Privacy Policy

All Continuums of Care (CoC) are responsible for the oversight and operation of a Homeless Management Information System. The Oakland-Berkeley-Alameda County CoC recognizes its responsibility to safeguard the privacy of information collected about people experiencing homelessness. At the same time, the CA-502 CoC affirms its support for sharing HMIS data to facilitate and enhance care coordination, reimbursement for services, homeless system planning, and public knowledge of homelessness. This Policy describes standards for the privacy of personal information collected and stored in the HMIS and elsewhere in print or electronic formats within the CA-502 CoC network. The standards protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. This Policy is based on principles of fair information practices recognized by the information privacy and technology communities.

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

1 Definitions and Scope

1.1. Definitions

- **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.
- **Coordinated Entry:** A process developed to ensure that all people experiencing a housing crisis have fair and equal access and are quickly identified, assessed for, referred, and connected to housing and assistance based on their strengths and needs. In the CA-502 CoC, the HMIS is used to support coordinated entry.
- **Personally Identifiable Information (PII):** Any information maintained by or for a Covered Homeless Organization 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.

Privacy Policy

Set forth below is a non-exhaustive list of information that may constitute PII on its own or in combination with other information:

- Full name
- Home address
- Business Contact Information
- Personal email address
- Social security number
- Passport number
- Driver's license number
- Certificate number
- Credit card numbers
- Date of birth
- Telephone number
- Log in details
- Personnel number
- Vehicle identifier or serial number
- Photograph or video identifiable to an individual
- Biometric information
- Medical information
- Criminal history
- Other information related to an individual that may directly or indirectly identify that individual (e.g., salary, performance rating, purchase history, call history, etc.) [3]

- **Covered Homeless Organization (CHO):** Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, discloses or processes PII on clients at-risk of or experiencing homelessness. This definition includes both organizations that have direct access to the CA-502 CoC HMIS, as well as those formally partnering organizations who do not but do record, use, or process PII of target population clients.
- **Recording:** Activities internal to any given CHO that involve creating a hard copy or electronic record of data that includes PII.
- **Uses:** Activities internal to any given CHO that involves interaction with PII.
- **Disclosures:** Activities in which a CHO shares PII externally with other entities.
- **Compelled Disclosures:** Activities in which a CHO is legally compelled by law to share PII.
- **Processing:** 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.
- **Permitted Uses and Disclosures:** The uses and disclosures of PII that are allowed by this Policy, in alignment with the federal HUD HMIS Privacy Standards. [1]
- **Privacy Notice:** A consumer facing document maintained and published by each CHO that describes its policies and practices for the processing of PII.

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

Privacy Policy

1.2 Applying this Policy

This Policy applies to any CHO that records, uses, or processes personally identifiable information (PII) for the CA-502 CoC HMIS, except for HIPAA covered entities as noted below. All PII maintained by a CHO in print or electronic formats is subject to these standards.

Any CHO that is covered under the Health Insurance Portability and Accountability Act (HIPAA) is required to comply with HIPAA and is not required to comply with the privacy standards in this Policy if the CHO determines that a substantial portion of its PII about clients at-risk of or experiencing homelessness is protected health information as defined in the HIPAA rules. Exempting HIPAA-covered entities from this Policy's privacy standards avoids all possible conflicts between the two sets of rules.

This Policy gives precedence to the HIPAA privacy and security rules because:

1. The HIPAA rules are more finely attuned to the requirements of the health care system;
2. The HIPAA rules provide important privacy and security protections for protected health information; and
3. Requiring a CHO to comply with or reconcile two sets of rules would be an unreasonable burden.

It is possible that part of a CHO's operations may be covered by this Policy while another part is covered by the HIPAA standards. A CHO that, because of organizational structure, legal requirement, or other reason, maintains personal information about a client at-risk of or experiencing homelessness that does not fall under this Policy (e.g., the information is subject to the HIPAA health privacy rule) must describe that information in its privacy notice and explain the reason the information is not covered. The purpose of the disclosure requirement is to avoid giving the impression that all personal information will be protected under this Policy if other standards or if no standards apply. [2]

2 Allowable HMIS Uses and Disclosures of Personally Identifiable Information (PII)

2.1 Uses and Disclosures Requiring Written Consent

2.1.1 CA-502 CoC Information Sharing Authorization-Housing (ISA-H) form

A CHO processing PII for the purposes identified below must obtain written consent from the individual using the ISA-H form.

