HUD CoC Committee Agenda
Monday, March 28th, 2022
1:00 p.m. – 3:30 p.m.

Zoom Link:  https://us02web.zoom.us/j/82227753659
Meeting ID: 822 2775 3659
One tap mobile: +16699006833, 82227753659# US (San Jose)

Meetings are public. Alameda County residents with lived experience of homelessness are 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) 1:00-1:05pm
2. HUD CoC Public Comment 1:05-1:15pm
3. Approval of Meeting Minutes, #2- 02.28.22 1:15-1:20pm
   Action Item
4. Homeless System Updates (All) 1:20-1:25pm
   Update
5. Governance Update (Chelsea) 1:25-1:30pm
   Update
6. Consulting Contracts Updates 1:30-1:50pm
   Action Item
   a. NOFO Contract Working Group Update
   b. EveryOne Home / HCD – HUD CoC Planning Grant
7. Review NOFO 2021 Competition Awards (Chelsea / Riley) 1:50-2:00pm
   Update
8. HMIS Privacy Policy Revisions (Jessica Hanserd / Suzanne) 2:00-2:25pm
   Action Item
   a. Approve revisions to the HMIS Privacy Policy that reflect an inferred consent model (a low barrier approach)
9. Coordinated Entry / Emergency Housing Voucher Update (Colleen) 2:25-2:30pm
   Update
10. YHDP Coordinated Community Plan Draft Review (All In / YAB) 2:30-2:50pm
    Update
    a. Presentation of the draft Youth Homelessness Demonstration Program (YHDP) Coordinated Community Plan prior to final review and approval at special meeting of the HUD CoC Committee in April
11. HMIS Data Quality Action Plan (Katie Haverly) 2:50-3:10pm
**Update**

12. Point in Time Count Shelter Data Review 3:10-3:25pm

*Action Item*

a. **CLOSED SESSION**

13. HUD CoC Committee Upcoming Events 3:25-3:30pm

- a. **Special meeting to vote on YHDP CCP** prior to HUD submission – TBD
- b. Monthly HUD CoC Committee meeting – **April 25th, 2022**
Present: C’Mone Falls (City of Oakland), Josh Jacobs (City of Berkeley), Riley Wilkerson (Alameda County Housing and Community Development), Lara Tannenbaum (City of Oakland), Paul Berry (Youth Action Board), Tunisia Owens (Family Violence Law Center)

Absent: Marnelle Timson (Consumer Member), Wendy Jackson (East Oakland Community Project), Paulette Franklin (Alameda County Behavioral Health Care Services)

Members of the public: Natasha Paddock (Alameda County Housing and Community Development), Patrick Crosby (Alameda County Housing and Community Development), Althimus Sigue (Youth Action Board), Hannah Moore (All-In), Sahra Nawabi (Youth Action Board), Colleen Budenholzer (Alameda County Health Care Services Agency), Tammy N. (Youth Action Board)

EveryOne Home Staff: Chelsea Andrews (Executive Director), Katie Barnett (Systems Planning Coordinator), Katie Haverly (Director of Research and Data Analytics)

Meetings are public. Alameda County residents with lived experience of homelessness are 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. HUD CoC Public Comment
3. Approval of Meeting Minutes, #1- 1.12.22 and #2 – 1.24.22
   a. Lara Tannenbaum (City of Oakland) motioned to approve the meeting minutes from 1/12/22 and 1/24/22.
      i. Josh Jacobs (City of Berkeley) seconded.
         1. C’Mone Falls - Yes
         2. Paul Berry - Yes
         3. Josh Jacobs - Yes
         4. Lara Tannenbaum - Yes
         5. Riley Wilkerson – Yes
            ii. Motion passed

4. Homeless System Updates (All)
   a. Josh Jacobs (City of Berkeley) and Lara Tannenbaum (City of Oakland) announced the City of Oakland and City of Berkeley were both awarded new state funding related to relocating residents of a specific encampment into interim or permanent housing.
b. Hannah Moore (All-In) announced that the Youth Homelessness Demonstration Program (YHDP) team will be holding two in-person youth systems modeling sessions on March 8th and March 10th, 9:00 AM to 12:00 PM at the Reach Ashland Youth Center in San Leandro.

c. Lara Tannenbaum (City of Oakland) noted that none of the projects in Alameda County were awarded funding for permanent housing from Project Homekey. This came as a shock to the cities and county, and responding to it will require advocacy that is already underway.

d. Lara Tannenbaum (City of Oakland) noted that HMIS system data reports are currently not generating properly due to changes in Bitfocus. Service providers will need to be made aware of this throughout the county.
   i. Natasha Paddock (Alameda County Housing and Community Development) noted the HMIS leads will be meeting with Bitfocus to clarify the source of this error and how to address it. This subject will likely be addressed at the next HMIS Oversight Committee.

