HMIS Oversight Committee Meeting
Agenda
March 9, 2022
9:00 a.m. – 11:00 a.m.

Join Zoom Meeting
Phone: 669 900 6833
Meeting ID: 871 7289 8029

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

1. Welcome (Mike Keller) 9:00 – 9:05
2. Approval of Meeting Minutes, 2/9/22 (Mike Keller) 9:05 – 9:10
   Action Item
3. HMIS Oversight Public Comment (Mike Keller) 9:10 – 9:15
4. Privacy and Security Policies (Jessica Hanserd) 9:15 – 9:40
   Action Item
   a. Point-in-Time Count (HIC/PIT)
   b. Occupancy Report
   c. HMIS Staffing Updates
   d. System performance measure issues in Clarity
7. New Agency Onboarding (HCD) 10:25 - 10:35
8. System Performance Measure Presentation FFY 21 (Katie) 10:35 – 10:55
Proposed items for April 13 meeting (Mike Keller) 10:55 – 11:00
   • Update HIC/PIT Data Submission
   • Update on Coordinated Entry 2.0
   • Review/update Agency Liaison Role
   • SHIE/CHR Discussion
   • Agency Onboarding Materials
     o Types of requests
HMIS Oversight Committee Minutes
February 9, 2022
9:00 a.m. – 11:00 a.m.

Attendees: Patrick Crosby (Alameda County Housing and Community Development), Riley Wilkerson (Alameda County Housing and Community Development), John Noe (Alameda County Housing and Community Development), Jonathan Russell (Bay Area Community Services), Nic Ming (Social Impact Wheel), Mike Keller (East Oakland Community Project), Dorcas Chang (EveryOne Home), Katie Haverly (EveryOne Home), Chelsea Andrews (EveryOne Home), Suzanne Warner (Office of Homeless Care and Coordination), Josh Jacobs (City of Berkeley), Tunisia Owens (Family Violence Law Center)

1. Welcome (Mike Keller) 9:00 – 9:05
   • Mike Keller (EOCP) announced that Tirza White is currently out on leave and that Chelsea Andrews and Katie Haverly will be filling in for Tirza.

2. Approval of Meeting Minutes, 1/12/22 9:05 – 9:10
   Action Item
   • Mike Keller (EOCP) made a motion to approve the meeting minutes.
   • 4 members approved. 0 Abstained. 0 opposed.
   • Motion passed.

3. HMIS Oversight Public Comment 9:10 – 9:15
   • No public comments

   • Chelsea Andrews (Executive Director) shared that data quality should be a standing monthly item. HMIS Committee should develop the workplan accordingly, to incorporate high level priorities agreed upon by HUD CoC Committee.
   • The last HUD CoC meeting did not have a presentation on the Longitudinal System Analysis (LSA) or Point In Time (PIT) Count but they are on the agenda for the next meeting.
   • Mike Keller (EOCP) made motion to approve work plan.
     o The committee discussed approving the workplan.
     • Some members expressed concern about approving a workplan that still needs to be adjusted.
     • Chelsea Andrews (Executive Director) responded that the approval of HUD CoC happened with the understanding that the workplan can be modified. She is concerned that delaying means that there is no course of action to follow and suggested a caveat with the motion.
     • Mike Keller (EOCP) shared that the committee is trying to approve the work
plan that can be modified and would be helpful to have a caveat.

