Oakland, Berkeley/Alameda County Continuum of Care

CA-502

Homeless Management Information System

Policies and Procedures Manual

Updated 2025

Summary:

A Continuum of Care (CoC) is a regional or local planning body that coordinates housing and services funding for homeless families and individuals. All CoCs are responsible for the oversight and operation of a Homeless Management Information System (HMIS), which is 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. The HMIS operates as a shared system among participating Covered Homeless Organizations (CHOs) to view client-level data.

Sharing HMIS data enhances care coordination, while facilitating reimbursement for services, homeless system planning, and improved public knowledge of homelessness. The HMIS 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 supports a more effective and efficient service delivery system.

Each CHO that participates in the Oakland–Berkeley–Alameda County Continuum of Care (CA-502) must decide to adopt the following standard documents in whole, or adapt them to include stricter protections as necessary:

- Security Policy
- Privacy Policy
- Privacy Notice
- Procedure Manual

Note: CHOs that are HIPAA-covered entities will use HIPAA-oriented versions of the documents above.

Any CHO that participates in CA-502 should use its forms in whole, without any changes. This includes the CA-502 Release of Information. The exception is that HIPAA-covered entities may use an alternate consent form.

- Release of Information (consent) form and Release of Information Revocation form
- Grievance Form
- Staff Attestation Form

Definitions

- **Client:** A living individual about whom a covered homeless organization collects or maintains protected personal information: (1) because the individual is receiving, has received, may receive, or has inquired about services: or (2) to identify service needs, or to plan or develop appropriate services within the CoC.

- **Continuum of Care (CoC):** The group organized to carry out the responsibilities prescribed in the CoC Program Interim Rule[1] for a defined geographic area. A CoC should be composed of representatives of organizations that include nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve homeless and formerly homeless veterans, and homeless and formerly homeless persons.

- **Covered Homeless Organization (CHO):** Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, discloses, or processes the personally identifiable information (PII) of clients at-risk of or experiencing homelessness. This definition includes both organizations that have direct access to the HMIS, as well as those formal partnering organizations that do not access the HMIS but do record, use, or process PII of target population clients. A list of CA-502 participating CHOs can be found at AC HMIS ROI Providers.

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

- **HIPAA-Covered Entities:** (1) Health care providers that transmit any patient information in an electronic form, including doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies. (2) Health plans, including insurance companies, HMOs, employer health plans. (3) Government programs such as Medicare, Medicaid, and the military and veterans' health care programs.

- **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. CA-502 uses Clarity Human Services by Bitfocus for its HMIS software.

[1] See https://www.govinfo.gov/content/pkg/FR-2012-07-31/pdf/2012-17546.pdf

- **HMIS Lead Agency:** An agency designated by a CoC to operate the CoC's HMIS on its behalf. Employees of the HMIS Lead Agency who support the participating CHOs by serving as an initial point of contact, providing technical assistance, coordinating with the HMIS vendor, maintaining process integrity, and overseeing the HMIS to ensure security and reliability.

- **HMIS Committee:** The CoC-designated subcommittee tasked with HMIS oversight. The HMIS Committee is actively involved in establishing and enforcing HMIS policies and procedures along with furthering the goals of the CoC. The committee is made up of CoC representatives, the HMIS Lead, health and services staff, jurisdictional staff, and one member from a CHO. The HMIS Committee acts as liaison between the HUD CoC Committee and the HMIS Lead Agency.

- **Release of Information (ROI):** This is a consent form used for housing and homeless services that allows for the client's PII to be shared with CHOs and other providers that assist clients. This form is required for any use or disclosure that is not listed in the CHO's privacy notice. Some organizations may require that this form be collected on all clients.

- **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. 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
  - Login details
  - Personnel number
  - Vehicle identifier or serial number
  - Photograph or video identifying an individual
  - Biometric information
  - Medical information
  - Criminal history
  - Other information that may directly or indirectly identify that individual (e.g., salary, performance rating, purchase history, call history, etc.)

- **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 allowable uses and disclosures.

- **Process:** Any operation or set of operations performed on PII, 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.

Roles and Responsibilities

HMIS User: An employee, volunteer, affiliate, associate, and any other individual acting on behalf of a CHO, who uses or enters data into HMIS. They must:

- Comply with federal regulations regarding HMIS.
- Comply with federal, state, and local laws that require additional privacy or confidentiality protections.
- Complete training as required.
- Understand and be able to explain their CHO's Privacy Notice.
- Follow their CHO's Privacy Notice and know where to refer clients if they cannot answer a client's question.
- Present their CHO's Privacy Notice to the client before collecting any information; and uphold the client's privacy in HMIS.
- Provide data entry in a manner that follows the CoC approved Data Quality Action Plan.[2]
- Uphold the client's information security and confidentiality in HMIS.
- Report security incidents and follow the Privacy and Security Breach procedure.

HMIS Liaison: An employee of the CHO designated to be a liaison to the HMIS Lead Agency. The following are liaison responsibilities:

- Helping the agency complete the HMIS onboarding process.
- Ensuring agreements are executed and files maintained (Partner MOU Agreement and HMIS Privacy and User Agreements).

- Onboarding new HMIS Users and providing one-on-one support as needed.
- Setting up and monitoring password screensavers.
- Ensuring staff complete required training and adhere to the governing principles, policies, and procedures of the HMIS system.
- Ensuring that staff are using an informed consent process and that the ROI and, if applicable, Information-Sharing Authorization (ISA) forms are uploaded to the HMIS and Community Health Record[3] in a timely manner.
- Performing initial and annual audits using the HMIS Network Security form, and HMIS Workstation Security form.
- Ensuring system software updates are maintained on workstations.
- Maintaining and updating firewall and virus protection on the CHO's network and workstations.
- Working with the HMIS Lead on unresolved software issues.
- Working with the HMIS Lead when the CHO requests administrative system changes.
- Running Provider Reports.
- Auditing User Reports.
- Responding to end-user system questions.
- Ensuring that the CHO does not exceed its allotted number of user licenses.
- Delegating and overseeing technical support and other tasks as needed.
- Responding to requests from the HMIS Lead
- Representing the CHO at HMIS user meetings, bringing ideas, concerns, and issues to facilitate system improvements.

HMIS Lead: Roles and responsibilities include:

- Supporting the HMIS by providing ongoing funding.
- Providing staff for the HMIS.
- Overseeing the day-to-day operation of the HMIS.
- Adopting written policies and procedures for the operation of the HMIS that apply to the HMIS Lead, its CHOs, and the CoC.
- Ensuring policies and procedures comply with all applicable Federal law and regulations, and applicable state or local governmental requirements.
- Responding to HMIS Committee advisement.
- Preparing and facilitating monthly user meetings. Ensuring participation across all CHOs within the CoC.

[3] The Community Health Record (CHR) is a web-based software tool that allows qualified health care providers to access aggregated patient records from multiple hospitals and medical labs throughout a community.

- Soliciting HMIS User feedback.
- Coordinating CHO onboarding.
- Coordinating HMIS notifications and system upgrades (in partnership with the vendor).
- Performing initial CHO setup and HMIS configuration.
- Conducting security inspections to ensure that new CHO partners meet HMIS security standards.
- Administering and managing HMIS User accounts, logins, and passwords for local CHO administrators.
- Maintaining and updating training modules (Privacy and Security, HMIS user training).
- Providing technical assistance within the continuum, troubleshooting and resolving problems.
- Performing data quality review on an ongoing basis.
- Reviewing and monitoring participating CHOs to ensure security, confidentiality, and quality of the information within the system and adherence to standard policy and procedures.
- Creating and running all required custom and collaborative reports.
- Serving as liaison with the system software vendor to resolve technical issues**.**
- Monitoring the number of agencies, HMIS Liaison/manager, and user licenses assigned and ensuring that the number of each is increased as needed.
- Notifying the HMIS Liaison of all system upgrades or notifications.
- Actively participating in CoC Committees related to HMIS data quality/updates.
- Coordinating and submitting Housing Inventory Chart (HIC), Longitudinal Systems Analysis (LSA), Annual Homeless Assessment Reports (AHAR).
- Uploading HMIS data to the state Homeless Data Integration System (HDIS).

The HMIS Committee: The following are the Committee responsibilities:

- Making all final decisions on planning, participation, and coordination of HMIS/data resources.
- Developing CoC policies governing use of the HMIS, in compliance with federal regulations.
- Making recommendations on the HMIS software application/vendor as needed.
- Supporting and protecting the rights and privacy of clients.
- Supporting and protecting the rights and privacy of service users.
- Reviewing privacy and security breaches, if escalated.
- Developing community-wide outcomes, measures, and goals.
- Reviewing data quality reports and recommending a quality improvement program for adoption by the CoC.