5. Governance Update (Chelsea)
   a. On February 2nd, the Continuum of Care (CoC) membership approved the new CoC governance structure. The timeline for implementing the new governance is approximately six months.
   b. A transition working group has formed and held its first meeting. The three co-chairs are Moe Wright (Leadership Board Chair), Natasha Paddock (Alameda County Housing and Community Development), and Kate Hart (System Coordination Committee Co-Chair).
   c. Updates about elections and the formation of a nominating committee will be forthcoming.

6. Point in Time Count Update
   a. Katie Haverly (Director of Research and Data Analytics) provided a summary of the Point in Time (PIT) Count, which took place on February 23rd.
      i. The Count was completed with the help of approximately 500 volunteers, including outreach teams, city and county staff, guides, and community members.
      ii. Volunteer engagement was notably high this year, with 99% of all teams and individuals that signed up completing the Count. In the past, the attrition rate on the day of the Count has been close to 20%.
      iii. Initial data from the Count will be available for cities and jurisdictions in early summer. The full data reports from Applied Survey Research (ASR) will be finished mid-summer. A full press conference will be held with all jurisdictional representation to release the data to the public simultaneously.
      iv. The deadline for data submission to HUD is April 30th, and that will be presented to the HUD CoC Committee for review and approval in April.
   b. Natasha Paddock (Alameda County Housing and Community Development) noted that ASR is in contract to deliver a dashboard for this year’s count data, which is expected to be available approximately two months in advance of the full report.

7. Emerging Leaders Update
   a. Katie Barnett (Systems Planning Coordinator) provided an update on the Emerging Leaders Program for individuals with lived experience of homelessness. The inaugural class will launch on March 1st, and two more cohorts will convene before the end of July.
   b. The number of applicants for the first cohort exceeded expectations, and recruitment will continue on a rolling basis.
8. CoC Consulting Contracts Overview
   a. Following the HUD CoC Committee in January, EveryOne Home met with the county to discuss the CoC’s consulting contracts. The recommendation is that each procurement is overseen by individual committees consisting of representatives from Housing and Community Development (HCD), Healthcare Services Agency (HCSA), EveryOne Home, and a representative from the HUD CoC Committee and Leadership Board.
      I. This approach will ensure that procurement is timely and that each process can involve individuals with relevant expertise.
      II. The recommendations of that committee will come to the HUD CoC Committee for approval.
      III. The need to form this committee for the Notice of Funding Opportunity (NOFO) consultant hiring process is urgent.
   b. Lara Tannenbaum (City of Oakland) asked for clarification about the potential conflict of interest if the county is responsible for monitoring itself.
      I. Natasha Paddock (Alameda County Housing and Community Development) clarified that HUD monitors HCD as the Collaborative Applicant in the NOFO competition. The support provided by the consultant would include monitoring sub-recipients of HCD funding, but the committee leading the procurement process could identify additional safeguards.
   c. C’Mone Falls (City of Oakland) asked committee members to check availability and follow up if they can serve on the committee to contract a NOFO consultant. If there are no volunteers, she will nominate someone and reach out to them directly.

9. HHAP Reminder
   a. C'Mone Falls (City of Oakland) provided an update on the Homeless Housing, Assistance, and Prevention (HHAP) grant status. Round One is almost finished. Jurisdictions will receive Round Two funds soon.
   b. The Round Three application was released, and jurisdictions will be working on the application process until summer. Anyone unfamiliar with HHAP is encouraged to learn about it in advance of decisions that will need to be made about its use.