1. To provide or coordinate services for an individual or household;
2. For functions related to payment or reimbursement for such resources and services;
3. To carry out administrative functions, including but not limited to legal, audit, personnel, oversight, contractual obligations, and management functions; or
4. For creating deidentified PII.
5. For academic research purposes as described in Section 2.1.2
6. For any other purpose not described above or in Section 2.2.

2.1.2 Additional requirements regarding uses and disclosures for academic research purposes

A CHO may use or disclose PII for internal quality improvement or evaluation conducted by an individual or institution that has a formal relationship with the CHO if the analysis is conducted either:

- By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the CHO;
- By an institution for use in a research project conducted under a written research agreement approved in writing by the CoC Board.

A written research agreement must:

1. Establish rules and limitations for the processing and security of PII during the research;
2. Provide for the return or proper disposal of all PII at the conclusion of the research;

3. Restrict additional use or disclosure of PII, except where required by law; and
4. Require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board, or other applicable human subjects protection institution.

Any research/ evaluation on the nature and patterns of homelessness at the CA-502 CoC-wide level that uses PII HMIS data may be conducted only based on specific agreements between researchers and the entity that administers the HMIS. These agreements must be approved by the CA-502 CoC Board and must reflect adequate standards for the protection of data confidentiality.

2.2 Uses and Disclosures that Do Not Require Written Consent

CHOs, like other institutions that maintain personal information about individuals, have obligations that may transcend the privacy interests of clients. The following permitted uses and disclosures recognize those obligations to use or share personal information by balancing competing interests in a responsible way. These permitted uses and disclosures do not require the individual's written consent.

Per the 2004 HMIS Data and Technical Standards, HUD permits the following uses and disclosures of PII, provided that the uses and disclosures are listed in a CHO's privacy notice.

2.2.1 Uses and disclosures required by law

A CHO may use or disclose PII when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law. For example, information may need to be disclosed to the Department of Health and Human Services to make sure that a client's rights have not been violated.

2.2.2 Uses and disclosures to avert a serious threat to health or safety

A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PII if:

1. The CHO, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
2. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

2.2.3 Uses and disclosures about victims of abuse, neglect, or domestic violence

A CHO may disclose PII about an individual whom the CHO reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority (including a social service or protective services organization) authorized by law to receive reports of abuse, neglect, or domestic violence under the following circumstances:

1. Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law; or
2. If the individual agrees to the disclosure; or
3. To the extent that the disclosure is expressly authorized by statute or regulation; and the CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PII for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A CHO that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if:

1. The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
2. The CHO would be informing a personal representative (such as a family member or friend), and the CHO reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the CHO, in the exercise of professional judgment.

2.2.5 Disclosures for law enforcement purposes

A CHO may, consistent with applicable law and standards of ethical conduct, disclose PII for a law enforcement purpose to a law enforcement official under any of the following circumstances:

- In response to a lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial officer, or a grand jury subpoena;
- If the CHO believes in good faith that PII disclosure is necessary to report specified types of criminal conduct to law enforcement to seek remediation. This Policy allows for the disclosure of PII to report crimes that occurred on the CHO's premises (e.g., crimes that cause harm to the CHO's premises, personnel, participants served, or other members of the public). Examples of criminal conduct covered include assault or bodily harm of any type, harassment, credible threats of violence, theft, destruction of property, and manufacture/production or distribution of controlled substances on CHO premises. It is not intended to cover minor infractions such as personal possession or use of controlled substances, unless covered elsewhere in this Policy (i.e., Section 2.2.2).
- If the official is an authorized federal official seeking PII for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought. [3]

3 Privacy Requirements and Responsibilities

All CHOs involved with the CA-502 CoC HMIS must comply with the privacy requirements described here with respect to:

1. Data collection limitations;
2. Data quality;
3. Purpose and use limitations;
4. Openness;
5. Access and correction; and
6. Accountability.