- Taking appropriate action to ensure accountability and improved performance as described in the quality improvement program.
- Ensuring compliance with federal requirements.
- Collaborating with the HMIS Lead Agency on all policies it is required to develop including Privacy, Security, and Data Quality Plans as required by federal regulation.
- Creating an annual HMIS Work Plan and using it to annually review HMIS performance and functionality.
- Monitoring the HMIS Lead Agency.

1. Onboarding and Implementation

1.1 CHO Partner Participation Agreement

The Participation Agreement is a signed memorandum of understanding (MOU) between a CHO and the CoC specifying the terms of CHO participation in the HMIS, including meeting technology and security requirements for the HMIS and data-sharing.

Procedure:

1. The **CHO Executive Director** or department head will request to participate in the HMIS using hmissupport@achmis.org. The **HMIS Lead** will direct them to complete the Agency Onboarding Questionnaire.[4]

2. The **HMIS Lead** will review the Questionnaire, and once any issues are resolved and the HMIS Committee approves, send out the HMIS Partner MOU via DocuSign.

3. The **CHO Executive Director** or department head, **Alameda County HMIS Lead** will sign the electronic agreement via DocuSign.

4. The onboarding process includes completing the tasks on the Agency/Jurisdiction Implementation Readiness Checklist.[5] In addition, **staff of the new CHO** will submit a Provider Assessment Form[6] for each program that will serve clients to be included in the HMIS.

---

[4] Found at Alameda: Agency Management (bitfocus.com)

[5] Found at Alameda: Agency Management (bitfocus.com)

[6] Found at Alameda: Agency Management (bitfocus.com)

1.2 HMIS Technology Requirements

All workstations (e.g., desktops, laptops, tablets) authorized to access the HMIS on behalf of a CHO must meet the following minimum requirements:

- Computer: 500 MHz, higher PC or MAC
- Web Browser: Apple Safari, Google Chrome, Microsoft Edge, Microsoft Internet Explorer 11, or Mozilla Firefox
- Hard Drive: 6 GB
- 128 MB RAM
- A supported version of an operating system (e.g., Windows 10, Windows 11, or Mac O/S 10.3 or higher)
- Anti-virus software and an active firewall
- Secure internet connection: Each computer should have access to at least a DSL/Broadband high-speed line. No dial up.
- SVGA monitor with 800x600+ resolution
- Keyboard and Mouse

1.3 Security Inspection

The network and each workstation used to access the HMIS and/or PII must pass a security inspection prior to use. This applies to all workstations used inside and outside an office environment, including those workstations approved for remote access. The HMIS Lead Team will follow the Security Inspection and Annual Review procedure (see Chapter 7, below).

1.4 HMIS User Agreements

HMIS User Agreements are agreements between the HMIS Lead Agency and individual CHOs employees, contractors, or volunteers who are authorized to collect or use data in the HMIS. These include 1) the Privacy Agreement, which acknowledges the user's commitment to protect clients' confidentiality; and 2) the User Agreement, in which users formally adopt the HMIS policy, responsibilities and code of ethics.

Procedure:

1. The **CHO's HMIS Liaison** will, in consultation with agency managers, determine which staff members need privacy and software training, direct staff to Alameda: Agency Management (bitfocus.com) and inform the HMIS Lead agency (via

hmissupport@achmis.org) bitfocus help desk when they have completed training and are ready for software licensing.

2. The **HMIS User** will sign the electronic agreements at time of the fist login, and annually thereafter.

2. User Training and Support

2.1 User Training

Prior to being issued an HMIS license and/or accessing any PII, staff and volunteers need to complete the HMIS Basics and Privacy and Security training. The Privacy/ Security course needs to be repeated annually. In addition, staff who will become HMIS users will also need to complete the HMIS Software User Training before gaining access to that system.

Staff who have not accessed the HMIS for 90 days will be locked out of the system and must repeat both the Privacy/Security and Software courses before their accounts will be reactivated.

Procedure:

1. **CHO Employees** will enroll in the required training(s) at **https://training.bitfocus.com/page/alameda**
    a. If they successfully complete training, they will proceed to step 3.
    b. Students who fail a quiz may repeat until successfully completed
2. Students will notify their agency's HMIS Liaison when they complete training
3. **HMIS Agency Liaisons** notify the Bitfocus Help Desk Team when a student successfully completes training. alameda@bitfocus.com

The **Bitfocus Help Desk Team** confirms that students have completed the required training. Help desk will create the account and will notify the liaison and user with the credentials. The HMIS user agreement will be signed at the time of the first login for all new users. The signing of the user agreements will have to be completed on an annual basis.

2.2 CHO or HMIS User Support

All requests for technical assistance and HMIS User support related to training shall be submitted to the HMIS Lead by an agency's HMIS Liaison. Users may submit requests for help directly to the HMIS Lead for password support and other issues.

Procedure:

1. **HMIS Users** who need help with issues related to training should contact their agency's **HMIS Liaison**. This allows the Liaison to keep track of staff training process, resolve requests if possible, and identify areas outside of training in which users may need support. Once users finish training, the HMIS Liaison emails hmissupport@achmis.org to ask the **HMIS Lead** to create an HMIS account for the individual.

3. After they complete training, **HMIS users** may contact the **HMIS Lead** directly via hmissupport@achmis.org for assistance but should copy the Liaison on those emails.

4. **HMIS Users** who need access to Coordinated Entry (CE) must submit their request to their agency's HMIS Liaison, who will pass the request on to the **HMIS Lead** and the CE Manager. Once the CE Manager approves, the Team will add CE access to the user's HMIS account.

5. The **HMIS Lead** reviews user requests, addresses the issue, or requests further information if needed. The Team includes the agency's **HMIS Liaison** in the email exchange.

2.3 Electronic Customer Portal Access

Electronic Customer Portal Access "The Customer Portal" is software that connects clients to Alameda County HMIS. Authorized clients may access a portion of their HMIS Record through the Customer Portal.

Procedure:

1. **Identity Verification**: Prior to sending a portal invitation, the client's identity and contact information will be verified by the Partner Agency. Clients will be required to share their full date of birth in HMIS prior to accessing the portal. To verify client identity, agencies should ask for the individual's full name and confirm two identifying pieces of information. Identifying information may include date of birth, contact phone number or address, social security numbers, photo, recent service history, HMIS ID number, or other individualized information in

the client record. Agency staff will verify that the client's email listed on the Contact tab in Clarity matches the Email registered to the portal account.

2. **Authorized Access:** Only the individual identified in the client record is authorized to access the Customer Portal account. Individuals must be aged 18 or older to access the Customer Portal. If the Customer Portal account is accessed by any unauthorized individual, the account should be immediately deactivated. Accounts may be reinstated once the client identity and credentials are verified. An authorized individual may request to have their portal account deactivated at any time.

3. **Portal Information and Communication:** Partner Agency Staff will respond to direct messages, requests, and information sent through the Customer Portal in a timely manner. Partner agency staff will review, and update information entered through the portal to ensure an accurate and complete client record. Information entered through the Portal is identified in Clarity with a portal icon.

3. Privacy Standards

The CoC's privacy standards protect the privacy of personal information collected and stored in the HMIS and elsewhere in print or electronic formats within the continuum.

3.1 Privacy Policy, Privacy Notice & Sign

The HMIS Privacy Policy describes the protections for keeping PII confidential while allowing for reasonable, responsible, and limited uses and disclosures of data (see Appendix B). The Privacy Notice is a consumer-friendly summary of the Privacy Policy that is meant to be easy for clients to understand and act upon. The Privacy

Notice will be sufficient for most clients however; they can request a copy of the Privacy Policy as well. Copies of the Privacy Notice and Privacy Policy should be available for distribution upon request. Clients may also access the CoC's standard Privacy Notice, the standard Privacy Policy, and a list of participating CHOs at AC HMIS ROI Providers.

Procedure:

1. **CHO Agencies** that adopt the CoC's standard Privacy Notice are encouraged to display it as a sign. CHOs that use a non-standard Privacy Notice, have at least two choices:
    a. Display the CHO's unique one-page Privacy Notice as the sign. This is recommended for CHOs that make slight adaptations to the CA-502 standard Privacy Notice.
    b. Display a sign with the following alternative HUD language:

    We collect personal information directly from you for reasons that are discussed in our privacy notice. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.[7]

2. In either case, **CHOs** must ensure that copies of the Privacy Policy and Privacy Notice are available and provided upon request.