10. HMIS Oversight
    a. Patrick Crosby (Alameda County Housing and Community Development) reported that the Longitudinal System Analysis (LSA) was submitted to HUD on time.
    b. The monthly HMIS provider trainings have been going very well. In February the focus was primarily on the Point in Time Count and data preparation for submission.
    c. Riley Wilkerson (Alameda County Housing and Community Development) asked for clarification about the HMIS problems with system performance measures related to individual programs.
       (i) The reporting systems weren’t designed to have the level of functionality that’s desired. Attempts were made to run reports that would return program-level data, but it was very slow and never fully functional. In late November, those reports stopped working entirely. It puts a lot of strain on the system, and Bitfocus has not shown interest in developing this feature.
       (ii) Data analysis reports have been taken down until the problem can be addressed.
    d. Katie Haverly (Director of Research and Data Analytics) asked if insight could be provided to the committee about the challenges related to data on race and ethnicity when looking at system performance measures in the HMIS system.
       (i) Trying to break down system performance measures by race and ethnicity causes the same problem with the system strain. The system performance measures reports are particularly complex due to the way HUD wants people
counted. Some of the measures count an individual once, while others count them multiple times based on their movement in or out of the system over time.

11. Coordinated Entry / Emergency Housing Vouchers (Colleen)
   a. There are 2,785 people enrolled in Housing Problem Solving and 4,520 people enrolled in Coordinated Entry. 823 individuals are on the Crisis Queue, and 1,208 are on the Housing Queue.
      I. The System Coordination Committee approved the Coordinated Entry policies in February.
      II. The first five Coordinated Entry training models are now available, which cover the core training for direct service staff. There’s been a significant increase in the number of completed trainings and requests for Coordinated Entry access and HMIS.

12. Emergency Housing Vouchers Update
   a. The total number of vouchers is 875. There have now been 993 people matched, 401 vouchers issued, and 66 leased up.
   b. Out of the 10% set-aside for the gender-based violence community, 77 applications have been submitted and 3 vouchers have been leased up. From the Transition Age Youth (TAY) set-aside, 26 applications have been submitted and 6 vouchers have been leased up.

13. YHDP Update/ Consulting Contracts Budget
   a. Hannah Moore (All-In) and Sahra Nawabi (YAB Peer Mentor) presented the YHDP planning budget.
      I. Approximately $10,000 has been used to obtain 15 iPads for Youth Action Board members and smart keyboards for YAB Peer Mentors.
      II. Stipends totaling $28,000 were budgeted for ten youth participants involved in Coordinated Community Plan (CCP) development and the upcoming YHDP NOFO.
      III. Other support costs in the budget include a data consultant and CCP/NOFO consultant, as well as CCP visual design and technical assistance.
      IV. Some funding is allocated for a TAP Youth Services Program Manager that will oversee the YHDP and other issues related to youth homelessness in the county. The Office of Homeless Care and Coordination is currently recruiting for this position.
   b. Hannah Moore (All-In) and Paul Berry (YAB Peer Mentor) shared an update on governance structure.
      I. The board will have 8 – 10 seats, and members will be intentionally recruited to reflect a broad range of experiences, including those who are emancipated, pregnant and parenting, LGBTQ, and those impacted by foster care and juvenile justice.
      II. Subcommittees will include Peer Mentors, a Communication Subcommittee, a Work Group, a Data Work Group, and Outreach Work Group.
   c. Paul Berry (YAB) motioned to approve the YHDP planning Budget.
      I. C'Mone Falls (City of Oakland) seconded.
         1. C'Mone Falls - Yes
         2. Paul Berry - Yes
         3. Josh Jacobs - Yes
         4. Lara Tannenbaum - Yes
         5. Riley Wilkerson - Yes
         6. Tunisia Owens – Yes
a. Motion passed.

14. HUD CoC Committee Upcoming Events
   a. Next meeting – **March 28th 1:00pm- 3:30pm**
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.orgwebsite 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.

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.

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.

For a list of organizations that are part of the Oakland-Berkeley-Alameda County Continuum of Care, please visit www.website or ask a staff member for a copy.
Each Covered Homeless Organizations (CHO) who participates in the CA-502 CoC must decide to adopt the CA-502 CoC Privacy Policy (Policy) and the CA-502 COC Privacy Notice (Notice) in whole or adapt them to include stricter protections, as necessary.

HIPAA-covered entities may be exempt. CHOs must also comply with federal, state, and local laws that require additional confidentiality protections, where applicable.