A CHO must comply with federal, state, and local laws that require additional confidentiality protections. All additional protections must be described in the CHO's privacy notice. A CHO

must comply with all privacy protections in this Policy and with all additional privacy protections included in its privacy notice, where applicable.

A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PII. When PII is shared between organizations, responsibilities for privacy may reasonably be allocated between the organizations. Organizations sharing a common data storage medium and PII may adopt differing privacy policies as they deem appropriate, administratively feasible, and consistent with this Policy, which allows for the de-duplication of clients at-risk of or experiencing homelessness at the CoC level.[5] Those differing privacy policies may mean that one CHO has a more rigorous privacy standard, but each policy must, at minimum, meet and not contradict the privacy standards set forth herein. In addition, CHOs must maintain documentation regarding changes to their privacy policies.

3.1 Data Collection Limitation

A CHO may collect PII only when appropriate to the purposes for which the information is obtained or when required by law. A CHO must collect PII by lawful and fair means and, where appropriate, with the knowledge of the individual.

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

3.2 Data Quality

PII collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PII must be accurate, complete, and timely, as defined by the CA-502 Data Quality Monitoring Plan. A CHO must develop and implement a plan to dispose of, or remove identifiers from, PII that is not in current use seven years after the PII was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention). [5]

3.3 Purpose Specification and Use Limitation

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

A CHO processing PII for the purposes of the CA-502 CoC HMIS must agree to additional restrictions on the use or disclosure of the client's PII at the request of the client, where it is reasonable to do so. This may include, but is not limited to, using de-identified client information when coordinating services through the HMIS.

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

3.4 Openness

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

This Policy may be amended at any time and amendments may affect PII obtained by a CHO before the date of the change. An amendment to this Policy regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

CHOs are obligated to provide reasonable accommodations for persons with disabilities throughout the data collection process. This may include but is not limited to, providing qualified sign language interpreters, readers, or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability. See 24 CFR 8.6; 28 CFR 36.303. Note: This obligation does not apply to CHOs who do not receive federal financial assistance and who are also exempt from the requirements of Title III of the Americans with Disabilities Act because they qualify as ''religious entities'' under that Act.

In addition, CHOs that are recipients of federal financial assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the

program. See HUD Limited English Proficiency Recipient Guidance published on December 18, 2003 (68 FR 70968). [7]

3.5 Access and Correction

In general, a CHO must allow an individual to inspect and to have a copy of any PII about the individual. A CHO must offer to explain any information that the individual may not understand. A CHO must consider any request by an individual for correction of inaccurate or incomplete PII pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

A CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PII:

1. Information compiled in reasonable anticipation of litigation or comparable proceedings;

2. Information about another individual (other than a health care provider or CHO);

3. Information obtained under a promise of confidentiality (other than a promise from a health care or CHO) if disclosure would reveal the source of the information; or

4. Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual. A CHO can reject repeated or harassing requests for access or correction.

A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the PII about the individual. [8]

3.6 Accountability

A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors, and associates) to sign annually a confidentiality agreement that acknowledges receipt of a copy of the CHO's current privacy notice and that pledges to comply with the privacy notice. [9]

Privacy Policy

In the event of an unlawful privacy or security breach, CHOs are required to notify the HMIS team within three business days following the CA-502 CoC Incident Reporting process. The HMIS team will respond within 3 business days of receiving the notification. The HMIS team will provide a written response or corrective action plan as appropriate. Corrective actions may include notifying the consumer, downgrading system access, terminating user privileges, and disciplinary actions up to and including termination.

---

[1] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.1.1 pg. 45928

[2] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.1.2 pg. 45928

[3] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.1.3 pg. 45928-45929

[4] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.1.3 pg. 45929

[5] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.2 pg. 45929-45930

[6] Federal Register/Vol. 69. No. 146/Friday, July 30, 2004/Notices SEC. 4.2.3 pg. 45930

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

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

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

[Organization Logo]

Privacy Notice

In order to serve you, [Organization Name] may collect, use, and share your information. We have a responsibility to protect your information and privacy. This Privacy Notice summarizes our Privacy Policy.