3. **HMIS Users** must ensure that a sign is displayed (at their workstation, desk, or any area where they are collecting and processing PII) that describes how information about the client may be used and disclosed, and how the client can get access to their information. In addition to English, Privacy Policy information will be available in Spanish and other languages used by clients that the CHO serves.

Best Practice:

Participating CHOs should post the Privacy Notice/ Sign in all locations where intake occurs. In an office setting, this might include a waiting room, an intake line, or another area where clients congregate before intake occurs.

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

For the mobile workforce, the Privacy Notice/ Sign can be taped to the back of a clipboard.

3.2 Assumed Consent

Client consent is assumed when all of the following take place: 1) CHOs post the Privacy Notice at each intake desk (or comparable location) that explains the reasons for collecting HMIS information, and the uses and disclosures that are allowable; 2) CHO staff discuss the contents of the notice with a client; and 3) the client agrees to provide personal information.

Agencies may follow this Assumed Consent procedure if:

- The use or disclosure is defined as allowable in the CA-502 Privacy Policy, and
- The use or disclosure is listed in their CHO's privacy notice (this may be the same as the CoC's standard Privacy Notice), and
- Their organization instructs them to do so.

If these are not all true, CHOs should follow the Explicit (written) Consent procedure described below. If staff members are unsure, they should consult their agency's HMIS Liaison.

Procedure

The **HMIS User**:

1. Assesses the client's decision-making capacity. If the client is not able to decide, CHO staff should present the information to the client's representative. The topic should not be introduced in a moment of crisis.

2. Asks if the client would like assistance reading the Privacy Notice. If the client prefers to read it on their own, CHO staff should make sure to give them enough time to get through it. If the client prefers a language other than English, staff should use an interpreter.

3. Refers to the Privacy Notice, uses plain language, avoids acronyms or jargon, and addresses any questions clients may have.

4. Checks for understanding and asks, "Was there any information that did not make sense or was confusing?"

5. Asks, "What questions do you have?"

6. Ensures that the client knows that the Privacy Notice and the Privacy Policy and that a list of participating organizations can be found at AC HMIS ROI Providers.
7. If requested, provides printed copies of the Privacy Notice and/or Privacy Policy.
8. Completes a Staff Attestation form confirming they completed these steps and ensures that the form is retained in their organization's records.

3.3 Explicit Consent

If the use or disclosure does not meet the requirements for the Assumed Consent procedure, or an organization wants staff to collect explicit (written) consent, they should follow the Explicit Consent procedure.

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

1.1.1. For any use or disclosure other than what is defined as allowable, and
1.1.2. For any use or disclosure that is not listed in the CHO's privacy notice.

CHOs that are HIPAA-covered entities may use an alternate consent form.

Procedure:

The **HMIS User and/or CHO employee**:

1. Looks in the HMIS to determine if the Release of Information form (ROI) has already been collected. If needed, they contact a team member to check the HMIS system. If not, proceed to step 4.
2. If there is an ROI on file but it is set to expire within the next three months, proceed to step 4.
3. If the ROI is on file and its expiration is beyond 3 months, skip to step 9, below.
4. Assesses the client's decision-making capacity. If the client is not able to decide, CHO staff should present the information to the client's representative. The topic should not be introduced in a moment of crisis.
5. Asks if clients would like assistance reading the ROI form. CHO staff should make sure to give them enough time to get through it. If the client prefers a language other than English, staff should use an interpreter.

6. In referring to the ROI form, uses plain language, avoids acronyms or jargon, and addresses any questions they may have.

7. Checks for understanding and asks, “Was there any information that did not make sense or was confusing?”

8. Asks, “What questions do you have?”

9. Ensures that the client knows that the Privacy Notice and Privacy Policy and the list of participating organizations is AC HMIS ROI Providers.

10. If requested, provides a printed copy of the Privacy Notice, Privacy Policy, and/or the signed ROI.

11. Asks the client to consent to release of information.
    a. If a client chooses not to consent, note “decline” in the HMIS and follow the CHO’s blind process.
    b. If the agency requires explicit written consent, ensures the form is completed, signed, and uploaded into the agency’s internal system. Before uploading, verifies that these four fields are completed.
        1. Client Name
        2. Client Date of Birth
        3. Client signature: wet or digital signature required – verbal consent not accepted
        4. Date of signature
12. Once the paper ROI form has been successfully uploaded, places it in the shred bin. CHO staff store them in a locked container or cabinet, until the forms can be put in the shred bin.

3.4 Updating or Revoking Consent

Clients have the right to update or rescind their consent and levels of data sharing at any time.

Procedure:

The **HMIS User** and/or **CHO employee:**

1. If a client requests to update their consent, informs the client that any changes will take effect as of the date the form is signed, and that any data or information shared before that time cannot be recalled. Follows procedure 6.3 Explicit Consent.

2. If a client requests to revoke their consent to share data for housing purposes, ensures the Release of Information Revocation (ROI-R) form is completed, signed, and stored at the agency. Informs the client that any changes will take effect as of the date the form is signed, and that any data or information shared before that time cannot be recalled.

3. Once the paper forms have been successfully uploaded to the HMIS, places them in the shred bin.

Best Practice:

Upload forms to the HMIS the same day they are received.

3.5 Client Access and Correction

In general, a CHO must allow individuals to inspect and have a copy of any PII about themselves. CHO staff must offer to explain any information that the individual may not understand. A CHO must consider any client's request to correct inaccurate or incomplete PII. 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:

- The information was compiled in reasonable anticipation of litigation or comparable proceedings;
- The information is about another individual (other than a health care provider or CHO);
- The information was obtained under a promise of confidentiality (other than a promise from a health care provider or CHO) and disclosure would reveal the source of the information;
- Disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual; or
- 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.

Procedure:

The **HMIS User** and/or **CHO employee** will:

1. Allow the client to review a printed “hard copy” of their HMIS record within five business days of their request.

2. If needed, will explain any information the client may not understand.

3. The **CHO** will consider all requests for correction of inaccurate or incomplete information pertaining to that client. Staff will make the correction in the HMIS and, if needed, mark the information as inaccurate or incomplete and describe any concerns about context (e.g., confirmed veteran who no longer wants to be recognized as a veteran but would lose veteran benefits if request was granted).

4. The **CHO** will consider any request for inspection of a client’s HMIS record. If denying the inspection, staff will refer to the allowable reasons listed above and document in the HMIS.

5. **CHO staff** will send the client a letter within five business days describing the response to their request. If granting the request for inspection, staff will enclose a printed copy of the HMIS record and ensure the letter is uploaded to the HMIS.

3.6 Client Grievance

Clients have the right to file a grievance based on denial of access, correction of data in the HMIS system, or if the client believes that participation in the HMIS will violate their privacy.

Procedure:

1. Each **CHO** will have its own Grievance Policy and related reporting form, approved by the agency’s **Executive Director**.

2. Upon notification of a complaint or grievance, the **HMIS User** and/or **CHO employee** will instruct the client to complete and sign a Grievance form.

3. **CHO staff** will determine if the grievance relates to an unlawful privacy and/ or security breach. If it does, they will follow the Privacy and/ or Security Breach procedure (see below).

4. The agency’s **Executive Director** will review the form and decide the appropriate follow-up action.

5. The **Executive Director** will follow-up with the client to share the agency’s response within 30 days.

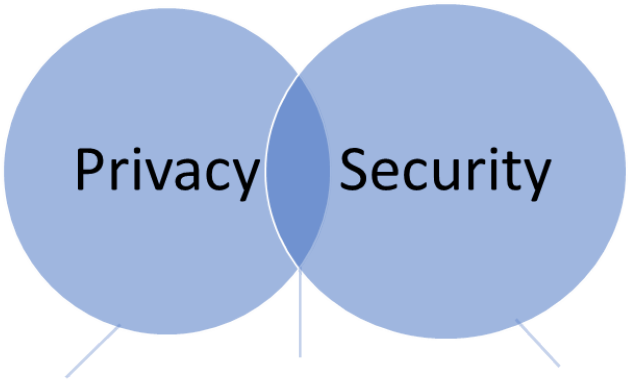
6. **CHO staff** will upload the Grievance form and any related correspondence to the HMIS record.

3.7 Privacy and/or Security Breach

A breach in privacy is an imminent or actual violation of privacy laws, principles, policies, and practices. A breach in security is an actual or imminent violation of computer security policies, acceptable use policies, or standard security practices. Not all privacy incidents are security incidents, and not all security incidents are privacy incidents, but some incidents can be both.