The following Policy recognizes the broad diversity of CHOs that participate in the CA-502 CoC Homeless Management Information System (HMIS), and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some CHOs (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. Unless exempt, CHOs must meet the minimum privacy standards described in the following Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for CHOs with additional needs or capacities.
All Continuums of Care (CoC) are responsible for the oversight and operation of a Homeless Management Information System. The Oakland-Berkeley-Alameda County 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 HMIS and elsewhere in print or electronic formats within the CA-502 CoC network. The standards protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. This Policy is based on principles of fair information practices recognized by the information privacy and technology communities.

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

1 Definitions and Scope

1.1. Definitions

- **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. This definition includes both organizations that have direct access to the CA-502 CoC HMIS, as well as those formally partnering organizations who do not but do record, use, or process PII of target population clients.

- **Disclose:** Activities in which a CHO shares PII externally with other entities. When data is entered into the CA-502 HMIS it is automatically available (disclosed) to all participating CHOs.

- **Homeless Management Information System (HMIS):** A local information technology system used to collect, store and report client-level information about individuals who are seeking services to resolve homelessness or the risk of homelessness.

Sharing HMIS data enhances care coordination, while facilitating reimbursement for services, homeless system planning, and improved public knowledge of homelessness. The HMIS system is designed to improve effectiveness and efficiency for clients, CHOs, provider agencies, jurisdictions, other systems of care, funders, and the community.
Improved knowledge gained from HMIS about various communities with special needs and their service usage aides with providing a more effective and efficient service delivery system.

CA-502 uses Clarity by BitFocus for its HMIS software.

- **Release of Information (ROI):** This consent form is used for housing and homeless prevention services, allowing for the consumer’s PII to be shared with CHOs and other providers that assist clients who are at-risk of or experiencing homelessness.

This consent form is required for any use or disclosure that is not listed as allowable in the CHOs privacy notice. For CHOs that adopt the CA-502 standard Privacy Policy and Privacy Notice in whole, this form will be rarely needed.

- **Participating CHOs:** A list of CA-502 participating CHOs can be found at [https://acgov.org/cda/hcd/documents/roi_providers.pdf](https://acgov.org/cda/hcd/documents/roi_providers.pdf).

- **Personally Identifiable Information (PII):** Any information maintained by or for a CHO 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-exhaustive 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.) [10]
• **Privacy Notice:** A consumer facing summary maintained and published by each CHO that describes its privacy policies and practices for the processing of PII, the reasons for collecting information and uses and disclosures that are allowable. Consent may be assumed for uses and disclosures that are properly disclosed in the Privacy Notice, provided it or its key information is posted as a sign at each intake desk (or comparable location) and on the CHO’s public website.

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

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

• **Use:** Activities internal to any given CHO that involves interaction with PII.

### 1.2 Applying this Policy

This Policy applies to any CHO that records, uses, or processes personally identifiable information (PII) for the Oakland–Berkeley–Alameda County Continuum of Care (CA-502) Homeless Management Information System (HMIS), except for HIPAA covered entities as noted below. 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 required to comply with HIPAA and is not required to comply with the privacy standards in 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’s privacy standards 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 CHO to comply with or reconcile two sets of rules would be an unreasonable burden.

It is possible that part of a CHO’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 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  Assumed Consent

Client consent for collecting PII is assumed when CHOs post the Privacy Notice or its key information at each intake desk (and comparable location) that explains generally the reasons for collecting HMIS information, and the uses and disclosures that are included in the CHOs Privacy Notice.

2.1 Mandatory Uses and Disclosures

Per the 2004 HMIS Data and Technical Standards, HUD requires two mandatory disclosures regardless of their inclusion in the Privacy Notice:

- Participants’ access to their own information
- Disclosures for oversight of compliance with HMIS data privacy and security standards

2.2 Permitted Uses and Disclosures

Per the 2004 HMIS Data and Technical Standards, HUD permits the following uses and disclosures of PII. If any of these uses and disclosures are not listed in the Privacy Notice, explicit consent is required:

1. To provide or coordinate services for an individual or household;
2. For functions related to payment or reimbursement for 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.

2.3 Additional Permissions
Per the 2004 HMIS Data and Technical Standards, HUD also permits the following uses and disclosures of PII, provided that these additional uses and disclosures are listed in the Privacy Notice. If any of these uses and disclosures are not listed in the Privacy Notice, explicit consent is required:

2.3.1 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.