What information do we collect?

We collect information that can be used to identify you, such as:

- Your name, address, date of birth.
- Contact information.
- Identification numbers.
- Photos or videos.
- Information about services you received.

When do we need your written consent?

We need your written consent before we can collect, use, or share your information to:

- Provide or coordinate services.
- Collect payments.
- Run the organization.
- Create data that can't identify you.
- Support research.
- Any other purpose not described below.

We can only collect, use, or share your information without your written consent to:

- Follow local, state, and federal laws.
- Keep you or others safe.
- Follow court orders, respond to threats, and ensure public safety.

What other steps do we take to protect your privacy?

In addition to following local, state, and federal laws, we will:

- Assist you if you need help or translation, as required by law.
- Explain and share this Privacy Notice and our Privacy Policy.
- Only collect the information we need.
- Have a plan for keeping information in good order and deleting old data.
- Share the least amount of information needed to complete a task.
- Allow you to review and correct your information and explain if your request is denied.
- Have a plan and train staff to handle questions, complaints, or a data breach.

Read our Privacy Policy online at [www.orgwebsiteaddress] or ask us for a printed copy.

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

Privacy Notice

For organizations in the Oakland-Berkeley-Alameda County Continuum of Care

In order to serve you, this organization may collect, use, and share your information. This organization has a responsibility to protect your information and privacy. This Privacy Notice summarizes this organization's Privacy Policy.

What information does this organization collect?

It collects information that can be used to identify you, such as:

- Your name, address, date of birth.
- Contact information.
- Identification numbers.
- Photos or videos.
- Information about services you received.

When does this organization need your written consent?

It needs your written consent before collecting, using, or sharing your information to:

- Provide or coordinate services.
- Collect payments.
- Run the organization.
- Create data that can't identify you.
- Support research.
- Any other purpose not described below.

It can only collect, use, or share your information without your written consent to:

- Follow local, state, and federal laws.
- Keep you or others safe.
- Follow court orders, respond to threats, and ensure public safety.

What other steps does this organization take to protect your privacy?

In addition to following local, state, and federal laws, it will:

- Assist you if you need help or translation, as required by law.
- Explain and share this Privacy Notice and its Privacy Policy.
- Only collect the information it needs.
- Have a plan for keeping information in good order and deleting old data.
- Share the least amount of information needed to complete a task.
- Allow you to review and correct your information and explain if your request is denied.
- Have a plan and train staff to handle questions, complaints, or a data breach.

Read this organization's Privacy Policy online at [www.orgwebsiteaddress] or ask a staff member for a printed copy.

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

Formatted

Each Covered Homeless Organizations (CHO) who participates in the CA-502 CoC must decide to adopt the CA-502 CoC Security Policy (Policy) in whole or adapt it to include stricter protections as necessary.

Organizations must also comply with federal, state, and local laws that require additional security protections, where applicable.

The following Policy recognizes the broad diversity of organizations that participate in the CA-502 CoC HMIS, and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some organizations (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. At a minimum, however, all organizations must meet the 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 organizations with additional needs or capacities

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

Updated 9/14/21

Oakland–Berkeley–Alameda County Continuum of Care (CA-502 CoC)
Homeless Management Information System (HMIS)

Security Policy

All Continuums of Care (CoCs) are responsible for the oversight and operation of a Homeless Management Information System. The Oakland-Berkeley-Alameda County CoC recognizes its responsibility to safeguard the security of information collected about people experiencing homelessness. At the same time, the CA-502 CoC affirms its support for sharing HMIS data to facilitate and enhance care coordination, reimbursement for services, homeless system planning, and public knowledge of homelessness. This Policy describes standards for the security of personal information collected and stored in the HMIS and elsewhere in print or electronic formats within the CA-502 CoC network. The standards seek to ensure the security of personal information. This Policy is based on principles of fair information practices recognized by the information security and technology communities.