In the event of an unlawful privacy or security breach, CHOs are required to notify the HMIS Lead within three business days. The HMIS Lead will respond within three business days of receiving the notification. The HMIS Lead will provide a written response or corrective action plan, as appropriate. Corrective actions may include notifying the impacted client(s), downgrading a user's system access, or terminating user privileges. The CHO will decide disciplinary actions up to and including termination.

Bitfocus, the vendor of Clarity Human Systems, is responsible for the disaster protection and recovery of the central server, as well as data disposal.



Use or disclosure of PII
- Without providing notice
- Without consent
- For an unauthorized purpose
- Blocking client access to review their PII
- Failure to meet required retention period
- Failure to address correction request or grievance

- Unauthorized access to PII
- Unauthorized disclosure of PII
- Unauthorized or inappropriate modification of PII

- Unauthorized access to system
- Malicious Code
- Inappropriate system usage (e.g., threatening email)
- An attack of network systems or applications

Procedure:

1. **HMIS Users** will notify their supervisors and their agency's HMIS Liaison of any suspected or confirmed breach immediately.

2. **HMIS Liaisons** will gather information and notify their Executive Directors and the HMIS Lead as soon as possible.

3. **Liaisons** should report any incident to the HMIS Lead within 3 business days.

4. **Executive Directors** will determine any disciplinary actions needed in accordance with agency policies and values within seven days of submitting the incident report.

5. The **HMIS Lead** team will review any information provided and discuss with the CHO within three business days.

6. The **HMIS Lead** will escalate the issue to the HMIS Committee, CoC Board, or another designated committee if needed.

7. The **HMIS Lead** will provide a written response, which may include a corrective action plan.

8. If a corrective action plan is issued, the **HMIS Agency Liaison**, and/or **Executive Director** of the CHO will implement remediation within 30 days for review by the HMIS Lead.

9. If needed, the **Executive Director** will send a written appeal letter of any action taken as a result of the initial incident to the HMIS Committee, CoC Board, or other designated committee.

SECURITY POLICY

INTRODUCTION

All Continuums of Care (CoCs) are responsible for the oversight and operation of a Homeless Management Information System (HMIS). 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 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.

Each Covered Homeless Organization (CHO) that participates in the CA-502 CoC must

decide to adopt the 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 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.
CA-502 Oakland, Berkeley/Alameda County CoC

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

DEFINITIONS AND SCOPE

DEFINITIONS

● Covered Homeless Organization (CHO): Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, discloses or processes personal Identifiable Information (PII) on clients at-risk of or experiencing homelessness. This definition includes both organizations that have direct access to the 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://achmis.org/docs/forms/AC_HMIS_ROI_Providers20220610.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. Below is a CA-502 Oakland, Berkeley/Alameda County CoC

A non-exhaustive list of information that may constitute PII on its own or in combination with other information.

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

● Privacy Notice: A document maintained and published by each CHO that describes for clients 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.

APPLYING THIS POLICY

This Policy applies to any CHO that records, uses, or processes personally identifiable information

(PII) for the CoC 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 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.
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.

1 SYSTEM SECURITY

1.1 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.

1.2USER AUTHENTICATION

Each user accessing an electronic device that contains 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 The HMIS on more than one workstation at a time or log on to the network at more than one location at a time.

1.3 VIRUS PROTECTION

A CHO must protect the 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 HMIS application is used and/or where PII is stored. A CHO must regularly update virus definitions from the software vendor.

1.4 FIREWALLS

A CHO must protect the 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 HMIS inside or outside the CHO, must be equipped with its own firewall.

1.5 PUBLIC ACCESS

The 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.

1.6 PHYSICAL ACCESS TO SYSTEMS WITH ACCESS TO HMIS DATA

A CHO always must staff computers stationed in public areas that are used to collect and store 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. 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, 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.

1.7 DISASTER PROTECTION AND RECOVERY

The 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 HMIS data.

1.8 DISPOSAL

To delete all HMIS data from a data storage medium (e.g., computer, 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, HMIS data, the CHO must take measures to render the data unrecoverable.

1.9 SYSTEM MONITORING

A CHO must use appropriate methods to monitor security systems. Systems that have access to any 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.

2 APPLICATION SECURITY

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

2.1 DISASTER PROTECTION AND RECOVERY

Bitfocus, the vendor of Clarity Human Systems, is responsible for the disaster protection and recovery of the central server, as well as data disposal.

2.2 APPLICABILITY

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

2.3 ELECTRONIC DATA TRANSMISSION

A CHO must encrypt all 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.

2.4 ELECTRONIC DATA STORAGE

A CHO must store all 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.

3 HARD COPY SECURITY

This section provides standards for securing hard copy data.

3.1 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 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 SECURITY

A CHO always must supervise any paper or other hard copy generated by or for the 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.

2 Security Inspection and Annual Review

At the time of HMIS onboarding, the HMIS Lead will give CHOs recommendations to ensure secure practices, a secure environment, and compliance with CoC policies. The network and each workstation used to access the HMIS and/or PII requires an inspection once prior to initial use and annually, due on June 30th. This applies to all workstations used inside and outside an office environment, including those workstations approved for remote access. This process is currently done virtually.

The following areas of security will be examined and documented:

- Physical and environmental security (cabinets, file drawers, desk)
- Workstation, including physical devices
- Printer location
- Individual or network firewalls
- Anti-virus protection
- Password protection (log-in, screensaver, files)
- License review

Procedure:

1. The **HMIS Agency Liaison** or technical designee will complete an HMIS Network Security form for each network and submit the completed and signed forms to the **HMIS Lead** at hmissupport@achmis.org for review.

2. The **HMIS Lead** will confirm receipt, review submitted forms, and store in a secure, central location. If needed, the Team will provide a written response and/ or a corrective action plan.

3. If a corrective action plan is issued, the **HMIS Agency Liaison**, technical designee, and **Executive Director** of the CHO will ensure the plan is followed within the specified schedule. They will send a written appeal letter to the CoC Board or designated committee, if necessary.

3 New HMIS Account Setup and Password Support

A unique username and password are required for HMIS users to access client data (PII) via any electronic device. Written information specifically pertaining to user access

(e.g., username and password) must not be stored or displayed in any publicly accessible location.

Procedure:

1. **HMIS Users** will ensure all applications and encryption passwords meet the following requirements:
   - At least eight characters long, including one number and one letter or symbol, and
   - Must not include the username, "HMIS," an HMIS vendor name, any entire word found in the common dictionary or any of the above spelled backwards.

2. For HMIS password support, users should contact hmissupport@achmis.org.

3. HMIS users should never share their passwords with anyone, including their HMIS Liaison or the HMIS Lead.

4 Physical Access and Workstation Security

CHOs must be diligent in ensuring the security of computers used to collect and store HMIS data. If possible, these computers should not be in areas accessible to the public. If that is not possible, staff members always should be stationed at these computers. When workstations are not in use and staff are not present, their password-protected screensavers must automatically turn on to ensure that the computers and data are secure and not accessible by unauthorized individuals. Password-protected screensavers are a standard feature with most operating systems, and the period before activation can be set by the CHO. If staff will be gone for an extended period, they 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 not in use.

Procedure:

1. **HMIS Users** should position their computer screens to prevent unauthorized viewing and ensure that screens automatically lock within 5-8 minutes of inactivity. If they are using a laptop, they should ensure that it is secured with a locking device.

2. Users should lock the screen when they are walking away from their workstation, or when an unauthorized person is approaching and could possibly view the screen.

3. Upon ending a shift, relocating to another workstation, or leaving the workstation for an extended period, users should log out of HMIS and shutdown the compute

4. In video conference meetings, users must be diligent about sharing HMIS data onscreen only with other users who have the same responsibility for protecting the information.

4.1 Remote Access Requests

Staff can only access PII or the HMIS system outside of their agency's office if they have been approved for remote access by the HMIS Lead. The Remote Access form must be completed and approved.

Procedure:

1. **HMIS Users** should discuss their remote access request with their supervisor.
2. The user's **Supervisor** will send the request to the agency's HMIS Liaison.
3. The **HMIS Agency Liaison** and technical support will inspect the remote workstation to assess compliance with the HUD HMIS Data and Technical Standards Final Notice.[8]
4. The **HMIS Liaison** will complete a Remote Access Request Form, sign it, and send it to the HMIS Lead.
5. The **HMIS Lead** will review the form and reply to the agency's HMIS Liaison with inspection results and any suggested corrections and will accept or deny the request in writing.
6. The **HMIS Agency Liaison** will follow-up with the HMIS User and Supervisor.

