HMIS Oversight Committee
Wednesday May 13, 2020
Link to Virtual Meeting

1. **Welcome** **9:00-9:05AM**
   - Next Meeting on Wednesday June 10th from 9-11
2. **HMIS Oversight Public Comment** **9:05-9:15 AM**
3. **Agency Onboarding Update** **9:15-9:35 AM**
   - Materials: updated onboarding queue
4. **HMIS Training and Privacy Update** **9:35-10:25 AM**
   - Impact of COVID-19 on training and privacy
   - Census Update to Privacy Policy
5. **Data Quality Plan Update** **10:25-10:40 AM**
   - Materials: updated implementation plan
6. **HMIS ROI** **10:40-11:00 AM**
   - Materials: Review current ROI and HUD requirements
7. **Future Topics:**
   - Data sharing: updating draft policy with language from November meeting
   - Review the current MOU and plan/strategize to revise that document
   - Agencies (e.g. BACS) are requesting way to synchronize data across databases to reduce double data entry. This also promises to improve timeliness and consistency.
   - HMIS Lead Monitoring
   - HMIS Lead workplan
   - Agency onboarding materials
   - Policy issues related to bringing on more PSH providers

224 W. Winton Ave., Suite 108
Hayward, CA 94544

phone 510.670.5404
fax 510.510.670.6378
www.acgov.org/cda/hcd

Privacy Policy

DATE: June 1, 2020
SUBJECT: Privacy and Confidentiality

STATEMENT OF PURPOSE:

1. To protect the privacy of agency clients
2. To comply with applicable laws and regulations.
3. To insure fair information practices as to:
    a. Openness
    b. Accountability
    c. Collection limitations
    d. Purpose and use limitations
    e. Access and correction
    f. Data Quality
    g. Security

STATEMENT OF POLICY:

1) Alameda County Housing & Community Development privacy practices will comply with all applicable laws governing Homeless Management Information System (HMIS, known as ACHMIS) client privacy/confidentiality. Applicable standards include, but are not limited to the following.
   a) Federal Register Vol. *69. No. 146 (I IMIS* FR *4848-N-02)* - Federal statute governing HMIS information – Friday, July 30, 2004.
   b) HIPAA - the Health Insurance Portability Act.
   c) 42 CFR Part 2. - Federal statute governing drug and alcohol treatment.
   d) Alameda County-wide Continuum of Care InHOUSE Policy and Procedures manual.
   e) Alameda County-wide Continuum of Care InHOUSE partner agency sharing agreement(s).

2) **Use of Information** PII (personally identifiable information which can be used to identify a specific client) can be used only for the following purposes:
   a) To provide or coordinate services to a client.
   b) For functions related to payment or reimbursement for services.
   c) To carry out administrative functions such as legal, audit, personnel planning, oversight and management functions.
   d) For creating de-personalized client identification for unduplicated counting.
   e) Where disclosure is required by law.
   f) To prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.
   g) To report abuse, neglect, or domestic violence as required or allowed by law.
   h) Contractual research where privacy conditions are met (including a written agreement).
   i) To report criminal activity on agency premises.
   j) For law enforcement purposes in response to a properly authorized request for information from a properly authorized source.
   k) To provide United States Census Bureau Data for sheltered clients with a written agreement.

3) **Collection and Notification** Information will be collected only by fair and lawful means with the knowledge or consent of the client.
   a) PII will be collected only for the purposes listed above, and entered into ACHMIS.
   b) Clients will be made aware that personal information is being collected and recorded and will be asked to express written consent to have their intake information shared with providers outside the ACHMIS system.
   c) A written sign will be posted in locations where PII is collected. This written notice will read:

"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.

The collection and use of all personal information is guided by strict standards of confidentiality. Our Privacy Notice is posted. A copy of our Privacy Notice is available to all clients upon request."

d) This sign will be explained in cases where the client is unable to read and/or understand it.