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

1 Definitions and Scope

1.1 Definitions

- **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.
- **Coordinated Entry:** A process developed to ensure that all people experiencing a housing crisis have fair and equal access and are quickly identified, assessed for, referred, and connected to housing and assistance based on their strengths and needs. In the CA-502 CoC, the HMIS is used to support coordinated entry.
- **Personally Identifiable Information (PII):** Any information maintained by or for a Covered Homeless Organization about a client at-risk of or experiencing homelessness that: (1) identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

  Set forth below is a non-exhaustive list of information that may constitute PII on its own or in combination with other information:

Security Policy

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

- **Covered Homeless Organization (CHO):** Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, discloses or processes PII on clients at-risk of or experiencing homelessness for an HMIS. This definition includes both organizations that have direct access to the CA-502 CoC HMIS as well as those organizations who do not but do record, use, or process PII of target population clients.
- **Recording:** Activities internal to any given CHO that involve creating a hard copy or electronic record of data that includes PII.
- **Uses:** Activities internal to any given CHO that involves interaction with PII.
- **Disclosures:** Activities in which a CHO shares PII externally with other entities.
- **Processing:** Any operation or set of operations performed on PII, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission, and destruction of the information.

Security Policy

1.2 Applying this Policy

This Policy applies to any CHO that records, uses, or processes personally identifiable information (PII) for the CA-502 CoC HMIS, with the exception of HIPAA covered entities as noted below. All PII maintained by a CHO in print or electronic formats is subject to these standards.

Any CHO that is covered under the Health Insurance Portability and Accountability Act (HIPAA) is required to comply with HIPAA and is not required to comply with the security standards in this Policy if the CHO determines that a substantial portion of its PII about clients at-risk of or experiencing homelessness is protected health information as defined in the HIPAA rules. Exempting HIPAA-covered entities from this Policy's privacy standards avoids all possible conflicts between the two sets of rules.

This Policy gives precedence to the HIPAA privacy and security rules because:

1. The HIPAA rules are more finely attuned to the requirements of the health care system;
2. The HIPAA rules provide important privacy and security protections for protected health information; and
3. Requiring a CHO to comply with or reconcile two sets of rules would be an unreasonable burden.

It is possible that part of a CHO's operations may be covered by this Policy while another part is covered by the HIPAA standards. A CHO that, because of organizational structure, legal requirement, or other reason, maintains personal information about a client at-risk of or experiencing homelessness that does not fall under this Policy (e.g., the information is subject to the HIPAA health privacy rule) must describe that information in its privacy notice and explain the reason the information is not covered. The purpose of the disclosure requirement is to avoid giving the impression that all personal information will be protected under this Policy if other standards or if no standards apply. [2]

Security Policy

2 SYSTEM SECURITY

2.1 Applicability

A CHO must apply system security provisions to all the systems where PII is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini-computers, mainframes, and servers.

2.2 User Authentication

Each user accessing an electronic device that contains CA-502 CoC data must have a unique username and password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

- Using at least one number and one letter or symbol;
- Not using, or including, the username, the HMIS name, or the HMIS vendor's name; and / or
- Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location. Individual users must not log on to more than one workstation at a time or log on to the network at more than one location at a time.

2.3 Virus Protection

A CHO must protect the CA-502 CoC HMIS and any electronic device used to store PII by using available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the CA-502 CoC HMIS application is used and / or where PII is stored. A CHO must regularly update virus definitions from the software vendor.

2.4 Firewalls

Security Policy

A CHO must protect the CA-502 CoC HMIS and any electronic device used to store PII from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, so long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization.

For example, a laptop, which can be used to access the CA-502 CoC HMIS inside or outside the CHO, must be equipped with its own firewall.

2.5 Public Access

The CA-502 CoC HMIS and any electronic device used to store PII that use public forums for data collection or reporting must be secured to allow only connections from previously approved computers and systems through Public Key Infrastructure (PKI) certificates, or extranets that limit access based on the Internet Provider (IP) address, or similar means. A public forum includes systems with public access to any part of the computer through the Internet, modems, bulletin boards, public kiosks, or similar arenas.