4.2 Anti-Virus Protection

A CHO must protect the HMIS, and any electronic device used to store PII, by using up-to-date anti-virus protection software. Anti-virus software should be present, active, and automatically updated with current versions. Anti-virus protection must include automated scanning of HMIS and/or PII files as users access them.

Procedure:

8 https://www.govinfo.gov/content/pkg/FR-2004-07-30/pdf/04-17097.pdf

1. **HMIS Users** will run anti-virus protection software updates promptly upon notification.

2. If a virus is identified or suspected, users will notify the **HMIS Liaison** immediately.

3. If a virus is identified or suspected, the **HMIS Liaison** will notify the **HMIS Lead** immediately.

4. The **HMIS Lead** will suspend access until the entire system is cleaned and declared secure.
    a. If the virus is on a CHO network, the Team will suspend access for the entire CHO.
    b. If the virus is only on a user's device used remotely (not on the CHO's network), the Team will suspend access for that user until the CHO verifies that the device is virus-free

4.3 Hard Copy Handling, Storage, and Disposal

A CHO must secure and supervise (e.g., locked drawer or cabinet) any paper or other hard copy containing PII that is either generated by or for the HMIS, including, but not limited to reports, data entry forms, and case/client notes.

Procedure:

1. **HMIS Users** and/or CHO employees will handle hard copy information (e.g., agreements, reports, data entry forms, and case/client notes) containing PII in areas that are not publicly accessible (for example, in a private office) and never leave the materials unattended.

2. Users should promptly remove documents containing PII from the printer.

3. Users must store hard copies containing PII in a locked drawer or cabinet within the office when not in use.

4. Users will dispose of hard copies containing PII by shredding them or placing them in a secure, locked shred bin.

4.4 Electronic Storage

A CHO must store all 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) is already storing data in binary format and no other steps need to be taken

Procedure:

1. **HMIS Users** will save computer files containing PII to a limited access folder. If multiple team members have access to that folder, the **CHO** should ensure that the file is password protected.

2. Users will share the passwords to the folder(s) and/or file(s) only with team members who are authorized to access client PII.

3. If the data is stored on a portable medium (e.g., flash drive, disks, CDs), users should ensure that the medium is password protected and stored in a locked drawer or cabinet when not in use.

4.5 Encryption and Electronic Transmission

CHO must encrypt all 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.

Procedure:

1. If multiple **HMIS Users** or CHO employees who handle PII have access to a folder containing HMIS data or PII, they should ensure that the folder or files are password protected.

2. When providing the password(s) of the folder(s) and/or file(s) to other users, staff must send the password(s) in a separate email from the data file itself.

3. Use of a secure messaging application (e.g., DropBox) is preferable to attaching the file to an email.

4. Users should follow their CHO's "encryption" process.

4.6 Electronic Disposal

Prior to disposing of any data storage medium that contains, or may contain, HMIS data, the CHO must take measures to render the data unrecoverable. To delete all HMIS data from a data storage medium (e.g., computer, phone, flash drive, CD), a CHO must reformat (at least twice) the storage medium to the standard that the CHO follows. The CHO must verify that the data is no longer recoverable.

Procedure:

1. The **HMIS Liaison** or their technical designee will reformat the hard drive of any storage medium that is being reused or disposed of at least twice, then verify that the data cannot be recovered.

2. For cloud storage, they will follow the application instructions to ensure that erased files cannot be recovered.

Data Quality Policies and Procedures

Alameda County Homeless Management Information System
2024 Data Quality Policies and Procedures

General Objective:

Data Quality (DQ) is built on five pillars: Timeliness; Completeness; Accuracy; Consistency; and Utilization. The policies and procedures provided in this document are designed to strengthen each of these pillars. This will improve data reliability and help measure the effectiveness of the provision of homeless services within Alameda County. Our intent is to empower our community partners to review data quality regularly and effectively and make consistent improvements in their data quality measures.

Data Quality Standards

The following data quality standards are the minimal standards to be met by all agencies entering data into HMIS. When data quality standards are met, reporting is more reliable and can be used to evaluate service delivery, project design and effectiveness, and efficiency of the system. To ensure that all HMIS users have the necessary support to meet the Alameda County HMIS DQ Standards, all HMIS users must complete required HMIS training before gaining access to the system, and all Coordinated Entry Users must complete required Coordinated Entry training before gaining access to the Coordinated Entry Agency.

Data Type	Benchmarks[1]
Project Descriptor Data Elements (Completeness)	95%
Universal Data Elements (Completeness)	95%
Project Specific Data Elements (Completeness)	95%
Timeliness	95%[2]
Accuracy	100%
Consistency	100%
Bed Utilization (ES)	80% MIN – 103% MAX
Bed Utilization (RRH)	80% MIN – 103% MAX
Bed Utilization (PSH)	80% MIN – 103% MAX
Bed Utilization (Safe Haven)	80% MIN – 103% MAX
Bed Utilization (TH)	80% MIN – 103% MAX

Data Quality Components

[1] For Street Outreach Projects - Only applies after client has a Date of Engagement
[2] These benchmarks apply to Year Three Goals as shown in following Timeliness chart

TIMELINESS:

Timeliness measures the time period between a program entry or program exit date and when the data is entered into HMIS. The shorter the period between the time the data was collected and the time the data was entered, the more beneficial the data is to the community to track services and provide accurate reporting. Timeliness data are used to inform and improve ACHMIS decisions on providing client services. Timely data support good client outcomes.

Timeliness Data Source: **DQR** Q6 and Q1 or **APR** Q6e and Q5a							
Data Entry / Days after collection	Project Starts	% of Total	Project Exits	% of Total	Year 1 Goals	Year 2 Goals	Year 3 Goals
0-3 days	DQR Q6 row 1 + 2	DQR Q6 row 1 + 2 / Q1 row 1 as %	DQR Q6 row 1 + 2	DQR Q6 row 1 + 2 / Q1 row 5 as %	>75% of client entries	>85% of client entries	>95% of client entries
4+ days	DQR Q6 row 3 + 4 + 5	DQR Q6 row 3 + 4 + 5 / Q1 row 1 as %	DQR Q6 row 3 + 4 + 5	DQR Q6 row 3 + 4 + 5 / Q1 row 5 as %	<25% of client entries	<15% of client entries	<5% of client entries

Policy:

Participating agencies/jurisdictions are required to use the Alameda County Continuum of Care (CoC) standard forms as the basis for collecting hard copy input for Universal Data Elements (UDEs) required by HUD at project enrollment, annual updates, and project exit. Additional fields may be added to provider forms as needed by each agency.

Standard:

The goal of the Alameda County CoC is for 95% of project entry and exit data to be entered in the HMIS within three days of actual Project Start, Project Exit, or Service Provision date.

Procedure:

Participating agencies/jurisdictions must run the HUD Annual Performance Report (APR) or HMIS Data Quality Report (DQR)[3] at the project level at least once a month to monitor overall agency performance, and for review with HMIS Lead Team.

Reports must be run at the project level to identify underperforming projects. The information is used to identify potential workflow issues or staffing issues that are contributing to delayed data entry.

HMIS Lead must present timeliness reporting to HMIS Committee on a quarterly basis.

The CoC must add timeliness to the scoring criteria for the annual CoC Local Competition for funding.

Best Practice:

Running reports on a monthly basis (agency staff or Agency Liaison) and correcting data quality

[3] The HUD Annual Performance Report (APR) includes additional data points not required for the data quality report so may take longer to run, and the HMIS Data Quality Report (DQR) is more specific and may run more quickly. Either report is acceptable for the purposes of the data quality plan.

issues uncovered by the reports builds a culture of timeliness.

Workflow and staffing issues are discovered early which greatly reduces the systemwide impact of data issues. Timeliness metrics must be included in program contracts and monitoring, as well as performance incentives and reporting requirements for funding.

COMPLETENESS

Completeness is a measure of whether all the required data elements are entered into HMIS, and whether all the persons being served are reported in HMIS. Error rates include missing data, data not collected, client doesn't know, client refused, and fields with data quality issues. To ensure that programs are eligible for federal, state, and county funding, data must be collected, among other requirements, for all clients being served and/or assessed.

There are two categories of data elements used in HMIS:

1. Universal Data Elements (UDE) - Required of all projects that participate in the Alameda County Homelessness Management Information System (ACHMIS).
2. Program Specific Data Elements (PSDE) - Requirements vary by project type and funding source.