2.3.2 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.

2.3.3 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.

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.

### 2.3.4 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 CHO 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 during 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 research 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 may be conducted only based on specific agreements between
researchers and the entity that administers the HMIS. These agreements must be approved by
the CA-502 CoC Board and must reflect adequate standards for the protection of data
confidentiality.

2.3.5 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 to seek remediation. This Policy allows for
the disclosure of PII to report crimes that occurred on the CHO’s premises (e.g., crimes
that cause harm to the CHO’s premises, 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. [3]

3 Explicit Consent

Explicit consent must be obtained using the Release of Information (ROI) form in either of the
following circumstances:

- For any use or disclosure other than what is defined as allowable (section 2)
- For any use or disclosure that is not properly disclosed in the CHO’s privacy notice
4 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.

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 Policy 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.

4.1 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 or comparable location (e.g., on a clipboard in the field) that explains generally the reasons for collecting this information and how to obtain a copy of its privacy notice. Staff must also verbally explain this information. [4]

### 4.2 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 must 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). [5]

### 4.3 Purpose Specification and Use Limitation

A CHO may use or disclose PII only if the use or disclosure is allowed by this Policy. This Policy limits the disclosure of PII to the minimum necessary to accomplish the purpose of the disclosure.

A CHO processing PII for the purposes of the CA-502 CoC HMIS must 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 may include, but is not limited to, using de-identified client information when coordinating services through the HMIS.

When a client has requested additional restrictions, a CHO, in the exercise of professional judgment, must provide a response. The response must include whether the CHO will agree to the request; and reasonable alternatives, if any, if the CHO determines the request cannot be reasonably accommodated. [6]

### 4.4 Openness

A CHO must publish a privacy notice describing its policies and practices for the processing of PII and must provide a copy of its privacy notice to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page. A CHO must post a sign stating the availability of its privacy notice 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 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, CHOs 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). [7]

### 4.5 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 provider or CHO);
3. Information obtained under a promise of confidentiality (other than a promise from a health care or CHO) 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. [8]

4.6 Accountability

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 the CHO’s current privacy notice and that pledges to comply with the privacy notice. [9]

In the event of an unlawful privacy or security breach, CHOs are required to notify the HMIS Administrator within 3 business days. The HMIS Administrator will respond within 3 business days of receiving the notification. The HMIS Administrator will provide a written response or corrective action plan as appropriate. Corrective actions may include notifying the consumer, downgrading system access, terminating user privileges, and disciplinary actions up to and including termination.
[7] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.4 pg. 45930
[8] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.5 pg. 45930-45931
[9] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.6 pg. 45931
[10] U.S. Department of Housing and Urban Development Privacy Policy, July 2020 pg. 6
Each Covered Homeless Organizations (CHO) who participates in the CA-502 CoC must decide to adopt the CA-502 CoC Security Policy (Policy) in whole or adapt it to include stricter protections, as necessary.

HIPAA-covered entities may be exempt. CHO must also comply with federal, state, and local laws that require additional security protections, where applicable.

The following Policy recognizes the broad diversity of CHO 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 CHO (e.g., such as those serving victims of domestic violence, runaway youth, or persons with substance use disorder) must implement higher levels of security 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. Unless exempt, CHO must meet the minimum security standards described in the following Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for CHO with additional needs or capacities.
All Continuums of Care (CoCs) are responsible for the oversight and operation of a Homeless Management Information System. The Oakland-Berkeley-Alameda County CoC recognizes its responsibility to safeguard the security 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 security of personal information collected and stored in the HMIS and elsewhere in print or electronic formats within the CA-502 CoC network. The standards seek to ensure the security of personal information. This Policy is based on principles of fair information practices recognized by the information security and technology communities.

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

## 1 Definitions and Scope

### 1.1 Definitions

- **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. This definition includes both organizations that have direct access to the CA-502 CoC HMIS, as well as those formally partnering organizations who do not but do record, use, or process PII of target population clients.

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

- **Homeless Management Information System (HMIS):** A local information technology system used to collect, store and report client-level information about individuals who are seeking services to resolve homelessness or the risk of homelessness.

