SANTA CRUZ COUNTY
Housing for Health
PARTNERSHIP

WATSONVILLE/SANTA CRUZ CITY & COUNTY CONTINUUM OF CARE (COC)

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

Policies and Procedures

Table of Contents

I. INTRODUCTION

The Watsonville/Santa Cruz City & County Continuum of Care's (CoC) Covered Homeless Organizations (CHOs) utilize a computerized record-keeping system that captures information about people experiencing or at-risk of homelessness called the Watsonville/Santa Cruz City & County CoC Homeless Management Information System (Watsonville/Santa Cruz CoC HMIS). The CoC uses HMIS data to improve housing and services quality; identify patterns and monitor trends over time; conduct needs assessments and prioritize services and housing resources for subpopulations experiencing or at-risk of homelessness; enhance inter-agency coordination; and monitor and report on the delivery, impact, and quality of housing and services. HMIS creates an unduplicated count of individuals and households at-risk of or experiencing homelessness and develops aggregate information that assists in developing policies and programs to end homelessness. In addition, the Watsonville/Santa Cruz CoC HMIS allows CHOs to share information electronically about consumers, including their service needs, to better coordinate services and housing.

The lead administrative entity for the CoC is the County of Santa Cruz Human Services Department Housing for Health Division (H4H). Bitfocus is the current Watsonville/Santa Cruz CoC HMIS Software as a Service (SaaS) vendor, serves as the HMIS administrator, and works to make the system an effective tool for all CHOs.

Aggregated, anonymous data from the Watsonville/Santa Cruz CoC HMIS is used to generate reports for federal, state, and local funders. HMIS is also used to produce reports for the annual Point-in-Time (PIT) count, Longitudinal System Analysis (LSA), the Annual Homeless Assessment Report (AHAR), Annual Performance Reports (APRs), System Performance Measures (SPMs), California's Homeless Data Integration System (HDIS), and other required reports provided to federal, state, and local funders.

Effective implementation of the Watsonville/Santa Cruz CoC HMIS can benefit individuals and families at-risk of or experiencing homelessness, CHOs, public policy planners, and the community. This document provides an overview of current policies, procedures, guidelines, and standards that govern Watsonville/Santa Cruz CoC HMIS operations, as well as the responsibilities for CHOs and HMIS End Users. The Appendices provide specific applicable policies.

II. GOVERNING PRINCIPLES

Described below are the overall governing principles upon which all decisions pertaining to the Watsonville/Santa Cruz CoC HMIS are based. Agencies, programs, and individual users are expected to read, understand, and adhere to the spirit of these principles, especially when written policies and procedures do not provide specific direction. The CoC policy board determines and reaffirms on an annual basis the selection of the HMIS vendor and system administrator, as well as the CoC administrative entity that oversees the HMIS vendor and system administration. The CoC operations committee proposes updates to HMIS policies, procedures, and forms on an annual and as needed basis that are ratified by the CoC Policy Board.

A. Confidentiality

The rights and privileges of consumers are crucial to the success of HMIS. These policies will ensure consumers' privacy without impacting the delivery and coordination of services and housing resources, which are the primary focus of programs participating in HMIS.

Policies regarding consumer data are founded on the premise that a consumer owns their own personal information; these policies aim to provide the necessary safeguards to protect consumer, agency, and policy level interests. Collection, access, and disclosure of consumer data through HMIS is only permitted by the procedures set forth in this document.

B. Data Integrity

Consumer data is the most valuable and sensitive asset of the Watsonville/Santa Cruz CoC HMIS. These policies ensure integrity and protect this asset from accidental or intentional unauthorized modification, destruction, or disclosure.

C. System Availability

The availability of a centralized data repository is necessary to achieve the service, housing, and outcome goals desired for people experiencing or at risk of homelessness, H4H, CHOs, and the CoC. The CoC and the HMIS vendor and Administrator are responsible for ensuring the broadest deployment and availability of the HMIS data system towards capturing collective efforts to address homelessness in Santa Cruz County given available resources.

III. HMIS BENEFITS

Use of the Watsonville/Santa Cruz CoC HMIS can provide numerous benefits for persons at-risk of or experiencing homelessness, H4H, CHOs, and the CoC.

Benefits for persons at-risk of or experiencing homelessness:

- Intake information and needs assessments are maintained, reducing the number of times persons at-risk of, or experiencing homelessness must repeat their stories to multiple staff members or CHOs
- Supports the coordination of services a and streamlines referrals within and among CHOs to ensure consumers are matched to available services and housing resources to end their housing crisis as quickly as possible
- Ensures consumer confidentiality by entering in and maintaining information in a secured system

Benefits for H4H, CHOs and the CoC:

- Provides online, real-time information regarding consumer needs, as well as available services and housing resources for persons at-risk of or experiencing homelessness
- Ensures consumer confidentiality by providing a secured system to help CHOs avoid data breaches and misuse of HMIS data
- Decreases duplicative consumer intakes and assessments
- Tracks consumer outcomes and service and housing history
- Generates data reports for local, state, and federal reporting requirements
- Facilitates the coordination of services and housing resources within and among CHOs
- Assists in defining and understanding the extent of homelessness throughout the CoC
- Supports evaluations of the effectiveness of specific interventions and projects and services and housing provided
- Supports the development of data-informed solutions to reduce and end homelessness

IV. ROLES AND RESPONSIBILITIES

A. Housing for Health Partnership – Policy Board

- Initial selection and annual confirmation of HMIS administrator and vendor
- Annual review and approval of HMIS policies and procedures and associated forms
- Approval of funding for HMIS when the funding source requires CoC approval

B. Housing for Health Partnership – Operations Committee

- Project direction, guidance, participation, and feedback
- Recommend changes to HMIS policies and procedures

- Advise on funding strategies
- Review of performance metrics, data quality, and compliance issues

C. Housing for Health Division – CoC Administrative Entity

- CHO oversight, coordination, and liaison for use of HMIS
- Development and maintenance of HMIS policies and procedures and related forms and documentation
- End user license monitoring
- Data quality and performance metrics monitoring

D. HMIS Vendor and System Administrator - Bitfocus

- Maintenance of Watsonville/Santa Cruz CoC HMIS website
- Central Server Administration
    - Server security, configuration, and availability
    - Setup and maintenance of hardware
    - Configuration of network and security layers
    - Anti-virus protection for server configuration
    - System backup and disaster recovery
    - User administration and license management
    - System uptime and performance monitoring
- Adherence to HUD Data Standards
- Maintain list of all Partner Agencies and make it available to the public including posting it on the Watsonville/Santa Cruz CoC HMIS portal
- Aggregate data reporting and extraction
- Watsonville/Santa Cruz CoC HMIS Help Desk
- HMIS training
- Data breach reporting to H4H
- Liaison with HUD on required federal data collection and reporting standards and expectations

E. Covered Homeless Organizations (CHOs)

1. CHO Executive Director

- Authorizing agent for Organization Partnership and Data Sharing Agreement
    - Designation of CHO HMIS Primary Contact
    - Ensuring agency compliance with HMIS policies & procedures

2. CHO HMIS Primary Contact

- Designated and primary liaison with H4H and Bitfocus on HMIS
- Request new user ID and licenses from HMIS vendor on behalf of CHO
- Maintain agency/program data in HMIS application
- End user adherence to privacy and security policies
- Ensure data breach reporting to HMIS vendor
- First level end user support
- Ensure compliance with most current HMIS policies and forms
- Ensure quality of HMIS data collection and entry by CHO staff/end users

3. CHO Staff/End User

- Sign the Watsonville/Santa Cruz CoC HMIS User Agreement and complete required Watsonville/Santa Cruz CoC HMIS training for staff/end users
- Take appropriate measures to prevent unauthorized data disclosure
- Report all privacy and/or security violations to HMIS lead
- Comply with relevant policies and procedures
- Collection and input of required data fields in a consistent, accurate, and timely manner
- Ensure a minimum standard of data quality by accurately answering the Universal Data Elements (UDE) and required program-specific data elements for every person whose information is entered into the Watsonville/Santa Cruz CoC HMIS
- Inform consumers about the CHO and CoC's use of the Watsonville/Santa Cruz CoC HMIS
- Take responsibility for any actions undertaken with one's username and password

F. HMIS License Availability and Access

CHOs may request end user licenses at any time from the HMIS vendor. H4H is informed when a CHO requests an end user license and determines whether to grant the request, based upon licenses available, licenses already assigned to the CHO, HMIS data requirements associated with the applicable program and its funding, CHO staff and data management capacity and need, and funding available. The CoC reserves the right to change the license acquisition and allocation process based upon CoC funding availability. H4H staff may bring HMIS access issues and questions to the CoC operations board for resolution if needed. Participating agencies and licensed users must comply with HMIS privacy and security standards and other established policies and procedures.

H4H in partnership with the CoC policy board establishes the number of available HMIS user licenses on a fiscal year basis with the development of an annual HMIS program budget. Increasing the number of available user licenses typically requires an HMIS budget augmentation that requires a minimum of 90 days to implement. H4H and HMIS vendor staff review HMIS licensed user activity on a quarterly basis and determine if adjustments to licensure status are necessary. In alignment with the HMIS policy that requires program participant data updates at least every 90 days, the HMIS vendor will notify users that do not access the system within a 90-day period that their access may be terminated.

Prioritized access to HMIS user licenses will be given to agencies and programs receiving federal or state funding that require HMIS participation, those that have contracts with H4H, or those with Central California Alliance for Health community supportive services housing contracts. CHOs that are eligible to be granted HMIS access must be able to meet the insurance and other contractual requirements associated with receiving funding from one or more of the above sources. Agencies and programs that fall in the priority groups listed above AND that provide services to underserved or disparately impacted groups will be given priority access to limited HMIS user licenses in times of budgetary constraints limiting available user licenses.

HMIS user licenses are available to CHO staff that provide direct services to participants of HMIS specific programs to document participant profiles, enrollments and exits, assessments, status updates, and service provision. HMIS licenses are not provided for view only purposes. Prioritized agencies and programs will be encouraged and supported to have all direct service staff utilize HMIS within their programs. In general, CHOs should have no more than one manager and data analysis license per program for running and using regular data quality reports at least every 90 days.

V. REQUIREMENTS FOR PARTICIPATION

A. CHO General Requirements

The following are the requirements for participating CHOs. Non-compliance with any of the requirements may result in loss of access to HMIS.