- Nic Ming (Social Action Wheel) shared that the caveat could include feedback from the workgroup and the HMIS Lead.
- Riley Wilkerson (HCD) emphasized the importance of setting up expectations that as it currently stands the workplan can’t be met.
  - Jonathan Russell (BACS) seconded the motion to approve the work plan with the caveat.
  - Motion passed.
- Mike Keller (EOCP) shared that creating a monthly 2 hour workgroup would be helpful to accomplish as much of the workplan as possible. A doodle poll was sent out to the committee.
  - The data quality action plan and the HMIS lead monitoring would be the first two topics.
  - Nic Ming (Social Action Wheel) shared that there may be some revisions to the workplan that the workgroup could continue to evaluate.
  - Nic Ming (Social Action Wheel) asked why the HUD CoC Committee would need to be apprised of the data quality action plan in February.
    - Chelsea Andrews (Executive Director) shared that it may have been similar to the timeline from the year before. If there is a recommendation to hold until March from this committee, Chelsea Andrews could share with HUD CoC Committee.
    - Nic Ming (Social Action Wheel) recommended going to the HUD CoC Committee in March for this.
  - Based on the doodle, the times for the standing workgroup would be the first Thursday of the month from March 3rd either from 1pm to 3pm or 2pm to 4pm.
  - Nic Ming (Social Action Wheel) asked whether other committee members could sit on the workgroup to support the efforts of the committee.
    - Chelsea Andrews (Executive Director) recommended that other committee members be in the workgroup but that other committee members be invited in as guests.

The committee will review the work plan in April or May.

5. **Data Quality Action Plan** (John Noe & Nic Ming) 9:35 – 10:05

- Nic Ming (Social Action Wheel) shared that the 2020 action plan was agreed to be outdated, and the data quality action plan needs to be revised. They spoke of the funder data liaison role supporting the monitoring of programs and data quality. They shared two documents regarding the proposed role of the funder data liaison (see google doc links below).

  - [HMIS Funders (Data) Liaison Role](#)
  - [HMIS Funders (Data) Liaison Outline](#)

- Patrick Crosby (HCD) commented that the HMIS lead could potentially provide the toolset and let the agencies know how to manage and improve their data quality, but the impact of not doing that needs to rest in the CoC. He shared that the HMIS lead should have a role, but the responsibility should not rest with the HMIS lead.
- Suzanne Warner (OHCC) shared that they have in a lot of situations where there are multiple funders for the same program. Going back to roles and responsibilities with
individual agencies needs to be taken into account.

- Chelsea Andrews (Executive Director) asked how contract management takes place for HUD CoC recipients and what the role of the collaborative applicant is.

- Jonathan Russell (BACS) commented that it would be helpful to have by program/service type expanded and more robust data quality and outcomes built into contracts and there has to be expanded expectation in contracts.

- Nic Ming (Social Action Wheel) shared that the funder liaison can help with ensuring accountability as they will be a new stakeholder handling the engagement with the agencies which can expand how contracts get represented.

- Jonathan Russell (BACS) suggested that it would be helpful if there was a typology for different kind of contracts to make it easier to liaison. He also mentioned that there are also natural liaisons that would be natural fits for this role.

- Natasha Paddock (HCD) asked how the funder liaison role would roll out and how does it connect back to the HMIS Oversight Committee? Is this role someone who will seek out info from funders, compile that, and do analysis so we understand the data that needs to be targeted?
  - Nic Ming (Social Action Wheel) responded that this could function collectively and that perhaps HMIS Oversight monthly meetings could have an agenda item for this. The roll out start can happen from having conversations with the HMIS workgroup and have conversations and get feedback from funders.

- Natasha Paddock (HCD) commented there must be topical level of analysis and feedback to all the funders. This group can help set the tone and facilitate the messaging and set expectations for the level and quality of data.

- Jonathan Russel (BACS) shared that he liked how it provides an accountability channel that we have not had. These funder’s liaison needs to be trained up on what those expectation is from the HMIS lead.
  - Mike Keller (EOCP) shared that his understanding of the data quality/liaison meeting could be space for training.
  - Jonathan Russell (BACS) clarified that the training would be help alleviate future burden from the HMIS Lead if the liaison knows the basics and had a robust understanding to hold accountability.

- Riley Wilkerson (HCD) added that we need to define what we mean by data quality and set up standards. He believes that the working group will be looking at the scope of what our data quality path is going to look like.