The table below shows the current Data Completeness thresholds by project type for each type of data element collected in HMIS: Universal Data Elements, Program Specific Data Elements at Entry, and Program Specific Data Elements at Exit.

Personally Identifiable Information - Data Source: DQR Q2 or APR Q6a				
Data Element	Error Count	% of Error Rate	Maximum Acceptable Error Rates (ES, TH, RRH, PSH)	Maximum Acceptable error rates for Street Outreach Programs
Name (3.1)	DQR Q2 row 1 col 1+2+3	DQR Q2 row 1 col 4 as %	5%	15%
Social Security Number (3.2)	DQR Q2 row 2 col 1+2+3	DQR Q2 row 2 col 4 as %	10%	20%
Date of Birth (3.3)	DQR Q2 row 3 col 1+2+3	DQR Q2 row 3 col 4 as %	5%	15%
Race Ethnicity (3.4)	DQR Q2 row 4 col 1+2	DQR Q2 row 4 col 4 as %	10%	20%
Gender (3.6)	DQR Q2 row 6 col 1+2	DQR Q2 row 6 col 4 as %	5%	15%
Overall Score*		DQR Q2 row 7 col 4 as %	10%	20%
Universal Data Elements – Data Source: DQR Q3 or APR Q6b				
Data Element	Error Count	% of Error Rate	Maximum Acceptable Error Rates (ES, TH, RRH, PSH)	Maximum Acceptable error rates for Street Outreach Programs
Veteran Status (3.7)	DQR Q3 row 1 col 1	DQR Q3 row 1 col 2 as %	5%	15%
Project Start Date (3.10)	DQR Q3 row 2 col 1	DQR Q3 row 2 col 2 as %	5%	15%
Relationship to Head of Household (3.15)	DQR Q3 row 3 col 1	DQR Q3 row 3 col 2 as %	5%	15%
Disabling Condition (3.8)	DQR Q3 row 4 col 1	DQR Q3 row 4 col 2 as %	5%	15%

Income and Housing Data Quality – Data Source: DQR Q4 or APR Q6c				
Data Element	Error Count	% of Error Rate	Maximum Acceptable Error Rates (ES, TH, RRH, PSH)	Maximum Acceptable error rates for Street Outreach Programs
Destination (3.12)	DQR Q4 row 1 col 1	DQR Q4 row 1 col 2 as %	5%	15%
Income and Sources (4.2) at Start	DQR Q4 row 2 col 1	DQR Q4 row 2 col 2 as %	5%	15%
Income and Sources (4.2) at Annual Assessment	DQR Q4 row 3 col 1	DQR Q4 row 3 col 2 as %	5%	15%
Income and Sources (4.2) at Exit	DQR Q4 row 4 col 1	DQR Q4 row 4 col 2 as %	5%	15%
Non-Cash Benefits (4.3) at Start	DQR Q4 row 5 col 1	DQR Q4 row 5 col 2 as %	5%	15%
Non-Cash Benefits (4.3) at Annual Assessment	DQR Q4 row 6 col 1	DQR Q4 row 6 col 2 as %	5%	15%
Non-Cash Benefits (4.3) at Exit	DQR Q4 row 7 col 1	DQR Q4 row 7 col 2 as %	5%	15%
Annual Assessment Data Source: APR Q16				
Annual Assessment	Error Count	% of Error Rate	Maximum Acceptable Error Rates (ES, TH, RRH, PSH)	Maximum Acceptable error rates for Street Outreach Programs
Adults Missing Annual Assessment	APR Q16 row 12 col 2	APR Q16 row 12 Q5a row 8 As col 2/%	5%	15%

Chronic Homelessness - Data Source: DQR Q5 or APR Q6d		
Starting into Project Type	% of Error Rate	Maximum Acceptable Error Rates
ES, SH, Street Outreach	DQR Q5 row 1 col 7 as %	5%,15% for Street Outreach
TH	DQR Q5 row 2 col 7 as %	5%
PH (all)	DQR Q5 row 3 col 7 as %	5%
CE	DQR Q5 row 4 col 7 as %	5%
	DQR Q5 row 5 col 7 as %	5%

*If overall score has more than 5% error rate those errors must be attributable to errors in race/ethnicity and/or social security number

Policy:

All data on standard collection forms must be collected. Error rates include missing data, data not collected, client doesn't know, client refused, and fields with data quality issues. To ensure that programs are eligible for federal, state, and county funding, data must be collected, among other requirements, for all clients being served and/or assessed. Those collecting data must attempt to have as few null, missing, "data not collected," "client refused," and "client doesn't know" field entries as possible.

Standard:

5%* or less error rate for ES, TH, RRH, PSH, Supportive Services Only, Homeless Prevention, Coordinated Entry and Other projects.

The Annual Assessment must be completed on all clients enrolled more than twelve months. The Annual Assessment must be completed within thirty days before or after the client's anniversary date.

Procedure:

Participating agencies/jurisdictions must run the HUD Annual Performance Report or the HMIS

DQ Report looking specifically at Personally Identifiable Information, Universal Data Elements, Income and Housing DQ, and Chronic Homelessness to ensure % error rates are within the standard guidelines listed above.

At a minimum the reports must be run on an agency-wide basis at least once a month to monitor overall agency performance. The information is used to identify data collection and data entry problems and resolutions to those problems such as staff training.

Completeness will be reviewed at the Agency Liaison Meeting that is convened monthly and facilitated by the HMIS Lead. Agencies should be prepared to share their performance, discuss challenges, and develop strategies to improve performance. Agency Liaisons must also run this report on a quarterly basis to review with the HMIS Lead Team.

Best Practice:

Running reports on a bimonthly basis and correcting issues uncovered by the reports builds a culture of completeness. Workflow and staffing issues are discovered early which greatly reduces the systemwide impact of data entry errors.

ACCURACY

Accuracy is a measure of how well the client record reflects the client experience. Accuracy is the most difficult to measure objectively. We look for indicators that are inconsistent in the client record. We also look for indicators that project data is unlike other similar projects. Accuracy is best checked by comparing project hard copy files (if available) to project data elements.

Policy:

Agency staff must maintain electronic client records in HMIS that accurately reflect the current situation. This must include maintaining the client's enrollment information and ensuring that project census data accurately reflects the project population on any given night or period of operation.

Standard:

Client characteristics (and demographics) and program data elements must be consistent with project eligibility requirements (for example veteran status, family structure, income requirements, etc.)

100% of PSH and 98.4% RRH entries must have move-in dates documented in HMIS once participant has moved in.

The enrolled project population must match the project capacity (+/- 5%). Exceptions must be established and reported to the HMIS lead for the Housing Inventory Count (HIC) monthly.

Current Living Situation Assessments must be conducted every calendar month for those actively enrolled in Coordinated Entry.

Program enrollments must be reviewed for:

- Multiple open entries into the same project type for the same client
- No defined head of household
- Multiple defined heads of household

Procedure:

Participating agencies/jurisdictions must run the HUD Annual Performance Report, DQ Report,

Missing Move-In Date Report and Project Households With Issues In Hoh Determination Report, in order to assure an acceptable level of data quality. In addition to required reports, there are many community reports located in the data quality section of the HMIS reporting tool that are relevant and helpful.

At a minimum, required reports must be run on an agency-wide basis at least once a month to monitor overall system performance. The information is used to identify potential data accuracy issues.

Accuracy must be reviewed at the Agency Liaison Meeting that is convened monthly and facilitated by the HMIS Lead. Agencies should be prepared to share their performance, discuss challenges, and develop strategies to improve performance. Agency Liaisons must also run this report on a quarterly basis to review with the HMIS Lead Team.

Accuracy must be reviewed by the HMIS Committee on at least a quarterly basis. Accuracy metrics must be included in program incentives and reporting requirements for funding.

Accuracy – Data Source: Missing Move-In Dates PSH & RRH 2024 & DQR Q1 or APR Q5a		
Project	Count in HMIS	Maximum Acceptable Error Rates
PSH – missing move-in date	Missing Move-In Dates	0.0%
RRH – missing move-in date	Missing Move-In Dates	2.0%

Best Practice:
Running reports on a monthly basis and correcting issues uncovered by the reports builds a culture of accuracy. Workflow and staffing issues are discovered early which greatly reduces the systemwide impact of data issues.

CONSISTENCY

Consistency is the degree to which all data is collected, entered, stored, and reflective of the use of HMIS as a standard operating procedure. Consistency will be representative of how well completeness, accuracy, and timeliness standards have been operationalized across the data collection and entry stages. Consistency may also refer to the data storage, table structure, and overall reliability of the HMIS database management process. In this regard, consistency bridges data quality across data collection, entry, and management stages and enables shared responsibility across multiple HMIS stakeholders.