Sharing HMIS data enhances care coordination, while facilitating reimbursement for services, homeless system planning, and improved public knowledge of homelessness. The HMIS system is designed to improve effectiveness and efficiency for clients, CHOs, provider agencies, jurisdictions, other systems of care, funders, and the community. Improved knowledge gained from HMIS about various communities with special needs and their service usage aides with providing a more effective and efficient service delivery system.

CA-502 uses Clarity by BitFocus for its HMIS software.

CA-502 uses Clarity by BitFocus for its HMIS software.
• **Participating CHO**s: A list of CA-502 participating CHO can be found at [https://acgov.org/cda/hcd/documents/roi_providers.pdf](https://acgov.org/cda/hcd/documents/roi_providers.pdf).

• **Personally Identifiable Information (PII):** Any information maintained by or for a CHO 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-exhaustive 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]

• **Privacy Notice:** A consumer facing document maintained and published by each CHO that describes its policies and practices for the processing of PII, the reasons for collecting information and uses and disclosures that are allowable. Consent may be assumed for uses and disclosures that are described as allowable in the Privacy Notice. The Privacy Notice must be posted at each intake desk (or comparable location) and on the CHO’s public website.

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

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

• **Use:** Activities internal to any given CHO that involves interaction with PII.
1.2 APPLYING THIS POLICY

This Policy applies to any CHO that records, uses, or processes personally identifiable information (PII) for the CA-502 CoC HMIS, with the exception of HIPAA covered entities as noted below. 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 required to comply with HIPAA and is not required to comply with the security standards in 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’s privacy standards 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 CHO to comply with or reconcile two sets of rules would be an unreasonable burden.

It is possible that part of a CHO’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 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 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 an electronic device that contains CA-502 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;
- 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 where PII is stored. A CHO must regularly update virus definitions from the software vendor.

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 CHO.

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 must be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations must 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 must log off the data entry system and shut down the computer. A laptop should never be left unattended and should be secured with a lock when used.

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
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 must 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:
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 must 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,
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.
Each Covered Homeless Organization (CHO) who participates in the CA-502 CoC must decide to adopt the CA-502 CoC Privacy Policy (Policy) and the CA-502 COC Privacy Notice (Notice) in whole or adapt them to include stricter protections, as necessary. HIPAA-covered entities may be exempt. CHOs must also comply with federal, state, and local laws that require additional confidentiality protections, where applicable.

The following Policy recognizes the broad diversity of CHOs that participate in the CA-502 CoC Homeless Management Information System (HMIS), and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some CHOs (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. Unless exempt, CHOs must meet the minimum privacy standards described in the following Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for CHOs with additional needs or capacities.
All Continuums of Care (CoC) are responsible for the oversight and operation of a Homeless Management Information System. The Oakland-Berkeley-Alameda County 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 HMIS and elsewhere in print or electronic formats within the CA-502 CoC network. The standards protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. This Policy is based on principles of fair information practices recognized by the information privacy and technology communities.

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

1 Definitions and Scope

1.1. Definitions

- **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. This definition includes both organizations that have direct access to the CA-502 CoC HMIS, as well as those formally partnering organizations who do not but do record, use, or process PII of target population clients.

- **Disclose:** Activities in which a CHO shares PII externally with other entities. When data is entered into the CA-502 HMIS it is automatically available (disclosed) to all participating CHOs.

- **Homeless Management Information System (HMIS):** A local information technology system used to collect, store and report client-level information about individuals who are seeking services to resolve homelessness or the risk of homelessness. Sharing HMIS data enhances care coordination, while facilitating reimbursement for services, homeless system planning, and improved public knowledge of homelessness. The HMIS system is designed to improve effectiveness and efficiency for clients, CHOs, provider agencies, jurisdictions, other systems of care, funders, and the community.
Improved knowledge gained from HMIS about various communities with special needs and their service usage aids with providing a more effective and efficient service delivery system.

CA-502 uses Clarity by BitFocus for its HMIS software.

- **Release of Information (ROI):** This consent form is used for housing and homeless prevention services, allowing for the consumer’s PII to be shared with CHO’s and other providers that assist clients who are at-risk of or experiencing homelessness.

  This consent form is required for any use or disclosure that is not listed as allowable in the CHO’s privacy notice. For CHO’s that adopt the CA-502 standard Privacy Policy and Privacy Notice in whole, this form will be rarely needed.

- **Participating CHO’s:** A list of CA-502 participating CHO’s can be found at [https://acgov.org/cda/hcd/documents/roi_providers.pdf](https://acgov.org/cda/hcd/documents/roi_providers.pdf).