1. Participation Agreement Documents

CHOs must complete the following documents:

- *Organization Partnership and Data Sharing Agreement*: Must be signed by each participating CHO's Executive Director. The Organization Partnership and Data

Sharing Agreement (see Appendix C) states the CHO's commitment to adhere to the policies and procedures for effective use of the Watsonville/Santa Cruz CoC HMIS.

- *HMIS User Agreement and Code of Ethics*: Details the HMIS User policies and responsibilities and is signed by each authorized end user prior to receiving an HMIS user license and annually thereafter.

2. Assign HMIS Agency Primary Contact

- The CHO shall designate a primary HMIS agency contact who will be responsible for communications regarding Watsonville/Santa Cruz CoC HMIS throughout the CHO, including with individual End Users. The CHO shall ensure the HMIS vendor is notified of any changes to the HMIS Primary Contact's name and contact information.
- The HMIS vendor will maintain a list of all designated HMIS Primary Contacts.

3. End User Access

- All potential end users must undergo a background check completed by the CHO, as detailed in the Organization Partnership and Data Sharing Agreement (see Appendix C). Individuals with a history of data fraud, identity theft, or misuse of confidential information, as well as any individuals under investigation for such issues, shall not be permitted an HMIS user license.
- End users must be paid staff, official volunteers, or contracted staff with a CHO. An official volunteer must complete a volunteer application with the CHO, undergo required HMIS user trainings, meet the background requirements as described above, and record volunteer hours with the CHO. The CHO must assume all responsibility/liability for actions of contracted staff or official volunteer(s).
- All end users must be at least 18 years old.
- The CHO HMIS Primary Contact will submit a request for new end user access to HMIS vendor. Each HMIS end user must have their own username and password to access the system.
- Prior to the end user gaining access to HMIS, H4H will assess the operational security of the user's workspace and confirm the workstation has virus protection properly installed and that a full-system scan has been performed within the last week.
- All end users must complete all required Watsonville/Santa Cruz CoC HMIS trainings before system access is granted (see below). All end users shall commit to abide by the governing principles of the Watsonville/Santa Cruz CoC HMIS and adhere to the terms and conditions of the HMIS User Agreement and Code of Ethics (see Appendix I).

B. CHO Training Requirements

1. New User Training

- All end users are required to attend a new end user privacy and security training and basic HMIS system training with HMIS vendor prior to receiving access to the system.
- Upon their first log in to the Watsonville/Santa Cruz CoC HMIS, end users must sign a confidentiality agreement that acknowledges they received and pledge to comply with the HMIS Privacy Policy (see Appendix E). All electronically signed new user agreements are stored in the HMIS system.
- Users must complete all required trainings and pass a knowledge-based quiz prior to gaining HMIS access.

2. Ongoing Training

- All end users are required to attend annual privacy trainings to retain their Watsonville/Santa Cruz CoC HMIS license. The annual training will include re-signing the user agreement and passing a knowledge-based quiz.
- HMIS vendor will provide regular trainings for the CHOs; specialized trainings can be provided when necessary. Refer to the HMIS website (Santa Cruz HMIS Home (bitfocus.com)) for the latest training and support schedule.

C. CHO Security Requirements

1. System Security

- *Equipment Security*. A CHO must apply security provisions to all systems where Personally Identifiable Information (PII) is stored, including, but not limited to, networks, desktops, laptops, mini-computers, tablets, mobile phones, mainframes, and servers. PII is any information about an individual which can be used to distinguish, trace, or determine their identity, including personal information like name, address, date of birth or social security number.

  Additional equipment security measures should be put in place for field-based use of mobile devices. HMIS users should only use business, and not 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, changing the browser's settings to not store form data (aka "autofill") or page caching when possible. Devices should enable remote device

or profile management by CHO IT administrators. Both iOS and Android include functionality that allow location and, if necessary, wipe lost or compromised devices. Mobile devices should use a built-in cellular connection or Wi-Fi hotspot with an encrypted connection. Public Wi-Fi 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.

- *User Authentication*. Each user accessing a machine that contains HMIS data must have a unique username and password that cannot be used by or shared with others. 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, HMIS name, vendor's name, or any of these spelled backwards.
  - Not consisting entirely of any word found in the common dictionary.

  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 to the network from more than one location at a time.
- *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.
- *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 located outside of the organization, including the Internet and other computer networks.
  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.
- *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. The CHO must maintain a fixed Internet Protocol (IP) address.

- *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 accessible by unauthorized individuals. A password-protected screensaver should be automatically turned on when a workstation is temporarily not in use for longer than five minutes. Password-protected screensavers are a standard feature with most operating systems; the amount of time can be regulated by a CHO. When leaving their workstation for more than five minutes, CHO staff should log off the data entry system and shut down the computer.
- *Disaster Protection and Recovery*. The HMIS Service Administrator copies HMIS data on a regular basis to another medium and stores this data in a secure off-site location where the required security standards apply. The data is stored in a central server in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors are used to protect systems used for collecting and storing the HMIS data.
- *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.
- *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; some allow the computer to email the log information to a designated user, usually a system administrator. Logs must be checked routinely to ensure only appropriate individuals are accessing and utilizing the data. The CHO HMIS Lead is responsible for communicating to end users' proper workstation configuration and the importance of protecting access to HMIS data among all CHO users.

2. Application Security

- *Applicability*. A CHO must apply application security provisions to the HMIS software during data entry, storage, review, and all other processing functions.

- *User Authentication*. A CHO must secure all electronic HMIS data with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements are noted earlier in C. CHO Security Requirements.
- *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 has secure direct connections.
- *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.

3. Hard Copy Security

- *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/client notes. Hard copies should be stored in a locked and secure file cabinet in an area not accessible to non-CHO staff.
- *Security*. In public areas a CHO must always supervise any paper or other hard copy generated by or for HMIS that contains PII, including by name list reports used to coordinate prioritization and referrals of participants to resources. 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.

D. CHO Violation of HMIS Operating Policies

Compliance with these Policies and Procedures is mandatory for participation in the Watsonville/Santa Cruz CoC HMIS system.

1. Violation of the Policies and Procedures

Violation of the policies and procedures contained within this document may have serious consequences.

- Any deliberate or unintentional action resulting in a breach of confidentiality or loss of data integrity will result in the withdrawal of system access for the offending individual.
- All such actions, either intentional or unintentional, must be reported to the HMIS vendor and H4H for review and resolution via data breach reporting requirements.

2. HMIS Data Misuse and Breach Reporting

A breach is defined as any of the following:

- An incident involving unsecured PII, if that PII was, or is reasonably believed to have been accessed or acquired by an unauthorized person.
- A suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII in violation of signed agreements.

Breaches must be reported using HMIS Data Misuse and Breach Incident Reporting form (see Appendix J). Send completed form to santacruz@bitfocus.com.

VI. PRIVACY

A. Consumer Acknowledgement of Privacy Practices

CHO staff are responsible for explaining the CoC's privacy practices to all consumers prior to entering their information into the Watsonville/Santa Cruz CoC HMIS. Specific responsibilities include:

- Ensure that an HMIS Consumer Notice is posted or available at any location consumer intake services are provided and personally identifiable information (PII) is entered into HMIS. Field based workers should have a copy of the notice available for review in the field.
- Provide consumers with a copy of the CoC Consumer Notice.
- Request the consumer sign an HMIS Consumer Information Sharing Authorization form and upload the signed document into HMIS. If a consumer refuses to sign the form, staff should sign the document and indicate the reasons the consumer refused to sign the document. Consumer requests for limiting HMIS data collection and entry should be honored and respected given that HMIS data collection is based on consumer self-report. Staff should enter the maximum amount of data into HMIS approved by the consumer. Staff can remove PII for a given client, i.e., name, date of birth, and social security number, if desired. *Anonymous data is preferable to no data collection.*

- Ensure the HMIS Consumer Information Sharing Authorization form is current and signed at least once every three years.

If a consumer is hesitant to sign the Acknowledgement, CHO staff should explain the benefits and value of HMIS participation to the consumer using strategies learned in the HMIS vendor provided training and briefly summarized in the Approaches to Responding to Consumer Concerns About Data Sharing (see Appendix K) found at Santa Cruz HMIS Home (bitfocus.com). The consumer can request limitations on the sharing of their information.

B. Allowable HMIS Uses and Disclosures of Consumer Information

A CHO may use or disclose Personally Identifiable Information (PII) from the Santa Cruz County HMIS under the following circumstances:

- To provide or coordinate services for an individual or household related to keeping or finding a permanent home including coordinated entry activities.
- Functions related to payment or reimbursement for services and housing provided.
- To carry out administrative and planning functions, including but not limited to legal, audit, personnel, oversight, required state and federal reporting, and management functions.
- For creating deidentified PII.

CHOs, like other institutions that maintain personal information about individuals, have obligations that may transcend the privacy interests of consumers. The following additional uses and disclosures recognize those obligations to use or share personal information by balancing competing interests in a responsible and limited way. Under this Policy, these additional uses and disclosures are allowed but not required.

A CHO may use or disclose PII from the Santa Cruz County HMIS under the following special circumstances:

- 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.

- 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:
  - 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
- The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

- 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:
  - Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law
  - If the individual agrees to the disclosure
  - 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:
  - The CHO, in the exercise of professional judgment, believes informing the individual would place the individual or other individuals at risk of serious harm or
  - 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.

- Uses and Disclosures for Academic Research or Evaluation Purposes. Any research or evaluation on the nature and patterns of homelessness that uses PII HMIS data will take place only based on specific agreements between researchers and the HMIS lead agency, H4H. These agreements must be approved by H4H staff according to

guidelines approved by the H4H Partnership Policy Board and must reflect adequate standards for the protection of confidential data.

Provided H4H staff approves, a CHO may use or disclose PII for its own program for academic research or evaluation conducted by an individual or institution that has a formal contractual relationship with the CHO if the research/evaluation is conducted either:

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

A written research/evaluation agreement must:

- Establish rules and limitations for the processing and security of PII during the research/evaluation
- Provide for the return or proper disposal of all PII at the conclusion of the research/evaluation
- Restrict additional use or disclosure of PII, except where required by law and
- Require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

A written research/evaluation agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board, or other applicable human subject protection institution. Such approval of a proposed research project may be required for some proposed uses of HMIS data. H4H staff in consultation with the H4H Partnership Policy Board will make this determination.