As with accuracy, strong data consistency also relies on excellent training—both for data collection and entry, as well as for project setup and report structures. Consistency in data entry for project types from provider to provider is essential. For example, a permanent supportive housing (PSH) project run by Provider A must have the same workflow as a PSH project run by Provider B. All stakeholders have a role in ensuring data consistency.

Policy:

Client and project data should be collected on data collection forms that are standardized and maintained by the CoC and communicated to the HMIS Lead. Supplemental data should be collected on supplemental assessments defined by the program funder. Agencies can collect additional supplemental data by coordinating with HMIS staff to develop a supplemental assessment that maintains data consistency across the CoC.

Standard:
All clients must have one single record; providers must avoid creating duplicate clients.

Project enrollments must be completed on forms that include all data elements required by the CoC.

Coordinated entry assessments must be completed using designated project-specific online assessments approved by the CoC and implemented in the HMIS.

Supplemental project data must be collected on supplemental forms and entered on supplemental data entry screens common to that project type.

Supplemental agency data should be collected on supplemental forms and entered on supplemental screens common to that agency's projects.

Procedure:
Participating agencies/jurisdictions must run the HUD Annual Performance report and any community reports found in the data quality section of the reporting tool. At a minimum, the reports must be run on an agency-wide basis at least once a month to monitor overall system performance. The reports can be run at the project level to identify underperforming projects. The information will be used to identify potential workflow issues or staffing issues that are contributing to delayed data entry. Agency Liaisons must also run this report on a quarterly basis to review with the HMIS Lead Team.

Best Practice:
Running reports on a monthly basis and correcting issues uncovered by the reports builds a culture of consistency. Workflow and staffing issues are discovered early which greatly reduces the systemwide impact of data issues.

Agencies must use regular reporting to ensure that project performance is meeting or exceeding project expectations and is consistent with project expectations.

Consistency – Data Source: # of Duplicates/Total Clients Created Measured by # of Duplicate Merge Requests in the quarter		
	Raw Number	Maximum Acceptable Error Rate = 0%
Total Clients Created	##	
Total Duplicate Clients	##	0%

UTILIZATION
Utilization is the measure of how completely bed and unit inventory information is captured in HMIS. Utilization is measured at the project level by dividing the total number of beds represented in HMIS (the numerator) by the total number of beds available in the project (the denominator). At the agency and system level, utilization is measured by dividing the total number of beds for a given project type by the total number of beds available for that project type, e.g., *x* Beds Utilized/*y* Beds Available = Total Utilization.

Policy:
All housing dedicated to improving the living situation of homeless people in Alameda County must capture client and project data in HMIS.

Standard:
Our community goal is 80% utilization across emergency shelter, seasonal shelter, rapid re-housing, permanent supportive housing, Safe Haven, and transitional housing beds that appear in the Housing Assessment Report (HSNG-102).

Procedure:
HMIS participating agencies must ensure that all beds are recorded in and enrolled through HMIS, regardless of funding source.

Agency Liaisons must run the HSNG-102 report on a quarterly basis to review with the HMIS Lead Team.

The HMIS Lead must present utilization rates to the HMIS Committee quarterly.

Partner agencies must communicate changes in bed capacity as soon as possible to the HMIS Lead for incorporation in the Housing Assessment Report (HSNG-102) and Housing Inventory Chart (HIC).

Utilization – Data Source: HSNG-102 – Housing Assessment Report				
Bed Type	Bed Count	HMIS Beds Filled	% HMIS Bed Utilization	Acceptable % Utilization
Year-Round ES Beds	Sum of Beds by type	Sum of HMIS Beds by type	HMIS Beds / Beds as %	80%
Seasonal Beds	Sum of Beds by type	Sum of HMIS Beds by type	HMIS Beds / Beds as %	80%
Year-Round RRH Beds	Sum of Beds by type	Sum of HMIS Beds by type	HMIS Beds / Beds as %	80%
Year-Round PSH Beds	Sum of Beds by type	Sum of HMIS Beds by type	HMIS Beds / Beds as %	80%
Year-Round Safe Haven Beds	Sum of Beds by type	Sum of HMIS Beds by type	HMIS Beds / Beds as %	80%
Year-Round TH Beds	Sum of Beds by type	Sum of HMIS Beds by type	HMIS Beds / Beds as %	80%

Data Quality Monitoring and Reporting Process

To ensure a high level of data quality in ACHMIS, it is necessary to establish individual responsibilities for Participating Agencies as well as the HMIS Lead/System Administrators.

The following section outlines the steps and specific actions to review and improve data quality in the ACHMIS. This process must be completed every quarter.

HMIS Lead: Sends Data Quality Corrections to Agency Liaison

- HMIS Lead generates the Data Quality Correction Report (DQCR) for all active projects in the ACHMIS for the previous quarter.
- HMIS Lead sends Agency liaisons the DQCR, which flags errors specified within the five data quality parameters, Timeliness, Completeness, Accuracy, Consistency, and Utilization, across fields associated with the Universal Data Elements (UDE) for active enrollments during the previous quarter.

Agency: Correct missing data/errors in HMIS

- Agencies complete missing information where possible and make appropriate corrections to the clients' enrollments in HMIS according to the DQ errors highlighted in the Data Quality Correction Report.

- Agencies review the Data Quality Corrections Reference Guide to see a description of the data quality errors highlighted in the report and see instructions on how to correct data issues.

HMIS Lead: Runs and publishes Data Quality Report Cards

- HMIS Lead publishes the Data Quality Report Cards Dashboard which assesses Data Completeness, Accuracy, and Timeliness for active enrollments during the previous quarter in all the projects participating in AC
- The Data Quality Report Cards Dashboard includes the percentage of data errors and valid responses for each UDE by project, the Average Data Completeness Score for each project, and the average number of days it takes agencies to record intake, exit, and services information in HMIS for each project.

In preparation for the data quality monitoring and reporting process, Agency Liaisons must utilize the additional reports and tools that HMIS Lead has made available to review the data quality in their projects. These reports and tools are explained further in the appendices of this document.

Incentives and Standards Reinforcement

This section describes actions that the Alameda County CoC may take to encourage agencies to have high data quality, and the interventions needed to assist projects that have not been able to meet the data quality thresholds. The implementation of incentives and standards enforcement will allow the HMIS Lead to prioritize the projects that need to be assisted with additional technical support.

Incentives

The HMIS Lead will report agencies with projects meeting data quality thresholds for all four quarters in the calendar year to the HMIS Committee.

The HMIS Lead will publish the list of agencies with projects that met data quality thresholds for all four quarters in the calendar year on the HMIS website.

Standards Reinforcement:

The HMIS Lead will provide technical support to projects with at least four data elements under 75% in any quarter.
The HMIS Lead will report agencies with projects requiring technical support in 4 consecutive quarters to the HMIS Committee.

If an agency applies for funding approved by the HMIS Committee and has projects targeted for technical support in at least four consecutive quarters, the agency will be required to address data quality issues in their application.

The HMIS committee will review projects targeted for technical support in 4 consecutive quarters and not receiving funding requiring HMIS participation to determine the appropriateness of the project's continued HMIS participation.

Projects removed from HMIS may reapply for access after three months.

Data Quality Appendices

Appendix A: Timeliness Reports

Timeliness reports show the time it takes for Homeless Services Providers to record intake, exit, and services information in ACHMIS for each project on a client level. These reports must be run every quarter in preparation for the Data Quality Report Cards publication. The following HMIS reports are located in the Reports Page of HMIS, under the Data Analysis tab, Data Quality section.

Project Start Data Timeliness Report:

This report shows the number of days taken to record Project Start data into HMIS for each client enrollment.

Services Data Timeliness Report:

This report shows the number of days taken to record Services data into HMIS for each client enrollment.

Project Exit Data Timeliness Report:

This report shows the number of days taken to record Project Exit data into HMIS for each client enrollment.

Appendix B: Completeness Reports

Completeness reports assess the degree to which all required data elements are answered in HMIS for all the clients to whom these data elements apply. Homeless Services Providers must run and review Completeness Reports quarterly to identify incomplete or missing information. The following reports are located in the Reports Page of HMIS, under the Data Analysis tab, Data Quality section.

Universal Data Elements (UDE) Completeness Report:

This report shows the client responses to the UDE defined by HUD in the FY 2024 HMIS Data Standards Manual. These data elements must be collected by all projects participating in ACHMIS.