4) **Data Quality** PII data will be accurate, complete, timely, and relevant.
   a) All PII collected will be relevant to the purposes for which it is to be used.
   b) Identifiers will be removed from data that is not in current use after 7 years (from date of creation or last edit) unless other requirements mandate longer retention.
   c) Data will be entered in a consistent manner by authorized users.
   d) Data will be entered in as close to real-time data entry as possible.
   e) Measures will be developed to monitor data for accuracy and completeness and for the correction of errors.
      i) The agency runs reports and queries monthly to help identify incomplete or inaccurate information.
      ii) The agency monitors the correction of incomplete or inaccurate information.
      iii) By the 15th of the following month all monitoring reports will reflect corrected data.
   f) Data quality is subject to routine audit by System Administrators who have administrative responsibilities for the database.

5) **Privacy Notice, Purpose Specification and Use Limitations** The purposes for collecting PII data, as well as it uses and disclosures will be specified and limited.
   a) The purposes, uses, disclosures, policies, and practices relative to PII data are to be outlined in this agency Privacy Notice.
   b) The agency Privacy Notice will comply with all applicable regulatory and contractual limitations.
   c) The agency Privacy Notice will be made available to agency clients, or their representative, upon request and explained/interpreted as needed.
   d) Reasonable accommodations will be made with regards to the Privacy Notice for persons with disabilities and non-English speaking clients as required by law.
   e) PII will be used and disclosed only as specified in the Privacy Notice, and only for the purposes specified therein.
   f) Uses and disclosures not specified in the Privacy Notice can be made only with the consent of the client.
   g) The Privacy Notice will be posted on the agency web site.
   h) The Privacy Notice will be reviewed and amended as needed.
   i) Amendments to or revisions of the Privacy Notice will address the retroactivity of any changes.
   j) Permanent documentation will be maintained of all Privacy Notice amendments/revisions.
   k) All access to, and editing of PII data will be tracked by an automated audit trail, and will be monitored for violations use/disclosure limitations.

6) **Record Access and Correction** Provisions will be maintained for the access to and corrections of PII records.
   a) Clients will be allowed to review their ACHMIS record within 5 working days of a request to do so.
   b) During a client review of their record, an agency staff person must be available to explain any entries the client does not understand.
   c) The client may request to have their record corrected so that information is up-to-date and accurate to ensure fairness in its use.
   d) When a correction is requested by a client, the request will be documented and the staff will make a corrective entry if the request is valid.
   e) A client may be denied access to their personal information for the following reasons:
      i) Information is compiled in reasonable anticipation of litigation or comparable proceedings;
      ii) Information about another individual other than the agency staff would be disclosed,
      iii) Information was obtained under a promise of confidentiality other than a promise from this provider and disclosure would reveal the source of the information
      iv) The disclosure of information which would be reasonably likely to endanger the life or physical safety of any individual.
   f) A client may be denied access to their personal information in the case of repeated or harassing requests for access or correction. However, if denied, documentation will be provided regarding the request and reason for denial to the individual and be made a part of the client's record.

g) A grievance process may be initiated if a client feels that their confidentiality rights have been violated, if access has been denied to their personal records, or if they have been put at personal risk, or harmed.
h) Any client grievances relative to the ACHMIS system will be processed/resolved according to agency grievance policy.
i) A copy of any client grievances relative to ACHMIS data or other privacy/ confidentiality issues and agency response are forwarded to CoC staff.
j) If a client is unsatisfied with the resolution of their grievance at the agency level, the client may request mediation at the system level.

7) **Accountability** Processes will be maintained to insure that the privacy and confidentiality of client information is protected and staff is properly prepared and accountable to carry out agency policies and procedure that govern the use of PII data.
a) Grievances may be initiated through the agency grievance process for considering questions or complaints regarding privacy and security policies and practices. All users of the ACHMIS system must sign a Users Agreement that specifies each staff persons' obligations with regard to protecting the privacy of PII and indicates that they have received a copy of the agency's Privacy Notice and that they will comply with its guidelines.
b) All staff, interns, volunteers or associates collecting PII intended for, or viewing data generated by ACHMIS must successfully complete Council-sponsored privacy and security certification training.
c) A process will be maintained to document and verify completion of training requirements.
d) A process will be maintained to monitor and audit compliance with basic privacy requirements including but not limited to auditing clients entered against signed ACHMIS Consent Releases. At minimum, a quarterly Compliance Review will be conducted and documented.
e) A copy of any staff grievances initiated relative to privacy, confidentiality, or ACHMIS system data will be forwarded to CoC Staff.
f) Regular user meetings will be held and issues concerning data security, client confidentiality, and information privacy will be discussed and solutions will be developed.

