SANTA CRUZ COUNTY
Housing for Health
PARTNERSHIP

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
Homeless Management Information System (HMIS) Security Policy

This Policy describes standards for the security of personally identifiable information collected and stored in the Watsonville/Santa Cruz City & County CoC HMIS. The standards seek to ensure the security of personal information. This Security Policy ("Policy") is based on principles of fair information practices recognized by the information security and technology communities and federal Housing and Urban Development (HUD) department HMIS guidance: (https://www.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf).

This Policy defines the security standards required of any organization within the CoC that records, uses, or processes personally identifiable information (PII) on consumers at-risk of or experiencing homelessness for HMIS. Organizations must also comply with federal, state, and local laws that require additional security protections, where applicable.

This Policy recognizes the broad diversity of organizations participating in 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, may choose to implement higher levels of security standards because of the nature of the consumers served or specific services provided. 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 this Policy. This approach provides a uniform *minimum standard* of data privacy and security protection for consumers at-risk of or experiencing homelessness with the possibility of more restrictive protections for organizations with additional needs or capacities.

The following sections discuss HMIS security standards.

I. HMIS Security Standards: Definitions

A. *Personally Identifiable Information (PII):* Any information maintained by or for a Covered Homeless Organization about a consumer 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.

B. *Covered Homeless Organization (CHO):* Any organization, including its employees, volunteers, affiliates, contractors, and associates, that records, uses, or processes PII on consumers at-risk of or experiencing homelessness for HMIS. This definition includes both organizations that have direct access to HMIS, as well as those organizations who do not, but do record, use, or process PII from HMIS.

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

II. Security Standards

This section describes the standards for system, application, and hard copy security. All CHOs must comply with these requirements.

System Security

A. *Equipment Security:* 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. A CHO must apply system security provisions to all systems where PII is stored, including, but not limited to, their networks, desktops, laptops, mini-computers, tablets, mobile phones, mainframes, and servers.

For CHOs using mobile devices, additional equipment security measures should be put in place for field-based use of devices. HMIS users should only use business rather than personal devices to access HMIS. Mobile devices should be encrypted. This functionality is built into the latest versions of both Android and iOS. Accessing HMIS should be done through a "Private" browsing window, e.g., an "incognito" window in Chrome, or changing the browser's settings to not store form data (aka "autofill") or page caching (not possible on all pages). Devices should enable remote device or profile management by CHO IT administrators. Both iOS and Android include functionality that allow you to locate and, if necessary, wipe lost or compromised devices. Mobile devices should use a built-in cellular connection or a cellular wifi hotspot with an encrypted connection. Public wifi hotspots should NOT be used for connecting to HMIS. A VPN connection should be used to help improve the security of the connection when possible.

B. *User Authentication:* Each user accessing a machine that contains HMIS 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:

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

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 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.

C. *Virus Protection*: A CHO must protect HMIS and any electronic device used to store PII from viruses by using commercially 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 housed. A CHO must regularly update virus definitions from the software vendor.

D. *Firewalls:* A CHO must protect 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 workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall so long as the server has a firewall. Firewalls are commonly included with all new operating systems. Older operating systems can be equipped with secure firewalls that are available both commercially and for free on the internet.

E. *Public Access:* 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.

F. *Physical Access to Systems with Access to HMIS Data:* A CHO must always 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 should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. Workstations temporarily not in use should automatically turn on a password-protected screensaver. 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 should log off the data entry system and shut down the computer.

G. *Disaster Protection and Recovery:* HMIS data should be copied on a regular basis to another medium and stored in a secure off-site location where the required security standards apply. A CHO that stores the data (Bitfocus) on a central server must have servers located in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors are used to protect systems used for collecting and storing all the HMIS data.

H. *Disposal:* To delete all HMIS data from a data storage medium, a CHO must reformat the storage medium. A CHO should reformat the storage medium more than once before reusing or disposing the medium.

I. *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.

Application Security

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

B. *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. The current standard is 128-bit encryption. 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.

C. *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.

Hard Copy Security

A. *Applicability:* A CHO must secure any paper or other hard copy containing PII that is either generated by or for HMIS, including, but not limited to reports, data entry forms, and case/consumer notes. Hard copies should be stored in a locked and secure file cabinet in an area not accessible to non-CHO staff.

B. *Security:* A CHO must, always, supervise any paper or other hard copy generated by or for HMIS that contains PII 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.