Oakland, Berkeley/Alameda County Continuum of Care

CA-502

Homeless Management Information System

Policies and Procedures Manual

Updated November 16, 2022

Table of Contents

1. **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

2. **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 personal 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.

- **HMIS Administrator Team:** 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 Administrator Team, health and services staff, jurisdictional staff, and one member from a CHO. The 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
  - Log in 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, 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.

3. 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 the HMIS.
- Comply with federal, state, and local laws that require additional privacy or confidentiality protections.
- Complete trainings 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 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).

[2] See https://everyonehome.org/wp-content/uploads/2022/08/2022-APPROVED-Data-Quality-Plan-FINAL-2022_06_08.pdf

- 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 Administrator Team on unresolved software issues.
- Working with the HMIS Administrator Team 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 Administrator.
- Representing the CHO at HMIS user meetings, bringing ideas, concerns, and issues to facilitate system improvements.

HMIS Lead Agency: 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 Administrator Team, 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.

HMIS Administrator Team: Responsibilities include:

- 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, 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 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.

4. Onboarding and Implementation

4.1. 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 Administrator Team** will direct them to complete the Agency Onboarding Questionnaire.[4]

2. The **HMIS Administrator Team** 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 Housing Community Development Department Director**, and **CoC Board Director** 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 https://achmis.org/onboarding.html
[5] https://achmis.org/docs/onboarding/Agency%20Implementation%20Readiness%20Checklist.pdf
[6] https://achmis.org/docs/onboarding/AC_HMISProviderAssessment2020.docx

4.2. 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

4.3. 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 Administrator Team will follow the Security Inspection and Annual Review procedure (see Chapter 7, below).

4.4. 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 https://achmis.org/ATutor/login.php, and inform the HMIS Lead agency (via

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

2. The CHO **HMIS Liaison** will email hmissupport@achmis.org and request that User agreements be sent to users via DocuSign.

3. The **HMIS User, CHO HMIS Liaison**, and **HMIS Administrator Team** will sign the electronic agreements via DocuSign.

5. User Training and Support

5.1. 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 180 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://achmis.org/ATutor/login.php**.**
    a. If they successfully complete training, they will proceed to step 3.
    b. Students who fail a quiz may repeat it a maximum of three times. ATutor locks them out if they fail a quiz three times.

2. Students will notify their agency's HMIS Liaison when they complete training or fail a test three times.

3. **HMIS Agency Liaisons** notify the HMIS Administration Team when a student successfully completes training. Alternatively, they will ask the Team to reset test for a student who fail a test three times so that the student can continue training.

4. The **HMIS Administrator Team** confirms that students have completed training and sends them the User Agreements to sign. Once all parties sign the agreements, the Team will create an HMIS account for the staff person and notify the HMIS Liaison of the new user license.

5.2. CHO or HMIS User Support

All requests for technical assistance and HMIS User support related to training shall be submitted to the HMIS Administrator Team by an agency's HMIS Liaison. Users may submit requests for help directly to the HMIS Administration Team 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 Administrator Team** to create an HMIS account for the individual.

3. After they complete training, **HMIS users** may contact the **HMIS Administrator Team** 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 Administrator Team** and the CE Manager. Once the CE Manager approves, the Team will add CE access to the user's HMIS account.

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

6. 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.

6.1. 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 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.

6.2. 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.

6.3. 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:

- For any use or disclosure other than what is defined as allowable, and
- 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.

6.4. 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.

6.5. 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.

6.6. 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.

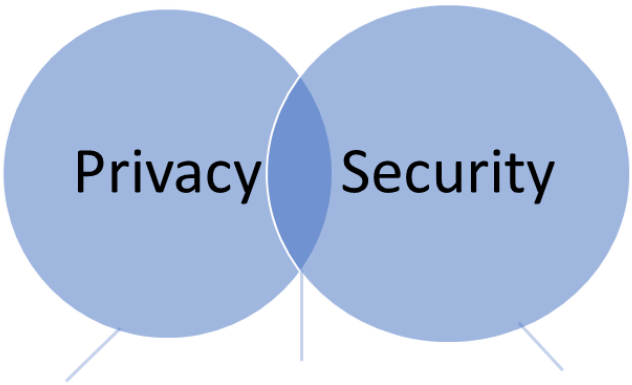
6. **CHO staff** will upload the Grievance form and any related correspondence to the HMIS record.

6.7. 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 Administrator Team within three business days. The HMIS Administrator Team will respond within three business days of receiving the notification. The HMIS Administrator Team will provide a written response or corrective action plan, as appropriate. Corrective actions may include notifying the client, 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 Administrator Team as soon as possible.

3. **Liaisons** should report any incident to the HMIS Administrator Team 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 Administrator Team.

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.

7. **Security Standards**

The CA-502 CoC recognizes its responsibility to safeguard the security of information collected about people experiencing homelessness. At the same time, the CoC affirms its support for sharing HMIS data to facilitate and enhance care coordination, reimbursement for services, homeless system planning, and public knowledge of homelessness. This Policy, in close alignment with the federal HUD HMIS Privacy and Security Standards, describes how to ensure the security of personal information collected and stored in the HMIS and elsewhere in print or electronic formats within the CoC network. A CHO must apply security provisions to all systems where PII is stored, including, but not limited to, the CHO's networks, desktops, laptops, tablets, phones, mainframes, and servers.

7.1. Security Inspection and Annual Review

At the time of HMIS onboarding, the HMIS Administrator Team 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 Administrator Team** at hmissupport@achmis.org for review.

2. The **HMIS Administrator Team** 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. 4. 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.

7.2. 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 Administrator Team

7.3. 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 computer.

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.

7.4. 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 Administrator Team. 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 Administrator Team.
5. The **HMIS Administrator Team** 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.

7.5. 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 virus is identified or suspected, the **HMIS Liaison** will notify the **HMIS Administrator Team** immediately.

4. The **HMIS Administrator Team** 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

7.6. 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 placing them in a secure shred bin.

7.7. 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 passwords 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.

7.8. 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 to other users, staff must send the password 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.

7.9. 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 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.

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 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 personal 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 explain to the 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 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 personal 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.