8) **Sharing of Information** Intake data will be shared with partnering agencies and may be shared with outside agencies, beyond the scope of the approved and required releases above, only with client approval
a) All routine data sharing practices with partnering agencies will be documented and governed by the CoC MOU Agreement that defines the agency-determined sharing practice.
b) Resident name,date of birth, and social security number are viewable in ACHMIS without express written consent for the purpose of searching for a client in the software.
c) A completed ACHMIS Client Release of Information (ROI) Form is needed before information may be shared electronically with outside agencies.
i) The ACHMIS release is to inform the client about what is shared and with whom it is shared.
ii) The client accepts or rejects the sharing plan.
iii) Revisions to the consent for sharing the Basic intake may be requested by the resident during the standard business hours. Changes will not be retroactive.
d) Clients will be informed about and understand the benefits, risks, and available alternatives to sharing their information prior to signing an ROI, and their decision to grant permission shall be voluntary.
e) Clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.
f) All Client Authorization for ROI forms related to the ACHMIS system will be placed in a file to be located on premises and will be made available to the CoC Staff for periodic audits.
g) ACHMIS-related Authorization for ROI forms will be retained for a minimum period of three (3) years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
h) If a client has previously given permission to share information and then chooses to revoke that permission by completing a new ROI, the ACHMIS Intake will be closed to further sharing.
i) All client ROI forms will include an expiration date, and once a Client ROI expires, any new information entered will be closed to sharing unless a new Client ROI is signed by the client and entered in the ACHMIS system.

9) **System Security** System security provisions will apply to all systems where PII is stored: agency's networks, desktops, laptops, mini-computers, cellular phones, mainframes and servers.
a) Password Access:
i) Only individuals who have completed Privacy and Security Certification and Software Training may be given access to the ACHMIS system through User IDs and Passwords,
ii) Temporary default passwords will be changed on first use.

iii) Access to PII requires a user name and password at least 8 characters long and using at least one number and one letter.
iv) Passwords will not use or include the users name or the vendor name, and will not consist entirely of any word found in the common dictionary or any of the above words spelled backwards.
v) User Name and password may not be stored or displayed in any publicly accessible location.
vi) Passwords must be changed routinely.
vii) Individuals with User IDs and Passwords will not give or share assigned User IDs and Passwords to access the ACHMIS system with any other person, organization, governmental entity, business.

b) Virus Protection and Firewalls:
i) Commercial anti-virus protection software will be maintained to protect all agency network systems and workstations from virus attack.
ii) Virus protection will include automated scanning of files as they are accessed by users.
iii) Virus Definitions will be updated regularly.
iv) All workstations will be protected by a firewall either through a workstation firewall or a server firewall.

c) Physical Access to Systems where ACHMIS Data is Stored
i) Computers stationed in public places must be secured when workstations are not in use and staff are not present.
ii) After a short period of time a pass word protected screen saver will be activated during time that the system is temporarily not in use.
iii) For extended absence from a workstation, staff must log off the computer.

d) Stored Data Security and Disposal:
i) All ACHMIS data downloaded onto a data storage medium must be maintained and stored in a secure location, not accessible to non-licensed users of the ACHMIS system or staff that do not have Privacy and Security certification.
ii) Data stored on a portable medium will be secured when not in use.
iii) Data downloaded for purposes of statistical analysis will exclude PII whenever possible.
iii) ACHMIS data downloaded onto a data storage medium must be disposed of by reformatting as opposed to erasing or deleting. This includes hard drives.
iv) A data storage medium will be reformatted a second time before the medium is reused or disposed of.

e) System Monitoring
i) User access to the ACHMIS Live Web Site will be monitored using the computer access logs located on each computer's explorer "history" button, or via a central server report.

f) Hard Copy Security:
i) Any paper or other hard copy containing PII that is either generated by or for ACHMIS including, but not limited to report, data entry forms and signed consent forms will be secured.
ii) Agency staff will supervise at all time hard copy with identifying information generated by or for the ACHMIS system when the hard copy is in a public area. If the staff leaves the area, the hard copy must be secured in areas not accessible by the public.
iii) All written information pertaining to the user name and password must not be stored or displayed in any public accessible location.

g) Authorized Location Access:
i) Access to the ACHMIS system is allowed only from authorized agency locations.