- Disclosure for Law Enforcement Purposes. A CHO may, consistent with applicable law and standards of ethical conduct, disclose PII for the following law enforcement purposes:
  - Legal processes and otherwise required by law
  - Limited information requests for identification and location purposes
  - Pertaining to victims of crime

- Suspicion that death has occurred because of criminal conduct
- If a crime occurs on the premises of the CHO
- Medical emergency, not on CHO's premises, when it is likely that a crime has occurred.

C. Use of a Comparable Database by Victim Services Providers

Victim services providers, private nonprofit agencies whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking, must not directly enter or provide personally identifying information in the Watsonville/Santa Cruz CoC HMIS if they are legally prohibited from participating in a HMIS. Victim service providers that are recipients of funds requiring participation in the HMIS but are prohibited from entering data in an HMIS, must use a comparable database to enter consumer information. A comparable database is a database that can be used to collect consumer-level data over time and generate unduplicated aggregated reports based on the consumer information entered into the database. The reports generated by a comparable database must be accurate and provide the same information as the reports generated by the Watsonville/Santa Cruz CoC HMIS.

D. End User Conflict of Interest

End users with records in the Watsonville/Santa Cruz CoC HMIS are prohibited from entering or editing information in their own record. All end users are prohibited from entering or editing information in records of individuals with whom they have familial or personal relationships. All end users must sign the Watsonville/Santa Cruz CoC HMIS End User Agreement, which includes a statement describing this limitation, and report any potential conflict of interest to their Program Director or Executive Director. H4H may run the audit trail report to determine if there has been a violation of the conflict-of-interest agreement.

VII. DATA QUALITY

Data quality is a term that refers to the reliability and validity of consumer-level data in HMIS. It is measured by the extent to which data in the system represents authentic characteristics within a community. With good data quality, the Watsonville/Santa Cruz CoC can provide a full and accurate picture of the individuals and families accessing local housing and homelessness response system resources.

Data quality can be measured by data completeness, the extent to which all expected data elements are entered for all consumers; data timeliness, the amount of time that passes between data collection and entry into HMIS, data consistency, the degree to which users enter data consistently and without contradiction across all programs in HMIS; and data accuracy, the extent to which data are entered accurately and consistently.

A. Data Completeness

Complete HMIS data is necessary to fully understand the demographic characteristics and service and housing resource use of persons with information in HMIS and to identify ways to improve services. Complete data facilitates confident reporting and analysis of the experience of homelessness in the CoC region. Data is considered complete if ALL consumers are entered into HMIS and all required data elements are captured.

The CoC's goal is to collect 100% of all data elements; however, it recognizes that this may not be possible in all cases. HUD HMIS data standards expect no null (missing) data for required data elements, and "Don't Know" or "Refused" or "Other" responses should not exceed 5%.

A null or missing rate of below 5 percent represents an ideal goal, and the CoC should work toward accomplishing this level of data completeness for all programs. For large-scale night-by-night shelters, alternate targets for data completeness will be considered based on past performance.

B. Data Accuracy

Data should be entered accurately into HMIS. Accuracy depends on the consumer's ability to provide the data and staff's ability to accurately enter the data in HMIS. Although HMIS data accuracy can be hard to assess, CHOs should conduct a brief audit or review of active consumer records monthly. The audit should check that data recorded in the consumer file matches data recorded in HMIS (e.g., entry and exit dates, household type, demographic characteristics, and history of homelessness) and that consumer data is in alignment with project characteristics (e.g., a family is not entered in a program for single adult men).

C. Data Consistency

Data consistency refers to all data entry staff understanding, collecting, and entering data consistently across all programs in HMIS. Data consistency requires data entry staff to have a common understanding of each data element, its response categories, and meaning. To

facilitate data consistency, H4H in partnership with the HMIS vendor will ensure the availability of trainings and materials that outline basic data elements, response categories, rationale, and definitions.

D. Data Timeliness

Entering data into HMIS in a timely manner is important because it facilitates up-to-date information for resource availability, allows data to be accessible when needed (service planning for people experiencing homelessness, monitoring or funding purposes, or for responding to requests for information), and reduces human error that occurs when too much time elapses between the provision of a service (data collection) and data entry. Expectations regarding timely data entry by project type are provided in the Data Quality and Improvement Process and Plan (see Appendix H) and can be found at Santa Cruz HMIS Home (bitfocus.com). To ensure that system-wide data is as accurate as possible, all Universal Data Elements and Program-specific Data Elements should be entered according to the standards outlined in Data Quality and Improvement Process and Plan (see Appendix H).

In addition to timely data entry, the CoC requires that CHO staff follow the expectations for conducting assessments as follows:

- Current Living Situation assessments are used to document the housing status during the first interaction with each consumer, and any subsequent consumer interactions if their housing situation changed. All consumers with an active/open HMIS enrollment that experience a significant status change in income, employment, non-cash benefits, living situation, or other key characteristics require an Update Assessment to be completed within 30 days of learning of the status change. At a minimum, the Current Living Situation and Update Assessments for each active consumer must be completed every 90 days even if there are no changes to document. This approach ensures consistency in data collection and reporting on the status of consumers in the system. For audit purposes, Current Living Situation and Update Assessments are considered timely if they were completed 30 days prior to or after the quarterly update date or within the 60-day window.

- All HMIS enrollments that are active/open require an annual assessment within 30 days of consumers' annual project start anniversary date (30 days prior to or after the anniversary date or within the 60-day window).

VIII. TECHNICAL SUPPORT

Technical Support is an important component of the success of an HMIS system. The Watsonville/Santa Cruz CoC's HMIS vendor is available to provide Technical Support quickly and professionally. Requests for Technical Support may include support in addressing HMIS Software problems, requests for HMIS enhancements, or other general Technical Support.

The online Watsonville/Santa Cruz CoC HMIS Help Desk can be accessed at Santa Cruz HMIS Home (bitfocus.com) and is operated by Bitfocus, the System Administrator. The Help Desk can also be reached Monday through Friday, 8am to 5pm, except County holidays by email at santacruz@bitfocus.com or by phone at 831.713.2288.

IX. GLOSSARY

Aggregated Public Data: Data that is published and available publicly. This type of data does not identify individual consumers.

Confidential Data: Information that contains personally identifiable information.

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 an HMIS. This definition includes both organizations that have direct access to the Watsonville/Santa Cruz CoC HMIS data system, as well as those organizations who do not have direct access but record, use, or process PII.

End User: An individual at a CHO who has an end user license to enter data into the Watsonville/Santa Cruz CoC HMIS.

HMIS System Administrator: The Watsonville/Santa Cruz CoC HMIS system administrator is Bitfocus. Bitfocus designs the Watsonville/Santa Cruz CoC HMIS, provides ongoing support to the HMIS Lead Agency, and is the vendor for the HMIS software product called Clarity.

Housing for Health (H4H): Division of the County of Santa Cruz Human Services Department that serves as the HMIS Lead Agency for the CoC.

Minimum Data Entry Standards: A mandatory set of data elements that must be collected and entered into the Watsonville/Santa Cruz CoC HMIS for each consumer served by participating projects. These standards include both the Universal Data Elements (UDEs) and Program-Specific Data Elements (PSDEs).

Personally Identifiable Information (PII): Any information maintained by or for a CHO 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.

Santa Cruz County Privacy Policy: The Policy that governs allowable uses and disclosures of personally identifiable information for the purposes of the Watsonville/Santa Cruz CoC HMIS.

Santa Cruz CoC Security Policy: The Policy that governs how equipment used to access the Watsonville/Santa Cruz CoC HMIS must be protected from misuse, a breach, or a violation of personally identifiable information.

Watsonville/Santa Cruz CoC HMIS: A web-based database that is used by homeless service organizations across the Watsonville/Santa Cruz CoC to record and store consumer-level information on the characteristics and needs of persons at-risk of or experiencing homelessness.

Shared Data: Unrestricted information entered by one CHO and visible to another CHO using the Watsonville/Santa Cruz CoC HMIS. Shared data also includes data disclosed from the Watsonville/Santa Cruz CoC HMIS for purposes laid out in the Privacy Policy.

Unpublished Restricted Access Data: Information scheduled, but not yet approved, for publication.

Victim Services Provider: A nonprofit organization whose primary mission is to provide services to victims and survivors of domestic violence, dating violence, sexual assault, or stalking.

APPENDIX A: HMIS CONSUMER INFORMATION SHARING AUTHORIZATION FORM

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
HMIS CONSUMER INFORMATION SHARING AUTHORIZATION FORM

This Organization participates in the Housing for Health Partnership (Watsonville/Santa Cruz City & County) CoC Homeless Management Information System (Watsonville/Santa Cruz CoC HMIS).

The Watsonville/Santa Cruz CoC HMIS is used to collect basic information about consumers receiving services from this and other Organizations. This helps: 1) Local Organizations get a more accurate count of individuals and families experiencing or at-risk of homelessness; 2) Identify the need for different services and housing resources in the community; 3) Connect individuals and families at-risk of or experiencing homelessness to the services and housing resources they need; and 4) Secure funding from agencies that request this data as a funding requirement.

The CoC and participating Organizations only collect information that is considered appropriate and necessary. The collection and use of all personal information are guided by strict standards of privacy and security. Every person and agency that is authorized to read or enter information into the HMIS database has signed an agreement to maintain the security and confidentiality of every consumer.

The Protected Personal Information (PPI) and other general information gathered may include, but is not limited, to the following:

Name	Program Start/End Dates	Domestic Violence
Date of Birth	Housing History	Legal History
Social Security Number	Employment Status	Substance Abuse*
Gender	Family Composition	Mental Health*
Ethnicity and Race	Veteran Status	Photo (if applicable)
Zip Code of Last Permanent Address	Medical history and conditions*	

*My information, especially my medical, mental health, and substance abuse history, cannot be released outside of the HMIS provider network without my further written consent, unless otherwise allowed by the regulations.