- **Mike Keller (EOCP) led a motion to explore this concept of a funder liaison and the data quality action plan in the workgroup and bring back to the committee. Josh Jacob seconded.**
  - 5 Approved. 0 Abstained. 0 Opposed.
  - **Motion Passed**

- John Noe (HCD) reviewed the items that have been complete or ongoing from the current data quality action plan from 2020.
  - John Noe (HCD) will send the updated document for the committee for review.
  - Nic Ming (Social Action Wheel) asked if there are any areas or items that seem missing that need to be represented moving forward in the data action plan?
    - Patrick Crobsy (HCD) shared that one area that needs focus on is where in the CoC is the responsibility going to lie for compliance. Questions he posed include: what is going to be the response for poor data quality, who will reach out to the agencies, the CoC or the Oversight Committee?
    - John Noe (HCD) agreed that there needs to be a more effective way to
approach compliance and doesn’t want the current way that to carry over into the funder liaison role.

- Mike Keller (EOCP) shared that one approach for better compliance could be looping the funders into the discussion through the liaison if issues continue to persist.

6. **HMIS Lead Monitoring** (Mike Keller)  
   **10:05 – 10:20**

   - Due to time constraints, this item was skipped and will be explored in a workgroup.

7. **Point-in-Time Count** (Patrick Crosby)  
   **Update**  
   **10:30 – 10:40**

   - Patrick Crosby (HCD) shared communications have been sent out to non-HMIS participating agencies regarding their HIC data. They started sending out data for review for permanent housing projects and rapid rehousing projects to start validating their data.
   - Patrick shared the occupancy report. They are trying to see how the data is trending.
     - In January, occupancy counts are going down. This may be because some agencies are reviewing their occupancy and correcting the data.
     - Providers can see the last two numbers when they run the HIC report in HMIS.
     - Mike Keller (EOCP) shared occupancy could be down because of COVID outbreaks.
   - Nic Ming (Social Action Wheel) asked what are we doing currently with the occupancy data?
     - The data is being shared with the HMIS Oversight committee. The agencies are made aware its being recorded.
   - Natasha Paddock (HCD) asked where is the opportunity for programs to course correct?
     - Nic Ming (Social Action Center) suggested that this report can be included to the monthly meeting to the HMIS liaison so they can review and the meetings can be structured to include conversations about the report.
     - Tunisia Owens (FVLC) suggested taking a sample of agencies that are under their count and reach out to those agencies to get responses for why the data is that way.
     - Chelsea Andrews (Executive Director) shared there could be an opportunity to provide context.
     - Natasha Paddock (HCD) wondered if the funder liaisons could help with this.

8. **Longitudinal Systems Analysis (LSA) Report** (Patrick Crosby)  
   **10:40 – 10:50**

   - Patrick Crosby (HCD) shared they are behind on LSA data. The good news is that they started with 4700 flagged errors and most have been attributed to and worked off by the vendor. Currently 240 errors are flagged and they are worked through figuring out which ones can be fixed.
   - The deadline is next Tuesday.
   - HUD chooses to compare the data to the HIC data. It is not a very comparable set of data because we do not include many projects from the HIC.

**Proposed items for March 9 meeting**  
**10:55 – 11:00**

- System Performance Measures
• HMIS Lead Monitoring
• Privacy & Security Policies
• Data Quality
• PIT Count
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(s) 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(s) 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(s) (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(s) 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(s) 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 CHOs: A list of CA-502 participating CHOs 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.

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; 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

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.

Updated 1/31/21
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 equipment are recommended.

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
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:

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
● 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,

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.
data entry forms, and case / client notes. Note: Many CHO's 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.
Privacy Notice
For organizations in the Oakland-Berkeley-Alameda County Continuum of Care

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

This Privacy Notice summarizes our Privacy Policy. The Privacy Notice and Policy can be found online at www.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.

Why do we collect and share your information?
We collect, use, or share your information to:
• Provide or coordinate services.
• Collect payments.
• Run the organization.
• Create data that can’t identify you.
• Support research.
• Follow local, state, and federal laws.
• Follow court orders, respond to threats, and ensure public safety.