10) **Agency HMIS/ACHMIS Grievance Policy** Clients will contact the Participating Agency with which they have an HMIS data related grievance for resolution of problems.
i) Participating Agencies will report all HMIS-related client grievances to the HMIS Lead Agency Senior Manager or designee.
ii) The purpose of the Grievance Policy is to allow clients to express concerns and have correction implemented.
iii) Continuum, agency, or client levels may be brought before the CoC Committee for a decision in accordance with the HMIS Grievance procedure.
iv) If a client wants to file a complaint:
1. The Client complaint is to be brought directly to the Participating Agency with which they have a grievance within seven days of the grievance.
2. The Participating Agency shall assist the client in the Grievance Procedure.
3. The complaint is to be stated in writing.
4. The complaint shall be returned to the Participating Agency's Executive Director or designee who has the ability and authority to take corrective action. If needed the HMIS Senior Manager or designee will assist in the identifying the appropriate party.

5. The client and the Participating Agency's representative meet together with the appropriate HMIS Lead Agency staff to resolve the complaint.
6. The actions and resolutions shall be in writing.
7. Should the client want to appeal the HMIS Lead Agency's decision, a grievance subcommittee of the CoC Committee will hear the complaint a scheduled meeting and resolve the complaint in a manner in which it makes its decision. This decision is final.
8. All actions and resolutions will be in writing. Both the client and the HMIS party involved will have a copy describing the resolution of the complaint.

Alameda County Homeless Management Information System (ACHMIS)

Data Quality Action Plan

Action Step Needed	Staff to be Involved	Staff Responsible	Timeline for action	Notes
Community Roll-out of Action Plan	John Noe	John Noe	January – March 2020	Will introduce Data Quality Report and Policies and Procedures to User Groups once approved by the CoC Committee.
Develop Agency Liaison role	Patrick Crosby, ACHMIS Administrator, will draft roles and responsibilities of an Agency Liaison	Oversight Committee (OC) will review, discuss, and finalize the Agency Liaison roles and responsibilities	December 2019 and January 2020	
Identify Agency Liaison	Agency Staff will identify an Agency Liaison and provide contact information to ACHMIS staff at HMISSupport@acgov.org; Agency Staff will identify replacements upon departure of a liaison	John Noe, ACHMIS DQ Lead, will develop and publish a roster of Agency Liaisons	February - March 2020	
Convene and Train Agency Liaisons	John Noe	John Noe	April 2020	Begin gathering of Liaisons for training on reports and expectations. Develop schedule for monthly meetings.

Alameda County Homeless Management Information System (ACHMIS)

Data Quality Action Plan

Action Step Needed	Staff to be Involved	Staff Responsible	Timeline for action	Notes
Generate Agency Data Quality (DQ) Reports	Agency Liaisons will generate the reports and ensure that they accurately reflect the agency's performance.	DQ Lead will collect and review reports	Beginning April 2020, continuing monthly as part of the Data Quality Meeting	
Identify agencies not meeting DQ standards	Agency Liaisons with measures that are out of tolerance will identify projects	DQ Lead will work with Liaisons to identify out of tolerance agencies	Monthly as preparation for User Group review	
Obtain explanation for not meeting DQ standards	Liaisons will provide explanations of issues causing non-compliance	DQ Lead will collect issues, analyze for trends and report to Oversight Committee (OC) as needed	Monthly as preparation for User Group review; Quarterly as preparation for OC review	
Identify plan to improve DQ	Liaison will develop a plan for improving DQ at the project level; may seek support from ACHMIS staff; identify training needs	DQ Lead will identify systemic issues; propose policy changes or clarifications; improve training curriculum; propose workflow changes or provide	Monthly bring change proposals to OC; provide process clarification to user community; emphasize workflow issues	