By signing this Authorization Form, I understand the following:

- This consent will be valid for 3 years from the date listed below.
- My Protected Personal Information (PPI) is protected by federal, state, and local laws governing confidentiality.
- I may sign this consent form, but I have the right to agree to share only certain or specific information upon my request.
- I may receive services, even if I do not sign this consent form. Providers may not refuse to provide me with services based on my refusal to sign this form, nor will it affect my eligibility for benefits or other supports.
- I may receive a copy of this consent form and the CoC Privacy Policy upon request.
- I have the right to review and receive a copy of my HMIS record, to correct my

record, or file a statement of disagreement at any time.
- I may revoke (withdraw) this Consent at any time, but I must do so in writing or by using the Revocation Form. Upon revocation, the CoC will remove my PPI from the HMIS database, but information and data previously obtained cannot be removed entirely.

I have the right to file a grievance against any organization whether I signed this consent or not if I think my privacy rights have been violated. The Grievance Form must be made available or provided to me upon request.

This Organization may use or disclose information without permission from the Watsonville/Santa Cruz CoC HMIS under the following circumstances:

- To provide or coordinate services and housing resources for an individual or families
- For functions related to payment or reimbursement for services or housing resources
- To carry out administrative functions
- When required by law, including a court order
- For research and/or evaluation purposes
- For creating de-identified (anonymous) data

Please note HMIS policies and laws may change over time and effect the use of data retroactively.

SIGNATURE AND ACKNOWLEDGEMENT OF THE HMIS CONSUMER INFORMATION SHARING AUTHORIZATION FORM

By signing this consent form, I authorize the HMIS participating organizations and their representatives to share Protected Personal Information regarding myself and/or my family members for the purposes of assessing my/our needs for housing, utilities, assistance, food, counseling, and/or other supportive services. I have read (or been read) this Consumer Authorization Form, have had the opportunity to ask questions and receive answers to my questions, and I freely consent to having my information (and of any children) entered into the HMIS database.

I acknowledge that I have received a copy of the HMIS Consumer Authorization Form of the Housing for Health Partnership CoC.

_____	OR	_____
Consumer Name (Please Print)		Name of Personal Representative
_____		_____
Consumer Signature		Signature of Personal Representative
_____		_____
Date		Relationship to Consumer
		_____
		Date

Program Use Only

1. I attempted to obtain written authorization of the Consumer Information Sharing Authorization Form, but acknowledgement could not be obtained because:
   ☐ An emergency prevented us from obtaining authorization

   ☐ A communication barrier prevented us from obtaining authorization

   ☐ The individual was unwilling to sign

   ☐ The interaction was completed over the phone or remotely and verbal authorization was obtained; written authorization will be obtained as soon as possible.

   ☐ Other: _____

2. The consumer requested the following data sharing limitations:
   Check one or more of the following requested limits:

   ☐ De-identified or anonymized data

   ☐ Limited responses to some questions

_____ _____

Staff Member Printed Name Staff Member Signature

_____

Date

Note to Staff: For instances when the consumer requests limitations to their data, please ensure a signed copy of this form is uploaded into HMIS ***prior to*** entering consumer information in HMIS. When client does not consent to have any information shared in HMIS and no profile is created, please save physical signed document in a secure location.

APPENDIX B: CONSUMER NOTICE

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
HMIS CONSUMER NOTICE

This Organization provides services for individuals and families at-risk of or experiencing homelessness. This Organization participates in the Housing for Health Partnership (Watsonville/Santa Cruz City & County) CoC Homeless Management Information System (Watsonville/Santa Cruz CoC HMIS).

The Watsonville/Santa Cruz CoC HMIS is used to collect basic information about consumers receiving services from this Organization. This helps the Organization get a more accurate count of individuals and families experiencing homelessness and identify the need for services and housing resources. The information also helps to connect individuals and families at-risk of or experiencing homelessness to the services and housing resources they need.

This Organization only collects information that is considered appropriate and necessary. The collection and use of all personal information are guided by strict standards of privacy and security. HMIS policies may change over time and effect the use of data retroactively.

This Organization may use or disclose information from the Watsonville/Santa Cruz CoC HMIS under the following circumstances:

- To provide or coordinate services and housing resources for an individual or family
- For functions related to payment or reimbursement for services or housing resources
- To carry out administrative functions
- When required by law
- For research and/or evaluation
- For creating de-identified (anonymous) data

A copy of the Watsonville/Santa Cruz City & County CoC Privacy Policy, describing allowable uses and disclosures of data collected for the purposes of the Watsonville/Santa Cruz CoC HMIS is available to all consumers upon request.

APPENDIX C: ORGANIZATION PARTNERSHIP & DATA SHARING AGREEMENT

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
Homeless Management Information System (HMIS)
Organization Partnership and Data Sharing Agreement

I. Purpose

The Watsonville/Santa Cruz City & County CoC's Covered Homeless Organizations (CHOs) utilize a computerized record-keeping system that captures information about people experiencing or at-risk of homelessness. The Watsonville/Santa Cruz City & County CoC Homeless Management Information System (Watsonville/Santa Cruz CoC HMIS) creates an unduplicated count of individuals and households at-risk of or experiencing homelessness and develops aggregate information that assists in developing policies to end homelessness. In addition, the Watsonville/Santa Cruz CoC HMIS allows CHOs to share information electronically about consumers, including their service needs, to better coordinate services.

II. Definition of Terms

The lead entity for the CoC implementation of HMIS is the County of Santa Cruz Human Services Department Housing for Health Division (H4H) and the system is administered by Bitfocus, the "HMIS System Administrator." In this Agreement, H4H is the "CoC HMIS Administrative Entity", "Covered Homeless Organization (CHO)" is an organization participating in HMIS, "Consumer" is a consumer of services, "Personally Identifiable Information (PII)" is information 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.

III. Audience and Agreement

This organizational partnership and data sharing agreement ("Agreement") permits the CHO listed below and its approved and designated users to access HMIS on their business computers and system through an internet connection. The HMIS users are the guardians entrusted with personal data to be entered and used in the HMIS on behalf of consumers. The CoC HMIS Administrative Entity has a primary function to manage the HMIS in partnership with its contracted HMIS System Administrator.

Prioritized access to HMIS user licenses will be given to agencies and programs receiving federal or state funding that require HMIS participation, those that have contracts with H4H, or those with Central California Alliance for Health community supportive services housing contracts. To qualify as an HMIS using agency, agencies must be able to meet the insurance and other contractual requirements associated with receiving funding from one or more of the above public funding sources.

PII is shared between and among CHOs that have established this Agreement with the CoC HMIS Administrative Entity. All CHOs granted access to HMIS must agree to abide by all relevant federal and state laws, and the CoC adopted HMIS Policies and Procedures pertaining to client confidentiality, user conduct, security, and the ongoing functionality and stability of services and equipment used to support HMIS.

A list of current organizations covered by this Agreement can be found at https://santacruz.bitfocus/participating-agencies. Please note that this list is updated over time.

The signature of the Executive Director or authorized designee of the CHO indicates agreement with the terms set forth for an HMIS account for the CHO.

IV. CHO HMIS General Responsibilities

The CHO is responsible for ensuring that its users comply with the requirements laid out in the CoC Privacy Policy and the CoC Security Policy. The CHO shall ensure that all staff issued a User ID and password for HMIS will comply with the following:

A. Read and abide by this Organization Partnership Agreement
B. Read and abide by the Santa Cruz County HMIS Policies and Procedures
C. Read and sign the Santa Cruz County HMIS User Agreement and Code of Ethics
D. Participate in new user privacy and security training and on-going security trainings on an annual basis
E. Participate in additional trainings as required by the Santa Cruz County HMIS Administrative Entity
F. Maintain a unique User ID and password, and not share or reveal that information to anyone

The CHO shall conduct background checks on all staff before referring potential users to attend a new user training and onboarding process. Individuals with a history of perpetrating fraud, identity theft, or misuse of confidential information, as well as any individual who is under investigation for such issues, shall not be permitted a user license.

The CHO is responsible for ensuring that its staff do not misuse the HMIS. Such misuses include and are not limited to: damage of computing resources, obtaining unauthorized resources, taking resources from another user, gaining unauthorized access to resources, or otherwise using computing resources without proper authorization.

Any user who finds a possible security lapse on the system is obligated to report it to the HMIS System Administrator immediately. They will notify the Watsonville/Santa Cruz CoC HMIS Help Desk, reach by phone at 831.713.2288, immediately of any breach, use, or disclosure of PII not provided for by this Agreement or the CoC Privacy Policy. Within one business day, the HMIS System Administrator will submit a completed HMIS Data Misuse and Breach Reporting form to: santacruz@bitfocus.com.

V. CHO Confidentiality and Informed Consent Responsibilities

The CHO agrees to abide by and uphold all privacy protection standards established for HMIS as well as their respective CHO's privacy and security procedures. The CHO will uphold relevant federal and state confidentiality regulations and laws protecting consumer records and information. The CHO will only release CHO consumer records outside of the HMIS provider network with written consent from the consumer, or the consumer's guardian, unless otherwise provided for in the HMIS policies and procedures and relevant federal and state laws. Access to HMIS is granted to the CHO listed below based on the following premises:

Oral Explanation: All consumers will be provided an oral explanation stating their information will be entered into a computerized record keeping system. The CHO will provide an oral explanation of the HMIS, informing consumers of how their information will be used, stored, and shared. The CHO is responsible for ensuring this procedure takes place prior to entering consumer PII into HMIS. The CHO shall arrange for a qualified interpreter or translator if an individual is not literate in English or has difficulty understanding the CoC Privacy Policy.

Written Explanation: Each consumer with PII information entered in HMIS should receive a copy of the HMIS consumer notice explaining HMIS and how HMIS data is used and shared. Consumers should sign an acknowledgement of receiving this information and a copy of this signed acknowledgement should be uploaded into the consumer's HMIS file.

Information Release: The CHO agrees not to release PII to any organization outside of participating HMIS CHOs without proper client consent except as provided by federal and state law or in circumstances outlined in the HMIS Privacy Policy.

Postings: The CHO must post a copy of the HMIS consumer notice at each intake desk or comparable location. Copies of notices must be made available to consumers upon their request.