- **Personally Identifiable Information (PII):** Any information maintained by or for a CHO 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-exhaustive 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.)

  [10]
Privacy Notice: A consumer facing summary maintained and published by each CHO that describes its privacy policies and practices for the processing of PII, the reasons for collecting information and uses and disclosures that are allowable. Consent may be assumed for uses and disclosures that are properly disclosed in the Privacy Notice, provided it or its key information is posted as a sign at each intake desk (or comparable location) and on the CHO’s public website.

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

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

Use: Activities internal to any given CHO that involves interaction with PII.

1.2 Applying this Policy

This Policy applies to any CHO that records, uses, or processes personally identifiable information (PII) for the Oakland–Berkeley–Alameda County Continuum of Care (CA-502) Homeless Management Information System (HMIS), except for HIPAA covered entities as noted below. 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 required to comply with HIPAA and is not required to comply with the privacy standards in 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’s privacy standards 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 CHO to comply with or reconcile two sets of rules would be an unreasonable burden.

It is possible that part of a CHO’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 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 Assumed Consent

Client consent for collecting PII is assumed when CHO's post the Privacy Notice or its key information at each intake desk (and comparable location) that explains generally the reasons for collecting HMIS information, and the uses and disclosures that are included in the CHO's Privacy Notice.

2.1 Mandatory Uses and Disclosures

Per the 2004 HMIS Data and Technical Standards, HUD requires two mandatory disclosures regardless of their inclusion in the Privacy Notice:

- Participants' access to their own information
- Disclosures for oversight of compliance with HMIS data privacy and security standards

2.2 Permitted Uses and Disclosures

Per the 2004 HMIS Data and Technical Standards, HUD permits the following uses and disclosures of PII. If any of these uses and disclosures are not listed in the Privacy Notice, explicit consent is required:

1. To provide or coordinate services for an individual or household;
2. For functions related to payment or reimbursement for 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.

2.3 Additional Permissions

Deleted: [3]

Deleted: [4]

Moved down [3]: 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
- 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:

Establish rules and limitations for the processing and security of PII during the research.

Moved down [4]: 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:

Establish rules and limitations for the processing and security of PII during the research.

Deleted: 1.2

Deleted: requirements regarding uses

Deleted: 2.2 Uses and Disclosures that Do Not Require Written Consent
Per the 2004 HMIS Data and Technical Standards, HUD also permits the following uses and disclosures of PII, provided that these additional uses and disclosures are listed in the Privacy Notice. If any of these uses and disclosures are not listed in the Privacy Notice, explicit consent is required:

2.3.1 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.

2.3.2 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.

2.3.3 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.

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.

2.3.4 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 CHO 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 during 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 research 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 may be conducted only based on specific agreements between

Moved (insertion) [3] Moved (insertion) [4]
researchers and the entity that administers the HMIS. These agreements must be approved by the CA-502 CoC Board and must reflect adequate standards for the protection of data confidentiality.

2.3.5 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 to seek remediation. This Policy allows for the disclosure of PII to report crimes that occurred on the CHO’s premises (e.g., crimes that cause harm to the CHO’s premises, 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. [3]

3 Explicit Consent

Explicit consent must be obtained using the Release of Information (ROI) form in either of the following circumstances:

- For any use or disclosure other than what is defined as allowable (section 2)
- For any use or disclosure that is not properly disclosed in the CHO's privacy notice
4 Privacy Requirements and Responsibilities

All CHOs 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.

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 Policy 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, CHOs must maintain documentation regarding changes to their privacy policies.

4.1 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 or comparable location (e.g., on a clipboard in the field) that explains generally the reasons for collecting this information and how to obtain a copy of its privacy notice. Staff must also verbally explain this information. [4]

### 4.2 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 must 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). [5]

### 4.3 Purpose Specification and Use Limitation

A CHO may use or disclose PII only if the use or disclosure is allowed by this Policy. This Policy limits the disclosure of PII to the minimum necessary to accomplish the purpose of the disclosure.

A CHO processing PII for the purposes of the CA-502 CoC HMIS must 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 may include, but is not limited to, using de-identified client information when coordinating services through the HMIS.