Action Step Needed	Staff to be Involved	Staff Responsible	Timeline for action	Notes
		process clarification	causing DQ problems Quarterly highlight improvements	
Identify technical support needs or retraining opportunities	Liaisons identify projects needing focused TA	DQ Lead provide or facilitate additional hands-on support to staff in coordination with Liaison	As needed Coordinated use of training facility; Hands-on facilitated training by ACHMIS staff; Supervised workflow compliance	Goal is to use proposed modularized Learning Management System tools to retrain aspects of workflow
Disseminate process improvement or process changes widely	Liaisons identify process issues needing improvement, suggest process changes	DQ Lead gather, synthesize, and present process recommendations to OC; OC consider changes and taken action to approve, deny, or postpone changes; DQ Lead process OC action and	Monthly User Group session will discuss recommendations to provide feedback to OC; OC will review, discuss, and take action on proposals; DQ Lead will incorporate	Resources will be updated and maintained on the HMIS Support Portal as identified on the ACHMIS website: http://acgov.org/cda/hcd/hmis/materials.htm

Action Step Needed	Staff to be Involved	Staff Responsible	Timeline for action	Notes
		publish process changes appropriately	changes into workflow training and publish revisions to the user community	
Publish system performance reports	Liaisons will prepare agency level reports, review reports, certify that they accurately reflect agency performance, and forward them to DQ Lead by deadlines; Liaisons will include their findings for areas out of tolerance	DQ Lead will prepare system-wide report, synthesize and incorporate agency findings, and provide reports to OC by deadlines	Quarterly OC will review system-wide reports highlighting areas of improvement and reviewing plans for improving areas out of tolerance	OC will determine at which point reports will be made public

MEMORANDUM

To: HMIS Oversight Committee
From: EveryOne Home Staff
Date: May 11, 2020
Re: Updating HMIS Release of Information (ROI)

QUESTIONS FOR DISCUSSION

Consider updating the Privacy Standards to expand flexibility in collecting PPI including allowing for:

- Digital signatures
- Verbal consent (if digital signatures are not possible)

BACKGROUND

Alameda County's HMIS developed privacy standards to comply with all applicable laws governing HMIS client privacy/confidentiality. Applicable standards include but are not limited to Federal Register Vol. 69. No. 146 (I IMIS FR 4848-N-02) -Federal statute governing HMIS information – Friday, July 30, 2004 and HIPAA.

With the COVID-19 pandemic, providers have needed to adjust intake procedures. As a result, it has become difficult to collect wet signatures from clients seeking services from the housing crisis response system.

Attached is the ROI used by Alameda County HMIS and an excerpt of the HUD HMIS Privacy and Security Standards relevant to updating the privacy standards. The HUD Privacy and Security Standards show the baseline requirements and "Additional Privacy Protections". Alameda County has chosen to implement a number of the "Additional Privacy Protections", as shown by the bolded text. For more information on how these standards are implemented, see the CoC Policies and Procedures.

What is HMIS and Why Should I Use It?

HMIS is a database system used to

- Coordinate efforts to help you obtain and maintain permanent housing
- Secure files electronically
- Ensure these projects continue receiving funding to keep them open
- Reduce the information you have to repeat and answer at multiple agencies

The HMIS system is used by many agencies throughout the county that provide services to homeless and low-income persons. A current list of participating health, housing, and human service agencies that provide housing-related supports is available at (acgov.org/cda/hcd/documents/roi_providers.pdf). HMIS data is used to assess your needs, track and improve services provided, and to match you to helpful resources based on priorities and standards established by the Alameda County HUD Continuum of Care (viewable at everyonehome.org).

When you request or receive services from a program participating in the Alameda County Continuum of Care, information collected about your household is entered into the HMIS system.

What information is shared about me?

My name, social security number, alias, date of birth, gender, race, ethnicity, veteran status, education, employment, if I have a disability, household relationships, living situation, income amount(s) and type, benefit(s) information, if I have health coverage and type, assessments, services needed and provided, and outcomes of services provided, including the name of the projects where I received services. Other information that might be collected (dependent on program) include income, non-cash benefits, health insurance, physical disability, developmental disability, chronic health condition, HIV/AIDS status, mental health, substance abuse, domestic violence, sexual orientation, etc. Additional information may include sharing of my photo and previously collected HMIS data.