VI. CHO Data Management Responsibilities

A. The CHO shall use the system to provide or coordinate services, link consumers with housing resources, develop reports and provide data, or conduct program evaluation, research, and improvement activities. PII will only be used and disclosed in accordance with the CoC HMIS Privacy Policy.
B. The CHO understands that all consumer data will be maintained on a remote, central server, which will contain all consumer information in an encrypted state. All PII is inaccessible to unauthorized users.
C. CHOs are bound by all restrictions placed upon the data by request from the consumer. The CHO shall diligently record in HMIS all consumer restrictions requested.
D. The CHO shall not knowingly enter false or misleading data under any circumstances.
E. The CHO shall maintain appropriate documentation of receipt of the HMIS Consumer Notice and Acknowledgement; this Acknowledgement must be updated every (3) three years.
F. The CHO shall consistently enter information into the HMIS database and will strive for real-time data entry. Data must be entered into the HMIS database within two business days, as outlined by the Santa Cruz Data Quality Improvement Process and Plan.
G. The CHO will not alter information in the HMIS database that is entered by another CHO with inaccurate information, i.e., CHO will not purposefully enter inaccurate information to over-ride information entered by another CHO.
H. The CHO shall not include profanity or offensive language in the HMIS database. This does not apply to the input of direct quotes by the consumer if the Organization believes that it is essential to enter these comments for assessment, service, and treatment purposes.
I. The CHO shall utilize the HMIS database for business purposes only.

J. The CHO shall not use the HMIS database with intent to defraud federal, state, or local governments, individuals, or entities, or to conduct any illegal activity.
K. The CHO may make aggregate data without PII available to other entities for funding or planning purposes pertaining to providing services to persons experiencing or at-risk of homelessness.
L. Once a report containing PII is downloaded from HMIS, it is the responsibility of the CHO to ensure the appropriate security protections of this data.
M. Consumers have the right to request information regarding to whom their PII is released in the Watsonville/Santa Cruz City & County CoC's CHOs.
N. The CHO will resist, through judicial proceedings, any judicial or quasi-judicial effort to obtain access to PII pertaining to consumers, unless expressly provided for in state and/or federal regulations.
O. CHOs will notify County H4H staff of their intent to terminate their participation in this Agreement.

VII. CoC HMIS Administrative Entity Rights

The CoC HMIS Administrative Entity reserves all rights, including HMIS system audit access, termination of agreements, of the HMIS application and the service resources that it owns and/or operates on behalf of the CoC. These procedures shall not be construed as a waiver of any rights of the CoC HMIS Administrative Entity or the CHO, nor shall they conflict with applicable acts of law.

VIII. Violations

An individual violating any of the guidelines outlined in this agreement will be reported immediately upon discovery. Such suspected violations will be confidentially reported to the CoC HMIS Administrative Entity or the HMIS System Administrator as outlined in the HMIS Policies and Procedures.

If this Agreement is terminated, the Watsonville/Santa Cruz City & County CoC shall maintain the right to the use of all consumer data previously entered by the terminating CHO; this use is subject to any restrictions laid out in the CoC Privacy Policy.

VIII. Agreement Terms and Conditions

A. No party shall transfer or assign any rights or obligations without the written consent of the other party.
B. This Agreement shall be in-force until revoked in writing by either party provided funding is available.
C. This Agreement may be terminated with 30 days written notice.
D. A violation of the above will result in immediate disciplinary action by the Watsonville/Santa Cruz City & County CoC.

HMIS - Organization Partnership and Data Sharing Agreement Signatory Page

This Agreement is executed between the CHO listed below, the CoC HMIS Administrative Entity, and the HMIS System Administrator. The Executive Director or authorized signatory for each entity will sign this Agreement.

I have read this HMIS Organization Partnership and Data Sharing Agreement and commit to ensuring staff from our CHO will utilize HMIS in accordance with the HMIS Policies and Procedures.

CHO Executive Director or Designee Signature	Date
CHO Executive Director or Designee Printed Name	Organization Name
CoC HMIS System Administrator Signature	Date
CoC HMIS System Administrator Printed Name	Organization Name
CoC HMIS System Administrative Entity Signature	Date
CoC HMIS System Administrative Entity Printed Name	Organization Name

APPENDIX D: PARTICIPATING COVERED HOMELESS ORGANIZATIONS

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
Interorganizational Data Sharing
Participating Covered Homeless Organizations

The following organizations have signed a CoC Interorganizational Data Sharing and Coordinated Services Agreement to use and disclose consumer-level information through the Watsonville/Santa Cruz City & County CoC Homeless Management Information System (Watsonville/Santa Cruz CoC HMIS) for the purposes of coordinating and providing services to consumers. Please note that this list of Organizations may change over time.

Abode Services
Association of Faith Communities
Bill Wilson Center
Cabrillo College
City of Santa Cruz
Covenant House
Community Action Board of Santa Cruz County
Downtown Streets Team
Encompass Community Services
Families In Transition
Front Street Housing, Inc.
Housing Authority of the County of Santa Cruz
Housing Matters
Nation's Finest
Pajaro Valley Shelter Services
Salvation Army
Santa Cruz County Health Services Agency
Santa Cruz County Human Services Department
Siena House
US Department of Veterans Affairs
Wings Homeless Advocacy

Consumer personally identifiable information (PII) is bound by strict confidentiality, through the CoC Privacy Policy and CoC Consumer Notice.

APPENDIX E: PRIVACY POLICY

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

This Policy describes standards for the privacy of personally identifiable information (PII) collected and stored in the Watsonville/Santa Cruz City & County CoC HMIS. The standards seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data that support efforts to prevent and end homelessness countywide. This HMIS Privacy Policy (hereinafter referred to as "Policy") is based on principles of fair information practices recognized by the information privacy 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 privacy standards required of any organization within the CoC that records, uses, or processes PII on consumers at-risk of or experiencing homelessness for the Watsonville/Santa Cruz CoC HMIS. Organizations must also comply with federal, state, and local laws that require additional confidentiality 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 privacy 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 privacy standards described in this Policy. This Policy 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 the Watsonville/Santa Cruz CoC HMIS privacy standards.

I. Watsonville/Santa Cruz CoC HMIS Privacy Standards: Definition of Terms

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 have direct access 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.
D. *Watsonville/Santa Cruz CoC HMIS Uses and Disclosures:* The uses and disclosures of PII that are allowed by this Policy.
E. *Uses and Disclosures:* Uses are those activities internal to any given CHO that involves interaction with PII, whereas disclosures are those activities in which a CHO shares PII externally with non-CHO entities.

II. Applying the Watsonville/Santa Cruz CoC HMIS Privacy Policy

This Policy applies to any Covered Homeless Organization (CHO) that records, uses, or processes personally identifiable information (PII) for the Watsonville/Santa Cruz CoC HMIS. All PII maintained by a CHO is subject to these standards.

III. Allowable HMIS and Coordinated Entry System (CES) Uses and Disclosures of PII

Consumer consent for any uses and disclosures defined in this section is assumed when organizations follow HUD HMIS Standards for notifying consumers of privacy policies. See Appendix E.1. for specific policy associated with Runaway and Homeless Youth (RHY) programs and services.

A CHO may use or disclose PII from the Watsonville/Santa Cruz CoC HMIS under the following circumstances:

A. To provide or coordinate services for an individual or household related to assistance with keeping or finding a permanent home.
B. For functions related to payment or reimbursement for services.
C. To carry out administrative and planning functions, including but not limited to legal, audit, personnel, oversight, required state and federal reporting, as well as management functions.
D. For creating deidentified PII. CHOs, like other institutions that maintain personal information about individuals, have obligations that may transcend the privacy interests of consumers. The following additional uses and disclosures recognize those obligations to use or share personal information by balancing competing interests in a responsible and limited way. Under this Policy, these additional uses and disclosures are permissive and not mandatory except for first party access to information and any required disclosures for oversight of compliance with this Policy. However, nothing in this Policy modifies an obligation under applicable law to use or disclose personal information.

A CHO may also use or disclose PII from the Watsonville/Santa Cruz CoC HMIS under the following special circumstances:

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.

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:

A. 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.

B. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

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:

A. Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law.

B. If the individual agrees to the disclosure.

C. 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:

A. The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm.

B. 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.

Uses and Disclosures for Academic Research or Evaluation Purposes

Any research or evaluation on the nature and patterns of homelessness that uses PII HMIS data will take place only based on specific agreements between researchers and the HMIS lead agency, the Housing for Health Division of the County of Santa Cruz Human Services Department. These agreements must be approved by the Housing for Health (H4H) Partnership staff members according to guidelines approved by the H4H Partnership (CoC) Policy Board and must reflect adequate standards for the protection of confidential data.

Provided H4H approves, a CHO may use or disclose PII from its own program for academic research or evaluation conducted by an individual or institution that has a formal relationship with the CHO if the research/evaluation is conducted either:

A. By an individual employed by or affiliated with the organization for use in a research/evaluation project conducted under a written research/evaluation agreement approved in writing by a program administrator, other than the individual conducting the research or evaluation, designated by the CHO; or
B. By an institution for use in a research or evaluation project conducted under a written research or evaluation agreement approved in writing by a program administrator designated by the CHO.

A written research or evaluation agreement must:

A. Establish rules and limitations for the processing and security of PII in the course of the research or evaluation.
B. Provide for the return or proper disposal of all PII at the conclusion of the research or evaluation.
C. Restrict additional use or disclosure of PII, except where required by law; and
D. Require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

A written research or evaluation 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.

Disclosure for Law Enforcement Purposes. A CHO may, consistent with applicable law and standards of ethical conduct, disclose PII for the following law enforcement purposes:

A. Legal processes and otherwise required by law.
B. Limited information requests for identification and location purposes.
C. Pertaining to victims of crime.
D. Suspicion that death has occurred as a result of criminal conduct.
E. If a crime occurs on the premises of the CHO.
F. Medical emergency, not on CHO's premises, and it is likely that a crime has occurred.

IV. Privacy Requirements

All CHOs involved with the Watsonville/Santa Cruz CoC HMIS must comply with the privacy requirements described in this Notice with respect to:

A. Data collection limitations
B. Data quality
C. Purpose and use limitations
D. Openness
E. Access and correction
F. 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 Notice and with all additional privacy protections included in its organization specific 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 consumers at-risk of or experiencing homelessness at the CoC level.

Data Collection Limitations

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 that explains generally the reasons for collecting this information (Watsonville/Santa Cruz City & County CoC Consumer Notice). Consent of the individual for data collection may be assumed when the Watsonville/Santa Cruz City & County CoC Consumer Notice is made available to each consumer prior to data collection, a consumer acknowledges receipt of the Notice via a signed acknowledgement form, and the notice is properly displayed and made available according to this Policy.