When a client has requested additional restrictions, a CHO, in the exercise of professional judgment, must provide a response. The response must include whether the CHO will agree to the request; and reasonable alternatives, if any, if the CHO determines the request cannot be reasonably accommodated. [6]

### 4.4 Openness

A CHO must publish a privacy notice describing its policies and practices for the processing of PII and must provide a copy of its privacy notice to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page. A CHO must post a sign stating the availability of its privacy notice 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 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, CHOs 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). [7]

4.5 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 provider or CHO);
3. Information obtained under a promise of confidentiality (other than a promise from a health care or CHO) 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. [8]

### 4.6 Accountability

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 the CHO’s current privacy notice and that pledges to comply with the privacy notice. [9]

In the event of an unlawful privacy or security breach, CHOs are required to notify the HMIS Administrator within 3 business days. The HMIS Administrator will respond within 3 business days of receiving the notification. The HMIS Administrator will provide a written response or corrective action plan as appropriate. Corrective actions may include notifying the consumer, downgrading system access, terminating user privileges, and disciplinary actions up to and including termination.


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

[8] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.5 pg. 45930-45931

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

[10] U.S. Department of Housing and Urban Development Privacy Policy, July 2020 pg. 6
Each Covered Homeless Organizations (CHO) who participates in the CA-502 CoC must decide to adopt the CA-502 CoC Security Policy (Policy) in whole or adapt it to include stricter protections, as necessary.

HIPAA-covered entities may be exempt. CHOs must also comply with federal, state, and local laws that require additional security protections, where applicable.

The following Policy recognizes the broad diversity of CHOs 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 CHOs (e.g., such as those serving victims of domestic violence, runaway youth, or persons with substance use disorder) must implement higher levels of security 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. Unless exempt, CHOs must meet the minimum security standards described in the following Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for CHOs with additional needs or capacities.
All Continuums of Care (CoCs) are responsible for the oversight and operation of a Homeless Management Information System. The Oakland-Berkeley-Alameda County CoC recognizes its responsibility to safeguard the security 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 security of personal information collected and stored in the HMIS and elsewhere in print or electronic formats within the CA-502 CoC network. The standards seek to ensure the security of personal information. This Policy is based on principles of fair information practices recognized by the information security and technology communities.

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

1 DEFINITIONS AND SCOPE

1.1 DEFINITIONS

- **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. This definition includes both organizations that have direct access to the CA-502 CoC HMIS, as well as those formally partnering organizations who do not but do record, use, or process PII of target population clients.

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

- **Homeless Management Information System (HMIS):** A local information technology system used to collect, store and report client-level information about individuals who are seeking services to resolve homelessness or the risk of homelessness.

Sharing HMIS data enhances care coordination, while facilitating reimbursement for services, homeless system planning, and improved public knowledge of homelessness. The HMIS system is designed to improve effectiveness and efficiency for clients, CHOs, provider agencies, jurisdictions, other systems of care, funders, and the community. Improved knowledge gained from HMIS about various communities with special needs and their service usage aides with providing a more effective and efficient service delivery system.
CA-502 uses Clarity by BitFocus for its HMIS software.

- **Participating CHO's**: A list of CA-502 participating CHO's can be found at https://acgov.org/cda/hcd/documents/roi_providers.pdf.

- **Personally Identifiable Information (PII)**: Any information maintained by or for a CHO 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-exhaustive 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]

- **Privacy Notice**: A consumer facing document maintained and published by each CHO that describes its policies and practices for the processing of PII, the reasons for collecting information and uses and disclosures that are allowable. Consent may be assumed for uses and disclosures that are described as allowable in the Privacy Notice. The Privacy Notice must be posted at each intake desk (or comparable location) and on the CHO’s public website.

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

This Policy applies to any CHO that records, uses, or processes personally identifiable information (PII) for the CA-502 CoC HMIS, with the exception of HIPAA covered entities as noted below. 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 required to comply with HIPAA and is not required to comply with the security standards in 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’s privacy standards 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 CHO to comply with or reconcile two sets of rules would be an unreasonable burden.

It is possible that part of a CHO’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 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 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 an electronic device that contains CA-502 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.
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 CHO.

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 must be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations must 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 must log off the data entry system and shut down the computer. A laptop should never be left unattended and should be secured with a lock when used.

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 in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors or equivalent modern 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 must 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:

- 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 must 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, 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.