Who can view and share information about me?

Information shared about me will ONLY be viewable by the participating agencies listed at (acgov.org/cda/hcd/documents/roi_providers.pdf). Each person or agency with access rights to the HMIS system must sign an agreement to maintain the security and confidentiality of client records.

Funders, cities, and other housing-related planning groups require HMIS to provide reports, which enable them to better understand the people-served, services provided and outcomes achieved. HMIS helps by pooling your data with others for these reports. This supports continued funding and improvement of services and housing projects for you and other homeless and low-income households. In addition, HMIS data is used for research purposes (including coordination with other systems of care), analysis about programs, specific service types, targeting of services, understanding best practices and improvements needed, or other uses to enhance the homeless and housing service delivery system. Keeping your information within the HMIS system helps us pool your data with others for these reports.

You have the right to receive a copy of all information collected about you and shared between the participating agencies. You may also amend and correct information collected about you that may be incorrect.

Client Name (Print): _____

Accompanying children: _____

(under the age of 18) _____

_____ I have received and reviewed the "What is HMIS and Why Should I Use It" information sheet.

(Initial Here)

Consent to share and view my data:

By signing below, I agree that program intake/exit and service information collected about me and my household can be shared among HMIS participating agencies for the purposes of helping me to obtain and maintain permanent housing.

- I understand that a regularly updated list of the agencies participating in HMIS is available at (acgov.org/cda/hcd/documents/roi_providers.pdf).

- I know that the agencies participating in the system (listed at acgov.org/cda/hcd/documents/roi_providers.pdf) must follow strict privacy laws regarding protection of electronic and paper records.
- I understand that this acknowledgement is valid for ten (10) years from the date that I sign this form.
- I understand that my name, date of birth, gender and Social Security Number are used to identify my record in the database.
- I understand that my photo may be shared in the system.
- I understand that my services and project data will be used in reporting and in research or analysis about programs, specific service types, targeting of services, or other uses to improve the homeless and housing service delivery system.

Signature of Client Date

Agency Representative Date

Agency Representative Printed Name

Alameda County HMIS

HUD HMIS Privacy and Security Standards- Summary Excerpt

NOTE:

The Alameda County-wide Homeless Continuum of Care Council has chosen to implement some of the "Additional Privacy Protections" listed in this document. Additional Privacy Protections with which participating agencies/jurisdictions are required to comply are bolded in this document

4.2. Privacy-Requirements

- All CHOs must comply with the baseline privacy requirements described here with respect to: data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability.
- A CHO may adopt additional substantive and procedural privacy protections that exceed the baseline requirements for each of these areas.
- A CHO must comply with federal, state and local laws that require additional confidentiality protections.
- All additional protections must be described in the CHO's privacy notice.
- A CHO must comply with all baseline privacy protections and with all additional privacy protections included in its privacy notice.
- A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PPI.
- When PPI is shared between organizations, responsibilities for privacy and security may reasonably be allocated between the organizations.
- Organizations sharing a common data storage medium and PPI may adopt differing privacy and security policies as they deem appropriate, administratively feasible, and consistent with these HMIS privacy and security standards, as long as these privacy and security policies allow for the unduplication of homeless clients at the CoC level.

4.2.1. Collection Limitation

Baseline Requirement.

- A CHO may collect PPI only when appropriate to the purposes for which the information is obtained or when required by law.
- A CHO must collect PPI by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.
- A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information.
- Consent of the individual for data collection may be inferred from the circumstances of the collection.
- Providers may use the following language to meet this standard:

  "We collect personal information directly from you for reasons that are discussed in our privacy statement. 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."

Additional Privacy Protections.

A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Restricting collection of personal data, other than required HMIS data elements;

(2) Collecting PPI only with the express knowledge or consent of the individual (unless required by law); and

(3) **Obtaining oral or written consent from the individual for the collection of personal information from the individual or from a third party.**

4.2.3. Purpose Specification and Use Limitation

Baseline Requirement

- A CHO must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures.
- A CHO may use or disclose PPI only if the use or disclosure is allowed by this standard and is described in its privacy notice.
- A CHO may infer consent for all uses and disclosures specified in the notice and for uses and disclosures determined by the CHO to be compatible with those specified in the notice.
- Except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards, all uses and disclosures are permissive and not mandatory.
- Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law.

