# Oakland–Berkeley–Alameda County Continuum of Care Homeless Management Information System

# Security Policy

## INTRODUCTION

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

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

HIPAA-covered entities may be exempt. CHOs must also comply with federal, state, and local laws that require additional security protections, where applicable.

The following policy recognizes the broad diversity of CHOs that participate in the HMIS, and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some CHOs (e.g., such as those serving victims of domestic violence, runaway youth, or persons with substance use disorder) must implement higher levels of security standards because of the nature of the clients they serve and/or service provisions. Others (e.g., large emergency shelters) may find higher standards overly burdensome or impractical. Unless exempt, CHOs must meet the minimum security standards described in the following policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for CHOs with additional needs or capacities.

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

# 1 Definitions and Scope

## 1.1 Definitions

- **Covered Homeless Organization (CHO):** Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, discloses or processes personal Identifiable Information (PII) on clients at-risk of or experiencing homelessness. This definition includes both organizations that have direct access to the HMIS, as well as those formally partnering organizations who do not but do record, use, or process PII of target population clients.

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

- **Homeless Management Information System (HMIS):** A local information technology system used to collect, store and report client-level information about individuals who are seeking services to resolve homelessness or the risk of homelessness.

  Sharing HMIS data enhances care coordination, while facilitating reimbursement for services, homeless system planning and improved public knowledge of homelessness. The HMIS system is designed to improve effectiveness and efficiency for clients, CHOs, provider agencies, jurisdictions, other systems of care, funders, and the community. Improved knowledge gained from HMIS about various communities with special needs and their service usage aides with providing a more effective and efficient service delivery system.

  CA-502 uses Clarity by BitFocus for its HMIS software.

- **Participating CHOs:** A list of CA-502 participating CHOs can be found at https://achmis.org/docs/forms/AC_HMIS_ROI_Providers20220610.pdf

- **Personally Identifiable Information (PII):** Any information maintained by or for a CHO about a client at-risk of or experiencing homelessness that: (1) identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual. Below is a

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.)

- **Privacy Notice:** A document maintained and published by each CHO that describes for clients its policies and practices for the processing of PII, the reasons for collecting information and uses and disclosures that are allowable. Consent may be assumed for uses and disclosures that are described as allowable in the Privacy Notice. The Privacy Notice must be posted at each intake desk (or comparable location) and on the CHO's public website.

- **Process:** Any operation or set of operations performed on PII, whether by automated means, including but not limited to collection, maintenance, use, disclosure, transmission, and destruction of the information.

- **Record:** Activities internal to any given CHO that involve creating a hard copy or electronic record of data that includes PII.

- **Use:** Activities internal to any given CHO that involves interaction with PII.

## 1.2 APPLYING THIS POLICY

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

Any CHO that is covered under the Health Insurance Portability and Accountability Act (HIPAA) is required to comply with HIPAA and is not required to comply with the

security standards in this policy if the CHO determines that a substantial portion of its PII about clients at-risk of or experiencing homelessness is protected health information as defined in the HIPAA rules. Exempting HIPAA-covered entities from this policy's privacy standards avoids all possible conflicts between the two sets of rules.

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

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

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

# 2 SYSTEM SECURITY

## 2.2 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 CoC data must have a unique username and password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

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

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

## 2.3 Virus Protection

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

## 2.4 Firewalls

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

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

## 2.5 Public Access

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

## 2.6 Physical Access to Systems with Access to HMIS Data

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

## 2.7 Disaster Protection and Recovery

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

## 2.8 Disposal

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

## 2.9 System Monitoring

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

# 3 Application Security

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

## 3.1 Disaster Protection and Recovery

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

## 3.2 Applicability

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

## 3.3 Electronic Data Transmission

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

## 3.4 Electronic Data Storage

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

# 4 Hard Copy Security

This section provides standards for securing hard copy data.

## 4.1 Applicability

A CHO must secure (e.g., locked drawer or cabinet) any paper or other hard copy containing PII that is either generated by or for the 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 always must supervise any paper or other hard copy generated by or for the HMIS that contains PII. When CHO staff are not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location.