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 should be accurate, complete, and timely, as defined by the Santa Cruz County Data Quality Improvement Process and Plan. A CHO must develop and implement a plan to dispose of, or remove identifiers from, PII that is not in current use after the PII was created or last changed unless a statutory, regulatory, contractual, or other requirement mandates longer retention.

Purpose and Use Limitations

A CHO may use or disclose PII only if the use or disclosure is allowed by this Policy. A CHO may assume consent for all uses and disclosures specified in this Policy and for uses and disclosures determined by the CHO to be compatible with those specified in this Policy. This Policy limits the disclosure of PII to the minimum information necessary to accomplish the purpose of the disclosure. Uses and disclosures not specified in this Notice can be made only with the consent of the consumer or when required by law.

A CHO processing PII for the purposes of the Watsonville/Santa Cruz CoC HMIS will agree to additional restrictions on the use or disclosure of the consumer's PII at the request of the consumer, where it is reasonable to do so. This can include, but is not limited to, the following additional restrictions:

A. Entering consumer PII into the Watsonville/Santa Cruz CoC HMIS so that it is not shared with any other CHO.
B. Using de-identified consumer information when coordinating services through HMIS.
C. Limiting responses to HMIS questions to those the consumer is willing to share with other CHOs.

A CHO, in the exercise of professional judgment, will communicate with a consumer who has requested additional restrictions, when it is reasonable to agree to these and alternatives in situations where it is not reasonable.

Openness

A CHO must adhere to this Policy describing its practices for the processing of PII and must provide a copy of this Policy to any individual upon request. A CHO must physically post the HMIS CoC Consumer Notice stating the availability of this Policy 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)].

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:

A. Information compiled in reasonable anticipation of litigation or comparable proceedings.
B. Information about another individual other than a health care or homeless provider would be compromised.
C. 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.
D. 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.

Accountability

A CHO must establish a procedure for collecting questions or complaints about this Policy to share with Housing for Health, the HMIS lead agency. Housing for Health requires each HMIS user, including employees, volunteers, affiliates, contractors, and associates, to sign a confidentiality agreement that acknowledges receipt of a copy of this Policy and that pledges to comply with this Policy. Users must complete a Privacy Training and pass a knowledge-based quiz prior to granting them HMIS access. This training must be completed annually.

Appendix E.1

This appendix addresses special considerations for Runaway and Homeless Youth (RHY) Program service providers, per the RHY Program HMIS Manual.

I. No Consent Required for Data Collection

Data collection is the process of collecting and entering information into the Watsonville/Santa Cruz CoC HMIS by RHY program staff. All RHY projects are required to collect specific data elements, including the HUD Universal Data Elements and program-specific data elements for the RHY-funded project for which they receive funding (Street Outreach Program, Basic Center Program, Transitional Living Program).

The Runaway and Homeless Youth Act requires that a RHY grantee "keep adequate statistical records profiling the youth and family members whom it serves (including youth who are not referred to out-of- home shelter services)."

RHY grantees are not required to obtain youth or parental consent to collect and enter youth data into the Watsonville/Santa Cruz CoC HMIS.

II. Consent Needed for Data Sharing

Data sharing refers to the sharing of consumer information per the Policy laid out in this document. For RHY grantees, data can only be shared if written consent is obtained from the parent or legal guardian of a youth who is under age 18, or with written consent from a youth who is 18 or older.

The RHY rule states the following regarding data sharing: Pursuant to the Act, no records containing the identity of individual youth served by a Runaway and Homeless Youth grantee may be disclosed except:

A. For Basic Center Program grants, records maintained on individual youth shall not be disclosed without the informed consent of the youth and parent or legal guardian to anyone other than another organization compiling statistical records, or a government organization involved in the disposition of criminal charges against the youth.

B. For Transitional Living Programs, records maintained on individual youth shall not be disclosed without the informed consent of the youth to anyone other than an organization compiling statistical records.

C. Research, evaluation, and statistical reports funded by grants provided under section 343 of the Act are allowed to be based on individual youth data, but only if such data are de-identified in ways that preclude disclosing information on identifiable youth.

D. Youth served by a Runaway and Homeless Youth grantee shall have the right to review their records; to correct a record or file a statement of disagreement; and to be apprised of the individuals who have reviewed their records.
E. The Department of Health and Human Services (HHS) policies regarding confidential information and experimentation and treatment shall not apply if HHS finds that state law is more protective of the rights of youth.
F. Procedures shall be established for the training of RHY program staff in the protection of these rights and for the secure storage of records. 45 CFR § 1351.21.

III. Special Consideration for RHY-Funded Programs

In consideration of the guidance laid out in the RHY Program HMIS Manual, RHY-funded grantees shall enter data into the Watsonville/Santa Cruz CoC HMIS for youth served and seeking services that will not be shared with any other CHO, unless the grantee receives written consent from the youth or parent/legal guardian of the youth served that allows the disclosure of the youth's PII for the permissible purposes laid out in this Policy.

APPENDIX F: SECURITY POLICY

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.

APPENDIX G: CONSENT TO DATA SHARING FOR RUNAWAY AND HOMELESS YOUTH

Watsonville/Santa Cruz City & County Continuum of Care (CoC) Consent for Data Sharing for Runaway and Homeless Youth (RHY)-Funded Programs

The Santa Cruz County Homeless Management Information System (HMIS) is a shared database and software application which confidentially shares consumer-level information related to homelessness in Santa Cruz County. We ask you to consent to the sharing of your information to help the Watsonville/Santa Cruz City & County Continuum of Care (CoC) provide quality housing and services to people at risk of or experiencing homelessness and/or who have very low-income.

Your information will be released to housing and services providers ("Covered Homeless Organizations" (CHOs)), which include community-based organizations and government agencies. CHOs use the information in HMIS to: improve the quality of housing and services; identify patterns and monitor trends over time; conduct needs assessments and prioritize services for subpopulations at risk of or experiencing homelessness or with very low-income; enhance inter-agency coordination; and monitor and report on the delivery, impact, and quality of housing and services.

BY CHECKING AND SIGNING THIS FORM, I UNDERSTAND THE FOLLOWING:

☐ I understand the following on *the sharing of my basic information with CHOs*:

- CHOs may change over time; a current list of CHOs has been provided to me and I may request an updated list at any time or view the list at https://santacruz.bitfocus.com/participating-agencies.
- Basic information includes: Name, Social Security Number, Date of Birth, Race, Ethnicity, and Gender.
- The collection, use, and release of this information is for the purpose of assessing my needs for housing, counseling, food, utility assistance, or other services.

☐ I understand that the information shared may include the following types of protected personal information (PPI):

- Identifying information (e.g., name, birth date, gender, race, ethnicity, social security number, phone number, residence address, or other similar identifying information)
- Medical, mental health and substance use information included in my responses to questions asked as part of the standard HMIS intake
- Financial and benefits information (e.g., employment status, income verification, public assistance payments or allowances, food stamp allotments, health care coverage, or other similar financial or benefits information)
- Housing status and related information
- Information about services provided by Partner Agencies (e.g., intake date, duration, and type of service)

☐ I understand CHOs use the PPI collected in HMIS to assess, prioritize, and refer me to housing options and other services. I also understand that CHOs communicate with each

other to coordinate prioritization, placement, and determine eligibility for housing and other services.

☐ I understand the CHOs and individual staff have signed agreements to maintain the security and confidentiality of my information.

☐ I understand that I may refuse to sign this Consent. My refusal will not affect my eligibility for benefits or services, or my ability to obtain services or receive support. My refusal does not disqualify me from receiving services or support.

☐ I understand that I may sign the Consent and still refuse to provide specific information that I do not want to share.

☐ I can revoke this Consent at any time but I must do so in writing. Revoking the Consent is not retroactive and will not affect any information shared while I gave my consent. I understand that this consent is valid for 3 years from the date listed below.

☐ My PPI is protected by federal, state, and local regulations governing the confidentiality of consumer records. My information cannot be released without my written consent, except when the rules say otherwise.

☐ I have the right to review my records, to correct a record or file a statement of disagreement, and to be notified of the people who have reviewed my records, except in limited circumstances to protect the health and safety of myself or others.

SIGNATURE

_____ _____

Print Name of Consumer or Legal Guardian Signature of Consumer or Legal Guardian

_____

Date

APPENDIX H: DATA QUALITY AND IMPROVEMENT PROCESS AND PLAN

Watsonville/Santa Cruz City & County Continuum of Care (CoC) Homeless Management Information System (HMIS) Data Quality Improvement Process and Plan

I. Data Quality Defined

Data quality is a term that refers to the reliability and validity of consumer-level data in HMIS. It is measured by the extent to which data in the system represents authentic characteristics within a community. With good data quality, the Watsonville/Santa Cruz City & County Continuum of Care (CoC) can accurately provide a full picture of the individuals and families accessing local homelessness response system resources. HMIS data is used to: improve housing and services quality; identify patterns and monitor trends over time; conduct needs assessments and prioritize services for subpopulations experiencing or at-risk of homelessness or living with very low incomes; enhance inter-agency coordination; and monitor and report on the delivery, impact, and quality of housing and services.

II. Data Quality Standards

Data quality can be measured by data completeness, the extent to which all expected data elements are entered for all consumers; data timeliness, the amount of time that passes between data collection and entry into HMIS; data consistency, the degree to which users enter data consistently and without contradiction across all programs in HMIS; and data accuracy, the extent to which data are entered accurately and consistently.

III. Data Completeness

Complete HMIS data is necessary to fully understand the demographic characteristics and service use of persons with information in HMIS and to identify ways to improve services. Complete data facilitates confident reporting and analysis of the experience of homelessness in the CoC region. Data is considered complete if ALL consumers are entered into HMIS and all required data elements are captured.

The CoC's goal is to collect 100% of all data elements; however, it recognizes that this may not be possible in all cases. HUD HMIS data standards expect no null (missing) data for required data elements, and "Don't Know" or "Refused" or "Other" responses should not exceed the percentages listed in the table below.[1]

A missing rate of below 5 percent represents an ideal goal, and the CoC should work toward accomplishing this level of data completeness for all programs. For large-scale night-by-night shelters, alternate targets for data completeness will be considered based on past performance.