Additional Privacy Protections.

A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Seeking either oral or written consent for some or all processing when individual consent for a use, disclosure or other form of processing is appropriate;

(2) Agreeing to additional restrictions on use or disclosure of an individual's PPI at the request of the individual if the request is reasonable. The CHO is bound by the agreement, except if inconsistent with legal requirements;

(3) Limiting uses and disclosures to those specified in its privacy notice and to other uses and disclosures that are necessary for those specified;

(4) Committing that PPI may not be disclosed directly or indirectly to any government agency (including a contractor or grantee of an agency) for inclusion in any national homeless database that contains personal protected information unless required by statute;

(5) Committing to maintain an audit trail containing the date, purpose and recipient of some or all disclosures of PPI;

(6) Committing to make audit trails of disclosures available to the homeless individual; and

(7) Limiting disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure.

4.2.4. Openness

Baseline Requirement.

- A CHO must publish a privacy notice describing its policies and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request.
- If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page.
- A CHO may, if appropriate, omit its street address from its privacy notice.
- A CHO must post a sign stating the availability of its privacy notice to any individual who requests a copy.
- A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. All amendments to the privacy notice must be consistent with the requirements of these privacy standards. A CHO must maintain permanent documentation of all privacy notice amendments.
- CHOs are reminded that they are obligated to provide reasonable accommodations for persons with disabilities throughout the data collection process. This may include but is not limited to, providing qualified sign language interpreters, readers or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability. See 24 CFR 8.6; 28 CFR 36.303. Note: This obligation does not apply to CHOs who do not receive federal financial assistance and who are also exempt from the requirements of Title Ill of the Americans with Disabilities Act because they qualify as "religious entities" under that Act.
- CHOs that are recipients of federal financial assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the program. See HUD Limited English Proficiency Recipient Guidance published on December 18, 2003 (68 FR 70968).

Additional Privacy Protections.

A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) making a reasonable effort to offer a copy of the privacy notice to each client at or around the time of data collection or at another appropriate time;

(2) giving a copy of its privacy notice to each client on or about the time of first data collection. If the first contact is over the telephone, the privacy notice may be provided at the first in-person contact (or by mail, if requested); and/ or

(3) adopting a policy for changing its privacy notice that includes advance notice of the change, consideration of public comments, and prospective application of changes.

4.2.5. Access and Correction

Baseline Requirement.

- A CHO must allow an individual to inspect and to have a copy of any PPI about the individual. A CHO must offer to explain any information that the individual may not understand.
- A CHO must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual.
- A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.
- In its privacy notice, a CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PPI:
  - (1) Information compiled in reasonable anticipation of litigation or comparable proceedings;
  - (2) information about another individual (other than a health care or homeless provider);
  - (3) information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or
  - (4) information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.
- A CHO can reject repeated or harassing requests for access or correction.
- A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

Additional Privacy Protections.

A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Accepting an appeal of a denial of access or correction by adopting its own appeal procedure and describing the procedure in its privacy notice;

(2) Limiting the grounds for denial of access by not stating a recognized basis for denial in its privacy notice;

(3) Allowing an individual whose request for correction has been denied to add to the individual's information a concise statement of disagreement. A CHO may agree to disclose the statement of disagreement whenever it discloses the disputed PPI to another person. These procedures must be described in the CHO's privacy notice; and/or

(4) Providing to an individual a written explanation of the reason for a denial of an individual's request for access or correction.

- A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices.
- A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

Additional Privacy Protections.

A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Requiring each member of its staff (including employees, volunteers, affiliates, contractors and associates) to undergo (annually or otherwise) formal training in privacy requirements;

(2) Establishing a method, such as an internal audit, for regularly reviewing compliance with its privacy policy;

(3) Establishing an internal or external appeal process for hearing an appeal of a privacy complaint or an appeal of a denial of access or correction rights; and/or

(4) Designating a chief privacy officer to supervise implementation of the CHO's privacy standards.

Security.

Baseline Requirement.

- A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PPI when the hard copy is in a public area.
- 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.