2.6 Physical Access to Systems with Access to HMIS Data

A CHO must, at all times, staff computers stationed in public areas that are used to collect and store CA-502 CoC HMIS data. When workstations are not in use and staff are not present, steps must be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations must automatically turn on a password-protected screensaver when the workstation is temporarily not in use. Password-protected screensavers are a standard feature with most operating systems and the amount of time can be regulated by a CHO. If staff from a CHO will be gone for an extended period of time, staff must log off the data entry system and shut down the computer. A laptop should never be left unattended and should be secured with a lock when used.

2.7 Disaster Protection and Recovery

The CA-502 CoC HMIS data is copied on a regular basis to another medium (e.g., tape) and stored in a secure off-site location where the required security standards apply. The CHO that stores the data in a central server stores that central server in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors or equivalent modern

technology is used to protect systems used for collecting and storing all the CA-502 CoC HMIS data.

2.8 Disposal

In order to delete all CA-502 CoC HMIS data from a data storage medium (e.g. computer, phone, USB drive, CD), a CHO must reformat the storage medium. A CHO must reformat the storage medium more than once before reusing or disposing the medium. Prior to disposing of any data storage medium that contains, or may contain, CA-502 HMIS data, the CHO must take measures to render the data unrecoverable.

2.9 System Monitoring

A CHO must use appropriate methods to monitor security systems. Systems that have access to any CA-502 CoC HMIS data must maintain a user access log. Many new operating systems and web servers are equipped with access logs and some allow the computer to email the log information to a designated user, usually a system administrator. Logs must be checked routinely.

3 APPLICATION SECURITY

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

3.1 Applicability

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

3.2 User Authentication

A CHO must secure all electronic CA-502 CoC HMIS data with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least

Commented [LRCC1]: RJL: I don't know the proper place for this but a huge problem with HIPAA data is a lot of covered entities do not properly secure laptops which, as we know, is a primary method of storing sensitive data. People leave laptops unattended (e.g., vehicles), and this becomes a problem when theft occurs. This has become a significant focus of the Office for Civil Rights for HIPAA enforcement, and they have levied fines for improperly storing laptops.

While this is not a HIPAA-based policy, the concern about properly securing laptops is very real and I think it is worth calling this out in this policy.

Commented [jH2R1]: Per Patrick, "I have been looking into the policies to see what we say about physical security. The focus has been primarily on technical security to protect the data even if the hardware is compromised. The privacy training emphasizes supervising, securing or shredding client data. The same applies to hardware. If the hardware can't be supervised, it needs to be secured both physically and electronically. If they feel it is necessary to spell that out more specifically in the policy, maybe we should. Electronic security is the primary concern."

Seems like this could be integrated into 2.5 or 2.6. it looks like it's a gap in our MOU as well, which you can find in my email. Are you able to recommend language?

Commented [JH3R1]:

eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

- Using at least one number and one letter or symbol;
- Not using, or including, the username, the HMIS name, or the HMIS vendor's name; and
- Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time or be able to log on to the network at more than one location at a time.

3.3 Electronic Data Transmission

A CHO must encrypt all CA-502 CoC HMIS data that are electronically transmitted over the Internet, publicly accessible networks, or phone lines to current industry standards. Unencrypted data may be transmitted over secure direct connections between two systems. A secure direct connection is one that can only be accessed by users who have been authenticated on at least one of the systems involved and does not utilize any tertiary systems to transmit the data. A secure network would have secure direct connections.

3.4 Electronic Data Storage

A CHO must store all CA-502 CoC HMIS data in a binary, not text, format. A CHO that uses one of several common applications (e.g., Microsoft Access, Microsoft SQL Server, or Oracle) are already storing data in binary format and no other steps need to be taken.

4 HARD COPY SECURITY

This section provides standards for securing hard copy data.

Security Policy

4.1 Applicability

A CHO must secure (e.g. locked drawer or cabinet) any paper or other hard copy containing PII that is either generated by or for the CA-502 CoC HMIS, including, but not limited to reports, data entry forms, and case / client notes. Note: Many CHOs will require stricter policies such as double locking (e.g. locked drawer in a locked office) due to other regulations or funding requirements.

4.2 Security

A CHO must, at all times, supervise any paper or other hard copy generated by or for the CA-502 CoC HMIS that contains PII. When CHO staff are not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location.