Data Element	Applies to:	Don't Know/ Refused Should Not Exceed
First Name*	All Consumers	5%
Last Name*	All Consumers	5%
SSN*	All Consumers	5%
Date of Birth*	All Consumers	5%
Race	All Consumers	5%
Ethnicity	All Consumers	5%
Gender	All Consumers	5%
Veteran Status	Adults Only	5%
Disabling Condition	All Consumers	5%
Living Situation	Adults & Heads of Households (HoH)	5%
Zip Code of Last Permanent Address	All Consumers	5%
Income and Sources (at entry)	Adults & HoH	5%
Income and Sources (at annual update)	Adults & HoH enrolled in program 365 days or more	5%
Income and Sources (at exit)	Leavers - Adults & HoH	5%
Non-Cash Benefits (at entry)	Adults & HoH	5%
Non-Cash Benefits (at annual update)	Adults & HoH enrolled in program 365 days or more	5%
Non-Cash Benefits (at exit)	Leavers - Adults & HoH	5%
Physical Disability	All Consumers	5%
Developmental Disability	All Consumers	5%
Chronic Health Condition	All Consumers	5%
Mental Health	All Consumers	5%
Substance Abuse	All Consumers	5%
Domestic Violence	Adults & HoH	5%
Destination	Leavers - Adults & HoH	5%
Move-in Date	Adults & HoH enrolled in PH with move-in date	5%

*For anonymized consumers the following data elements will be exempted from the 95% completeness standard: (1) Social Security Number; (2) first name; (3) last name; (4) date of birth. However, all "canned" (pre-programmed) reports in Clarity Human Services software will still show those elements as "missing" for anonymized consumers.

IV. Data Accuracy

Data should be entered accurately into HMIS. Accuracy depends on the consumer's ability to provide the data and staff's ability to document and accurately enter it. Although HMIS data accuracy can be hard to assess, Covered Homeless Organizations (CHO) should audit approximately 5% of active consumer records monthly. The audit should check that data recorded in the consumer file matches data recorded in HMIS (e.g., entry and exit dates, household type, demographic characteristics, history of homelessness, etc.) and that consumer data is in alignment with project characteristics (e.g., a family is not entered in a program for single adult men).

V. Data Consistency

Data consistency refers to all data entry staff understanding, collecting, and entering data consistently across all programs in HMIS. Data consistency requires data entry staff to have a common understanding of each data element, its response categories, and meaning. To facilitate data consistency, County of Santa Cruz Human Services Department Housing for Health Division (H4H), as the HMIS lead, will ensure the availability of training procedures and materials that outline basic data elements, response categories, rationale, and definitions.

VI. Data Timeliness

Entering data into HMIS in a timely manner is important for several reasons: it facilitates up-to-date information for resource availability, allows data to be accessible when needed (service planning for people experiencing homelessness, monitoring or funding purposes, or for responding to requests for information), and reduces human error that occurs when too much time elapses between the provision of a service (data collection) and data entry. To ensure that system-wide data is as accurate as possible, all Universal Data Elements and Program-specific Data Elements should be entered according to the following timeliness standards.

Entry/Exit Data

Program Type	Data Timeliness Standard: At Entry	Data Timeliness Standard: At Exit
Emergency Shelter	Within two business days of intake	**Night by Night**: at or before 30 calendar days after the last service date. Exit date backdated to last service **Entry/Exit**: Within two business days of exit
Transitional Housing/ Permanent Supportive Housing/ Homelessness Prevention Services Only	Within two business days of intake	Within two business days of exit
Outreach	Within two business days of intake	At or before 30 calendar days since last service date. Exit date to be backdated to last service
Day Shelter	Within two business days of intake	At or before 90 calendar days since last service date. Exit date to be backdated to last service

Service Data

All participating programs should enter services into HMIS within **two business days** as described in the chart below.

Program Type	Service Requirement
Night-by-night Emergency Shelters	Services to track bed nights and others as required by local funders
Street Outreach	Services required by local funders, where applicable
Day Shelters	Services required by local funders, where applicable
RHY-funded Programs	Additional data elements and services (see RHY HMIS Manual)
PATH-funded Programs	Additional data elements and services (see PATH HMIS Manual)

Current Living Situation Assessments

Current Living Situation assessments are used to document the housing status during the first interaction with each consumer, as well as any subsequent consumer interactions if the housing situation has changed. At a minimum, the Current Living Situation Assessment must be completed every 90 days even if there are no status changes.

Status Update Assessments

All consumers with an active/open HMIS enrollment that experience a significant status change in income, employment, non-cash benefits, living situation, or other key characteristics require an Update Assessment within 30 days of learning of the status change. At a minimum, the Update Assessment must be completed every 90 days even if there are no status changes.

Annual Assessments

All HMIS enrollments that are active/open require an annual assessment within the 30-day period either before or after participants' project start anniversary date each year (a 60-day window).

Continuous Data Quality Improvement Process

A continuous data quality monitoring and improvement process facilitates the ability of the CoC to achieve valid and reliable data. It sets expectations for both the community and end users to capture accurate data on persons accessing agency programs and services.

Roles & Responsibilities

The HMIS System Administrator, with input from H4H, will provide the following services to assist CHOs in correctly entering data into HMIS and addressing data quality issues:

- Work with CHO management to identify at least one CHO employee as an HMIS agency lead.
- Provide end user trainings and workflow documents.
- Produce data quality reports and information on how to correct identified data quality issues.
- Work to identify and, in conjunction with CHOs, resolve data quality issues that will impact local or federal reporting.
- Provide technical assistance to CHOs requesting assistance in correcting data quality issues.

- Provide other services as directed by the HMIS Agency Lead and H4H.

Working with their HMIS lead, CHOs will take primary responsibility for entering, verifying, and correcting data entry

- CHO staff will measure completeness by running recommended data quality reports and distributing those reports to staff tasked with improving data quality and completeness.
- It is the responsibility of CHO management to ensure staff tasked with correcting data quality issues do so in a timely manner.

Data Quality Review

At the CoC level, data are reviewed regularly, and issues are identified for follow-up. Follow-up on system wide issues will include a discussion at the monthly HMIS Provider Meeting. Other CHO-specific follow up will also be done by the HMIS vendor and H4H.

Monthly

Data quality dashboards, listing records with missing data or other data quality issues, are provided in the HMIS Data Analysis Tab or sent in scheduled emails monthly to assist CHO in identifying data errors. Staff reports are emailed monthly to all CHO leads to assist in monitoring CHO staff usage of the system.

Quarterly

On a quarterly basis, the HMIS vendor will review staff HMIS utilization and data quality statistics and inform CHOs of compliance issues.

Reporting Preparation

Approximately two months before any significant local or federal reporting deadlines, data impacting the reports are thoroughly reviewed by the HMIS vendor, with CHO follow up and technical assistance as needed.

Participating CHOs should run data quality reports (HUDX-225, described below) monthly. In the weeks prior to submitting a significant federal report (e.g., APR), data quality reports may need to be run daily to ensure any issues identified by the CHO or the HMIS vendor are addressed.

CHOs that review data regularly tend to have higher levels of data quality and do not have significant data quality issues to address when trying to meet federal reporting deadlines.

Minimizing Data Quality Issues

To minimize data quality issues:

- Enter consumer data as soon as possible. The more time between collecting data and entering it into HMIS, the more likely there will be data quality issues (see section above for data timeliness standards).
- Whenever possible, enter data during consumer visits so that consumers may help identify potential inaccuracies.
- Review Data Quality monthly and address any issues as soon as possible.
- Problem-solve with Program and HMIS staff around any ongoing issues.

VII. Support for CHOs and HMIS Users

To ensure that agencies and HMIS users have the tools necessary to address data quality issues efficiently, H4H and the HMIS vendor provide a range of support resources.

Recommended Reports for Data Review

HMIS includes an extensive library of reports. The following reports are recommended as a starting place for reviewing data and identifying data quality issues:

- **[GNRL-16] Program Roster** (Program Based Reports) is used to check individuals enrolled in a program during a particular reporting period. The report summarizes data entered for each consumer including entry and exit dates and assigned staff. Run the report monthly to confirm high level data on program consumers during a reporting period accurately reflects the work done by the program.
- **[HUDX-225] HMIS Data Quality Report [FY 2022]** (HUD Reports) includes program or agency level data that highlights key HUD data quality issues. When run as a web output report, the report provides details on the source of errors. It is recommended to run the report at least once every quarter.
- **[DQXX-102] Program Data Review** (Data Quality Reports) includes program and client specific data quality issues; the web output report provides information on errors with specific consumers' data. It is recommended to run the report quarterly.
- **Data Analysis Report – Santa Cruz Clarity System Reports – Quarterly Status Update Report** is only available to HMIS manager level users. The report contains information at the agency and program level of all consumers who are due for a quarterly status, living situation, or annual update.

Technical Assistance

CHOs can request HMIS technical assistance as follows:

- The Watsonville/Santa Cruz CoC HMIS Helpdesk (santacruz.bitfocus.com | santacruz@bitfocus.com) can provide initial troubleshooting assistance and escalate issues to the Watsonville/Santa Cruz CoC HMIS System Administration team as needed.
- The HMIS System Administration team may proactively contact CHOs directly or at the request of funders, H4H, the CHO itself, or as otherwise needed, to identify and address data quality issues.
- The System Administration team offers guides, trainings, dashboards, and other resources to help agencies proactively identify and resolve data quality issues (santacruz.bitfocus.com/general-training).

Key Reports and Processes that Rely on High Data Quality

The quality of the HMIS data impacts the ability of individual programs to provide accurate reports to funders and the CoC's use of the data for system improvement activities. Data quality issues such as high rates of missing consumer data and missing or inaccurate enrollment, exit and assessment data can impact program and CoC funding. Data quality issues challenge H4H in producing accurate reports for funders, elected officials, and other stakeholders. The Continuous Data Quality Improvement Process described above supports accurate HMIS information for these reports and processes, including but not limited to:

Annual Performance Review (APR) - Program
Recipients of HUD funding through the homeless CoC grant competition are required to submit an Annual Performance Report (APR) electronically to the federal Department of Housing and Urban Development (HUD) annually.

Annual CoC Competition Application to HUD
The CoC competes in an annual national competition for HUD CoC Program funds. System-wide data is required as part of the competition application, as is aggregate data for all projects receiving CoC funding.