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

What other steps do we take to protect your privacy?
In addition to following local, state, and federal laws, we will:
• Assist you if you need help or translation, as required by law.
• Explain and share this Privacy Notice and the Privacy Policy. This Notice summarizes the Policy.
• Only collect the information we need.
• Have a plan for keeping information in good order and deleting old data.
• Share the least amount of information needed to complete a task.
• Allow you to review and correct your information, and explain if your request is denied.
• Have a plan and train staff to handle questions, complaints, or a data breach.

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

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

Updated 2/17/22
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.
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 CHO.

- **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.
CA-502 Standard Privacy Policy

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.

- **Information Sharing Authorization (ISA-H):** 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]

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org .

Updated 03/04/22
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.

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.

Updated 03/04/22
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

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.

Updated 03/04/22
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

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.

Updated 03/04/22
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

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.

Updated 03/04/22
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 Information Sharing Authorization (ISA-H) 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

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.

Updated 03/04/22
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.

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.

Updated 03/04/22
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

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.

Updated 03/04/22
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.

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.

Updated 03/04/22
[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

Please send any questions, concerns, or other feedback to jessica@hanserdhealth.com and SWarner@acgov.org.

Updated 03/04/22
Scorecard Evolution and Changes

- RBA Committee has created a new and updated proposed scorecard that
  - Includes 13 indicators **disaggregated by race/ethnicity** including ALL system performance measures
- Includes **other data sources** including 211 and census data
- Includes indicators to **monitor the new coordinated entry system**
- Includes indicators to **monitor HMIS performance**
- Presentation of new scorecard and data to be given in **February** to HUD CoC for review and approval
HUD System Performance Measures

• **6 key performance measures** that every Continuum of Care (CoC) reports to HUD annually as part of the CoC funding competition.

• **Standard Measures**: defined by the US Dept of Housing and Urban Development (HUD) and provided to Homeless Management Information System (HMIS) vendors so that each CoC measures performance identically across the country.

• **Creates a common language** for talking about outcomes and performance.
For more information about the measures and their calculation, see System Performance Measures, An Introductory Guide.
6 System Performance Measures

1. Number of Persons Homeless
2. First Time Homelessness
3. Length of Time Homelessness
4. Exits to Permanent Housing
5. Returns to Homelessness
6. Employment & Income Growth
1. **Number of Homeless Persons**

**What does it measure?**
- Change in the number of sheltered homeless people in HMIS each year (HMIS, annual)
- Change in the number of unsheltered homeless people (PIT Count, biennial)

**How does it measure?**
- Provides an unduplicated count of people who stayed in Emergency Shelter, Safe Haven, and Transitional Housing programs over the course of the year.

**What do we want to see?**
- Reductions in the number of people who are homeless within a comprehensive HMIS.
- Right now, we may want to see an increase in unduplicated individuals served by shelters as a sign of system flow to permanent housing.
Unduplicated Annual Count of Sheltered Homeless Persons in HMIS

- **Unduplicated Total Sheltered Homeless Persons in HMIS**
- **Emergency Shelter**
- **Safe Haven**
- **Transitional Housing**

**FFY 2016**
- Unduplicated Total: 3547
- Emergency Shelter: 1570
- Safe Haven: 0
- Transitional Housing: 0

**FFY 2017**
- Unduplicated Total: 3481
- Emergency Shelter: 1370
- Safe Haven: 4
- Transitional Housing: 0

**FFY 2018**
- Unduplicated Total: 2963
- Emergency Shelter: 1121
- Safe Haven: 56
- Transitional Housing: 0

**FFY 2019**
- Unduplicated Total: 4034
- Emergency Shelter: 1075
- Safe Haven: 55
- Transitional Housing: 0

**FFY 2020**
- Unduplicated Total: 5377
- Emergency Shelter: 1042
- Safe Haven: 96
- Transitional Housing: 0

**FFY 2021**
- Unduplicated Total: 5052
- Emergency Shelter: 929
- Safe Haven: 61
- Transitional Housing: 0

*EveryOneHome*
2. **First Time Homelessness**

**What does it measure?**

- How many people became homeless for the first time during the reporting period.