(logo)
Oakland–Berkeley–Alameda County Continuum of Care
Information Sharing Authorization for Housing (ISA-H)

Authorization for Sharing Your Personally Identifiable Information

Client Name: _____ Date of Birth: _____

The organizations that make up Oakland–Berkeley–Alameda County Continuum of Care ("Organizations") are asking for your authorization to allow sharing of your protected personally identifiable information ("information"). If you agree, your information will be shared with (to and from) the Organizations and other providers that assist clients who are at-risk of or experiencing homelessness. This includes providers of the following types of services:

- Homeless assistance
- Housing service
- Medical
- Behavioral health
- Related software

Sharing information makes it easier to:

- Connect you with housing programs, services, or resources.
- Coordinate your shelter, housing, or other services.
- Limit the amount of information you need to repeat.
- Improve the quality of services.

Signing this Authorization Form ("Form") is your choice.

By signing this Form, you authorize your information to be shared with (to and from) the Organizations and types of providers shown above to:

- Provide or coordinate services.
- Collect payments.
- Run the organizations.
- Create data that can't identify you.
- Support research.

Draft designed to mirror HCSA Information Sharing Authorization form. Please send any **questions, concerns or other feedback** to *jessica@hanserdhealth.com* and SWarner@acgov.org .

Updated 9/14/21

(logo)
Oakland–Berkeley–Alameda County Continuum of Care
Information Sharing Authorization for Housing (ISA-H)

If you do not sign this Form, you can still receive some services. Not signing may keep you from being able to fully take part in certain programs.

What will be shared?

Information will be shared about programs and services you got in the past, get now and in the future. This includes data about shelter, housing, and related needs.

Information shared may include details that may directly or indirectly identify you, such as:

- Full name
- Home address
- Personal email address
- Social security number
- Passport number
- Driver's license number
- Date of birth
- Telephone number
- Medical information
- Criminal history
- Photos/ images

How will my information be shared?

Your information will be shared in electronic, verbal, and written formats.

Who will be sharing my information?

Your information will be shared with (to and from) the Organizations and the types of providers described above. This may also include organizations involved in providing services now, in the past, and in the future. A

list of the Organizations and providers can be accessed at (url).

What is still shared if I don't sign?

State and Federal laws already allow for some sharing of information. Signing this Form does not change what can be shared under these laws. For example, the Organizations can collect, store, use, and share your information to:

- Follow local, state, and federal laws.
- Keep you or others safe.
- Follow court orders, respond to threats, and ensure public safety.

What rules do Organizations need to follow?

In addition to following local, state, and federal laws, organizations will:

- Assist people who need help or translation, as required by law.
- Explain and share their Privacy Notice and Privacy Policy.
- Only collect the information they need.
- Have a plan for keeping information in good order and deleting old data.
- Share the least amount of information needed to complete a task.
- Allow you to review and correct your information and explain if your request is denied.
- Have a plan and train staff to handle questions, complaints, or a data breach.

(logo)
Oakland–Berkeley–Alameda County Continuum of Care
Information Sharing Authorization for Housing (ISA-H)

If I sign, can I change my mind later?

You have the right to change your mind about sharing and can revoke (take back) this authorization at any time. This form is valid for 5 years or until the date that you cancel or change it in writing.

- To cancel or make a change, talk with your Housing Provider. You can complete a new Form to reflect the change(s). Any changes will take effect as of the date the new Form is signed.
- Any data or information shared before that time cannot be recalled.

I have the right to:

- Refuse to sign this Form.
- Receive a copy of this Form.

By signing this Form I agree that:

- I have read this Form or a representative has read it to me.
- I understand it.
- I give authorization for my information to be shared as described above.
- This authorization will remain in effect for a period of 5 years, or until I change my authorization in writing. I can do this by contacting my Housing Provider.

[redacted]

Client Signature _____ Date _____

If signed by a person other than the client, please write that person's name and relationship to the client:

Representative's Name _____ Relationship to Client _____

Draft designed to mirror HCSA Information Sharing Authorization form. Please send any **questions, concerns or other feedback** to *jessica@hanserdhealth.com* and SWarner@acgov.org .

Updated 9/14/21