB drive, CD), a CHO must reformat the storage medium. A CHO should reformat the storage medium more than once before reusing or disposing the medium. Prior to disposing of any data storage medium that contains, or may contain, CA-502 HMIS data, the CHO must take measures to render the data unrecoverable.

2.9 SYSTEM MONITORING

A CHO must use appropriate methods to monitor security systems. Systems that have access to any CA-502 CoC HMIS data must maintain a user access log. Many new operating systems and web servers are equipped with access logs and some allow the computer to email the log information to a designated user, usually a system administrator. Logs must be checked routinely.

3 APPLICATION SECURITY

These provisions apply to how all the CA-502 CoC HMIS data are secured by the HMIS application software.

3.1 APPLICABILITY

A CHO must apply application security provisions to the software during data entry, storage, and review or any other processing function.

3.2 USER AUTHENTICATION

A CHO must secure all electronic CA-502 CoC HMIS data with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhcsolutions.com and copy SWarner@acgov.org.
Security Policy

- Using at least one number and one letter or symbol;
- Not using, or including, the username, the HMIS name, or the HMIS vendor’s name; and
- Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users should not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

3.3 Electronic Data Transmission

A CHO must encrypt all CA-502 CoC HMIS data that are electronically transmitted over the Internet, publicly accessible networks, or phone lines to current industry standards. Unencrypted data may be transmitted over secure direct connections between two systems. A secure direct connection is one that can only be accessed by users who have been authenticated on at least one of the systems involved and does not utilize any tertiary systems to transmit the data. A secure network would have secure direct connections.

3.4 Electronic Data Storage

A CHO must store all CA-502 CoC HMIS data in a binary, not text, format. A CHO that uses one of several common applications (e.g., Microsoft Access, Microsoft SQL Server, or Oracle) are already storing data in binary format and no other steps need to be taken.

4 Hard Copy Security

This section provides standards for securing hard copy data.

4.1 Applicability

A CHO must secure (e.g. locked drawer or cabinet) any paper or other hard copy containing PII that is either generated by or for the CA-502 CoC HMIS, including, but not limited to reports,

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhcsolutions.com and copy SWarner@acgov.org.
Security Policy

data entry forms, and case / client notes. Note: Many CHOs will require stricter policies such as double locking (e.g. locked drawer in a locked office) due to other regulations or funding requirements.

4.2  SECURITY

A CHO must, at all times, supervise any paper or other hard copy generated by or for the CA-502 CoC HMIS that contains PII. When CHO staff are not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location.

Please note this is Work in Process modeled after another COC. Please send any questions, concerns or other feedback to jessica@hanserdhcsonline.com and copy SWarner@acgov.org.