**How does it measure?**

- Counts the number of people who entered Emergency Shelter, Transitional Housing, Rapid Re-Housing, and Permanent Supportive Housing programs during the year and subtracts those with a project entry within the prior 24 months.

**What do we want to see?**

- Decreasing number of people becoming homeless for the first time
First Time Homelessness

- Emergency Shelter/ Safe Haven/ Transitonal Housing/ Permanent Housing Programs - 1st Time Homeless

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1,134</td>
<td>2,688</td>
<td>2,979</td>
<td>2,245</td>
<td>3,622</td>
<td>3,733</td>
<td>2,900</td>
</tr>
</tbody>
</table>

FFY = Fiscal Year
3. **Length of Time Homeless**

**What does it measure?**

- **Measure 1a**: How effective is our system in ending homelessness?
- **Measure 1b**: How long are people experiencing homelessness?

**How does it measure?**

- **Measure 1a**: Length of time from first *Emergency Shelter, Safe Haven, or Transitional Housing* enrollment to housing move in.
- **Measure 1b**: Length of time from self-described start of homelessness to housing move in.

**What do we want to see?**

- Shorter is better: Reduction in the average and median length of time homeless.
- Also desirable: average and median are the same.
Length of Time Homeless – Average # of Nights

- FFY 2015: 170
- FFY 2016: 186
- FFY 2017: 170
- FFY 2018: 208
- FFY 2019: 196
- FFY 2020: 204
- FFY 2021: 237

Emergency Shelter/ Safe Haven/ Transitional Housing - Average # Nights in Program
What does it measure?

• Whether our interventions are effective and long-lasting in ending homelessness

How does it measure?

• Follows people who exited to permanent housing during the FY two years previous and counts the number of people who reappear in HMIS in the subsequent 2 years.

• Provides data on returns to homelessness at less than 6 months, 6-12 months, 13-24 months, and total in 2 years

What do we want to see?

• Reduce returns to homelessness.

• Identify when households are vulnerable to returning to homelessness post-housing
# of Persons who Exit to Permanent Housing

Destinations that Return to Homelessness in 2 Years

<table>
<thead>
<tr>
<th>Year</th>
<th># of Returns to Homelessness in 2 Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>FFY 2015</td>
<td>373</td>
</tr>
<tr>
<td>FFY 2016</td>
<td>433</td>
</tr>
<tr>
<td>FFY 2017</td>
<td>433</td>
</tr>
<tr>
<td>FFY 2018</td>
<td>311</td>
</tr>
<tr>
<td>FFY 2019</td>
<td>312</td>
</tr>
<tr>
<td>FFY 2020</td>
<td>352</td>
</tr>
<tr>
<td>FFY 2021</td>
<td>432</td>
</tr>
</tbody>
</table>
Measure 1a: How effective is our system in ending homelessness?

Measure 1b: How long are people experiencing homelessness?

Extent to which Persons who Exit to Permanent Housing Return to Homelessness in 2 Years

<table>
<thead>
<tr>
<th>Year</th>
<th>% Returning to Homelessness in 2 Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>FFY 2015</td>
<td>19.0%</td>
</tr>
<tr>
<td>FFY 2016</td>
<td>18.0%</td>
</tr>
<tr>
<td>FFY 2017</td>
<td>18.7%</td>
</tr>
<tr>
<td>FFY 2018</td>
<td>15.2%</td>
</tr>
<tr>
<td>FFY 2019</td>
<td>17.6%</td>
</tr>
<tr>
<td>FFY 2020</td>
<td>17.7%</td>
</tr>
<tr>
<td>FFY 2021</td>
<td>18.0%</td>
</tr>
</tbody>
</table>

FFY = Federal Fiscal Year
5: Exits to or Retention of Permanent Housing

What does it measure?

- How many people achieved a positive housing outcome:
  - Street Outreach: moved indoors
  - Emergency Shelter, Safe Haven, Transitional Housing, Rapid Re-Housing exited our system to permanent housing
  - Permanent Supportive Housing retained permanent housing.