Common Program Specific Data Elements (PSDE) reports:

PSDE at Entry Completeness Report:

This report shows the client responses to the Common PSDE at Project Entry defined by HUD in the FY 2024 HMIS Data Standards Manual. These data elements are collected across most HMIS Federal Partner programs at the start of the clients' enrollments.

PSDE at Exit Completeness Report:

This report shows the client responses to the Common PSDE at Project Exit defined by HUD in the FY 2024 HMIS Data Standards Manual. These data elements are collected across most HMIS Federal Partner programs at the end of the clients' enrollments.

Federal Partner Program Specific Data Elements:

The following reports show the client responses to the data elements developed by each Federal Partner defined by HUD in the HMIS Federal Partner Programs Manual. These data elements can be limited to one or two federal partner programs or a single component of one of the Federal Partner programs.

HOPWA Specific Data Elements:

This report shows the client responses to the Federal Program Specific Data Elements that need to be collected by HOPWA funded projects as defined in the HOPWA Program HMIS Manual.

PATH Specific Data Elements

This report shows the client responses to the Federal Program Specific Data Elements that

need to be collected by PATH funded projects as defined in the PATH Program HMIS Manual.

RHY Specific Data Elements

This report shows the client responses to the Federal Program Specific Data Elements that need to be collected by RHY funded projects as defined in the RHY Program HMIS Manual.

VA Specific Data Elements

This report shows the client responses to the Federal Program Specific Data Elements that need to be collected by Department of Veterans Affairs (VA) funded projects as defined in the VA Program HMIS Manual.

Appendix C: Accuracy Reports

Dashboard: Alameda CE Dashboard (Current Living Situation Assessment & CE Enrollment DQ)
Missing Move-in Dates: Missing Move-in Dates (Data Analysis)
[DQXX-120-AD] Project Households with issues in HoH determination

Appendix D: Consistency Reports

[HUDX-227-AD] Annual Performance Report
[HUDX-225-AD] HMIS Data Quality Report

Appendix E: Utilization / Bed Utilization Reports

Entry/Exit Program Bed Utilization Over the Reporting Period
Housing Assessment Report: [HSNG-102]

Appendix F: HMIS Annual Monitoring Tool

Universal Data Elements (UDE) - Required of all projects that participate in HMIS.
Program Specific Data Elements (PSDE) - Requirements vary by project type and funding source.

HMIS Lead - Annual HMIS & Data Quality Monitoring Checklist Timeframe Monitored (Start-to-End Dates):			
✓	**Monthly Monitoring Standards – If answer is no, add comment**	**Yes**	**No**
☐	Project has submitted UDE report on time each month?	☐	☐
☐	Project is meeting completeness standards for UDEs each month?	☐	☐
☐	Project has submitted PSDE report on time each month?	☐	☐
☐	Project has met PSDE benchmarks each month?	☐	☐
✓	**Random Quarterly Monitoring Standards – If answer is no, add comment**	**Yes**	**No**
☐	PDDEs - Has project had a random quarterly monitoring for PDDEs? If yes, list quarter(s) monitored:	☐	☐
☐	Are the projects PDDEs current and accurate as required by the Data Quality Plan standard?	☐	☐
☐	Has the project notified the CoC HMIS Administrator of changes as required by the Data Quality Plan standard?	☐	☐
☐	**Timeliness** - Has project had a random quarterly monitoring for timeliness? If yes, list quarter(s) monitored:	☐	☐
☐	Are entries and contacts being recorded as required by the Data Quality Plan standard?	☐	☐
☐	Are exits being recorded as required by the Data Quality Plan standard?	☐	☐
☐	Street Outreach Only: Are contacts being recorded as required by the Data Quality Plan standard?	☐	☐

☐	Street Outreach Only: Are no-contact exits being recorded as required by the Data Quality Plan standard?	☐	☐
☐	**Accuracy** - Has project had a random quarterly monitoring for accuracy? If yes, list quarter(s) monitored:	☐	☐
☐	Are accuracy measures being updated/addressed as required by the Data Quality Plan standard?	☐	☐
☐	**Consistency** - Has project had a random quarterly monitoring for consistency? If yes, list quarter(s) monitored:	☐	☐
☐	Are consistency measures being updated/addressed as required by the Data Quality Plan standard?	☐	☐
☐	**Bed Utilization** - Has project had a random quarterly monitoring for bed utilization? If yes, list quarter(s) monitored:	☐	☐
☐	Does the project utilization fall within standards specified in the Data Quality Plan standard?	☐	☐
✓	**Annual Monitoring Standards – If answer is no, add comment**	**Yes**	**No**
☐	**PDDEs** – Did the project respond to the annual PDDE monitoring as required by the Data Quality Plan standard?	☐	☐
	PDDEs – Is the projects:		
☐	- Organization information accurate?	☐	☐
☐	- Project information accurate?	☐	☐
☐	- CoC information accurate?	☐	☐
☐	- Funding source information accurate?	☐	☐
☐	- Bed and unit inventory accurate?	☐	☐
☐	**Accuracy** – Did the project respond to the annual accuracy monitoring as required by the Data Quality Plan standard?	☐	☐
☐	**Accuracy** – Are accuracy measures being updated/addressed as required by the Data Quality Plan standard?	☐	☐

Appendix A: Agreements

A.1 HMIS User Agreements

HMIS User Agreements are agreements between the HMIS Lead Agency and an agency's employees, contractors, or volunteers who collect or use data in the HMIS. These include 1) the Privacy Agreement, which acknowledges the user's commitment to protect clients' confidentiality; and 2) the User Agreement, in which users formally adopt the HMIS policy, responsibilities and code of ethics. See Privacy Agreement.

A.2 HMIS Partnership Agreement (MOU)

The Participation Agreement is a signed memorandum of understanding (MOU) between an agency providing services to people who are homeless (the CHO) and the CoC. The MOU specifies the terms of CHO participation in the HMIS, including meeting technology and security requirements for the HMIS and data-sharing. See AC HMIS MOU.

Appendix B: Consumer-Facing Documents

B.1 Client Grievance Form

Clients have the right to file a grievance based on denial of access, correction of data in the HMIS system, or if the client believes that participation in the HMIS will violate their privacy. See Grievance Form.

B.2 Release of Information (ROI) Form

When a client signs an ROI, they formally agree that agencies providing services to people who are homeless can access their personally identifying information (PII). The ROI specifies that their PII will only be used to improve services, secure continued funding, and for research purposes to better understand the people-served, services provided, and outcomes achieved. See Release of Information (ROI) .

B.3 Release of Information (Revocation) Form

Clients have the right to update or rescind their consent and levels of data sharing at any time. Staff will explain to them that any changes will take effect as of the date the form is signed, and that any data or information shared before that time cannot be recalled. See Release of Information (Revocation) Form

B.4 Privacy Policy

The HMIS Privacy Policy describes the protections for keeping PII confidential while allowing for reasonable, responsible, and limited uses and disclosures of data. The CoC's Privacy Policy is available to clients upon request. See Privacy and Policy.

B.5 Privacy Notice

The Privacy Notice is a consumer-friendly summary of the Privacy Policy that is meant to be easy for clients to understand and act upon. The Privacy Notice will be sufficient for most clients however, they can request a copy of the Privacy Policy as well. See Privacy Notice.

B.6 Alternative Privacy Notice

The alternative notice is for HIPAA-covered agencies and other service providers that want a signed ROI. A HIPAA Privacy Notice must describe the organization's duties to protect health information privacy and how providers use and disclose protected health information. It must also explain that the patient's permission is needed for health records to be shared. Other service providers may use their own one-page Privacy Notice or use the language that HUD suggests in the Federal Register/Vol. 69. No.

146/Friday, July 30, 2004/Notices SEC. 4.2.1 pg. 45929. See https://www.govinfo.gov/app/details/FR-2004-07-30 . See Alternative Policy Notice.

Appendix C: Other Documents

C.1 Informed Consent Tips

Being “informed” means having an understanding of the facts. If the client doesn’t understand the information provided, they can’t give informed consent. This document provides tips to help clients make an informed choice about sharing their personal information. See Informed Consent Tips.

C.2 Security Policy

The HMIS Security Policy outlines the steps that the CoC, HMIS Lead, and participating agencies will take to ensure that client personally identifiable information is not accessible to anyone who is not authorized to see it. See Security Policy.

C.3 Staff Attestation Form

With this form, staff of service provider agencies formally confirm that they reviewed the Privacy Notice with the client, offered assistance with reading the Notice, and gave the client an opportunity to ask questions. See Staff Attestation Form.