How does it measure?

- Counts people with successful housing outcomes and divides by total exits:
  - Street Outreach: exits to temporary housing and permanent housing destinations (excludes temporary homeless destinations)
  - Emergency Shelter, Safe Haven, Transitional, and Rapid Re-Housing: Permanent housing destinations
  - Permanent Supportive Housing: retention and exits to other permanent housing destinations

What do we want to see?

- Increasing the proportion of people who move indoors from street outreach, exit to permanent housing, or retain permanent housing
# Successful Exits to Permanent Housing from ES, SH, TH, and RRH

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>FFY 2015</td>
<td>1,663</td>
</tr>
<tr>
<td>FFY 2016</td>
<td>1,418</td>
</tr>
<tr>
<td>FFY 2017</td>
<td>1,389</td>
</tr>
<tr>
<td>FFY 2018</td>
<td>1,279</td>
</tr>
<tr>
<td>FFY 2019</td>
<td>1,344</td>
</tr>
<tr>
<td>FFY 2020</td>
<td>1,323</td>
</tr>
<tr>
<td>FFY 2021</td>
<td>1,198</td>
</tr>
</tbody>
</table>
% Successful Exits to Permanent Housing from ES, SH, TH, and RRH

- FFY 2015: 47.7%
- FFY 2016: 46.7%
- FFY 2017: 46.2%
- FFY 2018: 52.1%
- FFY 2019: 53.8%
- FFY 2020: 37.1%
- FFY 2021: 44.6%

% successful exits to permanent housing from Safe Haven, Emergency Shelter, Transitional Housing and Rapid Rehousing
Measure 1: Length of Time Homeless

What does it measure?

• Changes in cash income for adult system stayers and leavers.

How does it measure?

• Compares earned income and cash benefits at program entry, annual update, and exit assessment for adults in Safe Haven, Emergency Shelter, Transitional Housing, Rapid Re-Housing, and Permanent Supportive Housing projects.

What do we want to see?

• A growing percentage of adults who gain or increase employment or non-employment cash income over time.
Adults with Increased Total Income

**STAYERS** = Those that are still enrolled in any project type in HMIS and that have had an annual assessment

**LEAVERS** = Those that have exited the system

<table>
<thead>
<tr>
<th>Year</th>
<th>Adult Stayers with Increased Total Income</th>
<th>Adult Leavers with Increased Total Income</th>
</tr>
</thead>
<tbody>
<tr>
<td>FFY 2015</td>
<td>17.9%</td>
<td>37.7%</td>
</tr>
<tr>
<td>FFY 2016</td>
<td>18.7%</td>
<td>38.1%</td>
</tr>
<tr>
<td>FFY 2017</td>
<td>27.3%</td>
<td>33.1%</td>
</tr>
<tr>
<td>FFY 2018</td>
<td>24.9%</td>
<td>32.8%</td>
</tr>
<tr>
<td>FFY 2019</td>
<td>22.5%</td>
<td>28.0%</td>
</tr>
<tr>
<td>FFY 2020</td>
<td>22.7%</td>
<td>25.0%</td>
</tr>
<tr>
<td>FFY 2021</td>
<td>24.1%</td>
<td>24.4%</td>
</tr>
</tbody>
</table>

EveryOneHome
Summary of Findings

• *First time homelessness* has **decreased by 22%** since FFY 2020.

• *Average length of time homeless* in ES, SH, TH programs has **increased by 16%** since FFY 2020.

• *Returns to homelessness* has hovered around 18% for the last 3 years.

  • Those that identify as Multi-Racial, African American, Native American, and Native Hawaiian/Pacific Islander have disproportionately higher rates of returns to homelessness.
Summary of Findings

• Successful exits to PH from ES, SH, TH, and RRH projects has increased by 7.5% since last FFY

• Since FFY 2020, for system leavers/exiters there has been a 1.4% increase in total income and for system stayers there has been a slight decrease income (0.6%)