Coordinated Entry (CE) APR
The CE program is required to submit a special CE Annual Performance Report (APR) electronically to HUD, annually. The CE APR includes data from the HMIS as well as narrative responses.

HMIS APR
Since the Watsonville/Santa Cruz CoC HMIS receives HUD funding through the annual CoC funding competition, H4H is required to submit a special HMIS Annual Performance Report (APR) annually. The HMIS APR includes data from the HMIS as well as narrative responses.

Point in Time Count (PIT)
The PIT count is an enumeration of persons experiencing sheltered and unsheltered homelessness typically on a single night in January. HUD requires the sheltered portion of the count be generated from HMIS data. **Approximate due date: April 30**

Housing Inventory Count (HIC)
The HIC is a comprehensive inventory of all housing, including all beds, units, or bed vouchers, dedicated to homeless and formerly homeless individuals and families within a CoC. **Approximate due date: April 30**

System Performance Measures (SysPM)
HUD SysPM are a tool used to measure the local homeless response as a coordinated system rather than individual programs and funding sources. HUD uses the system-level performance information in its annual CoC national funding competition award decisions and to gauge the state of the homeless response system nationally.
Approximate due date: Feb/March

Longitudinal Systems Analysis Report (LSA)
The LSA is used to produce HUD's Annual Homeless Assessment Report (AHAR) to the U.S. Congress. The AHAR provides nationwide estimates of homelessness, including information about the demographic characteristics of persons experiencing homelessness, service use patterns, and the capacity to house homeless persons. The LSA, produced from a CoC's HMIS, provides annual information on how people experiencing homelessness use the system of care. The LSA data is submitted in the form of CSV files uploaded to HUD's Homeless Data Exchange.

Stella is a strategy and analysis tool that helps CoCs understand how their system is performing and models an optimized system that fully addresses the area's homelessness. The extent of the tool's usefulness to a CoC for evaluation and planning purposes depends on the completeness and accuracy of the LSA data.
Approximate draft due date: Oct 31, **Approximate final due date: Dec 31**

In preparation for development of these reports, CHOs and the HMIS vendor employ the continuous data quality improvement practices described above. Specifically:

- Throughout the year:
    - HMIS Vendor:
        - Conduct data quality reviews based on feedback from H4H staff and CHOs including following up with CHOs as needed.
        - Provide CHOs with dashboards and other information about specific data quality issues that need to be addressed.
        - Provide trainings on data quality topics.
    - CHOS:
        - Follow up on data issues as identified by the HMIS vendor or H4H staff.
        - Ensure staff understand how to maintain high data quality through ongoing training and support.

- As a report deadline approaches:
    - CHOs: begin data quality reviews well in advance, focused on ensuring consumers are accurately enrolled in programs including all required information and no null values.
    - HMIS Vendor: help CHOs to resolve data quality issues upon request.

APPENDIX I: USER AGREEMENT AND CODE OF ETHICS

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
Individual HMIS User Agreement and Code of Ethics

The primary focus in the design and management of the Watsonville/Santa Cruz CoC HMIS is to help consumers get and keep permanent homes. Achievement of this goal requires continual quality improvement of programs and services and the maintenance of consumer confidentiality by treating personal data with respect and care.

As the guardians entrusted with this personally identifiable information (PII), Watsonville/Santa Cruz CoC HMIS users have a moral and legal obligation to ensure that appropriate methods are practiced with the collection, access, and utilization of data. Each user must ensure that consumer data is only used for the purpose for which it is collected. Proper user training, adherence to the Watsonville/Santa Cruz City & County CoC Privacy Policy, and a clear understanding of consumer confidentiality are vital to achieving these goals. All Users are required to attend a CoC approved training class prior to their first use of the HMIS and annually thereafter.

Please check each box below to indicate your understanding and acceptance of the proper use of the HMIS system and data. PLEASE READ CAREFULLY. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination from HMIS access and may result in disciplinary action from the CHO as defined in the CHO's personnel policies.

BY CHECKING <u>EACH BOX</u> AND SIGNING THIS FORM, I UNDERSTAND THE FOLLOWING:

I agree to maintain the confidentiality of Consumer information in the HMIS in the following manner:

☐ My user ID and password are for my use only and must not be shared with anyone.

☐ I must take all reasonable means to keep my password physically secure.

☐ I understand that the only individuals who can view information in HMIS are authorized users and the consumers to whom the information pertains.

☐ I may only view, obtain, disclose, or use the database information that is necessary to perform the official duties of my job.

☐ I acknowledge that it is a consumer's decision about which information to share for entry into HMIS and the data will only be shared with authorized HMIS partner agencies.

☐ I will ensure that an HMIS Consumer Notice is posted at any location consumer intake services are provided and personally identifiable information (PII) is entered into HMIS.

☐ I will always provide consumers with a copy of the CoC Consumer Notice and an Acknowledgement of its receipt shall be signed at least every three years. A copy of the signed Acknowledgement will be uploaded and stored in the HMIS system.

☐ If I have a conflict of interest in entering data within HMIS, I will disclose that to my supervisor. If I am a consumer with information in the Watsonville/Santa Cruz CoC HMIS,

or if I have immediate family members with information in the Watsonville/Santa Cruz CoC HMIS, I will not make changes to those files.

To prevent casual observers from seeing or hearing HMIS Consumer information:

☐ If I am logged into HMIS and must leave the work area where the computer is located, I must log off HMIS before leaving the work area. Failure to log off HMIS may result in a breach of consumer confidentiality and system security.

☐ Hard copies of HMIS information must be kept in a secure file. When hard copies of HMIS information are no longer needed, they must be properly destroyed to maintain confidentiality.

☐ I will not discuss HMIS confidential Consumer information with staff, Consumers, or Consumer family members in a public area.

☐ I will not discuss HMIS confidential Consumer information on the telephone in any areas where the public might overhear my conversation.

☐ I will not transmit confidential consumer or identifying information via unsecured and unencrypted email.

☐ I will not leave messages on my agency's answering machine or voicemail system that contains HMIS confidential Consumer information.

☐ If I notice or suspect a security breach, I must immediately notify my Agency Administrator and Bitfocus.

As an HMIS User, I understand and will abide by the following Code of Ethics:

☐ Users must be prepared to answer Consumer questions regarding HMIS.

☐ Users must faithfully respect Consumer preferences about the sharing of their information within the HMIS.

☐ Users must accurately record Consumer's preferences by making the proper designations as to sharing of Consumer information and/or any restrictions on the sharing of Consumer information.

☐ Users must not refuse services to a Consumer, or potential Consumer, if that Consumer refuses to allow sharing personal information with other agencies via the HMIS.

☐ The User has primary responsibility for information entered by the User. Information that Users enter must be truthful, accurate and complete to the best of User's knowledge.

☐ Users will not solicit from, or enter information about, Consumers into the HMIS unless the information is required for a legitimate business purpose, such as providing services to the Consumer, and/or is required by the program funder.

☐ Users will not use the HMIS database for violation of any law, to defraud any entity or to conduct any illegal activity.

☐ Upon Consumer written request, Users must allow a Consumer to inspect and obtain a copy of the Consumer's own information kept within the HMIS, unless sharing this information could result in significant harm to the health and safety of the consumer or others.

☐ Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding need not be provided to the Consumer.

☐ Users must permit Consumers to file a written complaint regarding the use or treatment of their personal information within the HMIS. Consumers may complete an HMIS Data Misuse and Breach Reporting form located at santacruz@bitfocus.com. Consumer will not be retaliated against for filing a complaint.

I understand and agree to comply with all the statements listed above.

_____	_____	_____
Print Name	Signature	Date
_____	_____	_____
Agency Name	Work Phone Number	Email Address

APPENDIX J: HMIS DATA MISUSE AND BREACH REPORTING FORM

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
HMIS Data Misuse and Breach Incident Reporting Form

This form is used to notify the Watsonville/Santa Cruz City & County CoC of any of the following in relation to its Homeless Management Information System (HMIS) and the use of data from HMIS:

- An incident involving unsecured Personally Identifiable Information (PII), if that PII was, or is reasonably believed to have been accessed or acquired by an unauthorized person.
- A suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII in violation of signed agreements.

PII is any information about an individual which can be used to distinguish, trace, or identify their identity, including personal information like name, address, date of birth or social security number.

The form can be submitted electronically via DocuSign (click **here**), by secure email to **santacruz@bitfocus.com**, or either mailed or delivered in person at:

Please complete as much of this form as possible. Depending on the specific nature of the incident, Bitfocus (the HMIS Administrator) or a Housing for Health (H4H) Division staff member (the HMIS Lead) will contact you.

Person Reporting the Incident

First Name: _____ Last Name: _____

Agency: _____ Email: _____

Title (if applicable): _____ Phone Number (include area code): _____

Incident Details

Organization: _____

Organization Street Address: _____

Organization City and Zip: _____

Date and time of incident: _____

Date and time you learned of the incident: _____

Type of Incident (Check all that apply)

- ☐ Unauthorized Access
- ☐ Unauthorized Disclosure
- ☐ Loss
- ☐ Theft
- ☐ Other (describe): _____

Location of Incident (Check all that apply)

- ☐ Desktop computer
- ☐ Laptop computer
- ☐ Other electronic device

- ☐ Paper
- ☐ Other (describe): _____

Brief Description of Incident (specific data accessed, used, or disclosed in ways that constitute a breach, specific consumer(s) involved): _____
_____
_____

IF YOU ARE A CONSUMER REPORTING AN INCIDENT, YOU DO NOT NEED TO COMPLETE THE REST OF THIS FORM.

Estimated number of client data records breached:

Safeguards in Place Prior to Incident (Check all that apply):

- ☐ None
- ☐ Privacy safeguards (Training, Policies and Procedures, etc.)
- ☐ Security administrative safeguards (Risk Analysis, Risk Management, etc.)
- ☐ Security physical safeguards (Facility Access Controls, Workstation Security, etc.)
- ☐ Security technical safeguards (Access Controls, Transmission Security, etc.)

Actions Taken in Response to Incident (Check all that apply):

- ☐ Adopted encryption technologies
- ☐ Changed password/strengthened password requirements
- ☐ Created a new/updated Security Risk Management Plan
- ☐ Implemented new technical safeguards
- ☐ Implemented periodic technical and nontechnical evaluations
- ☐ Improved physical security
- ☐ Performed a new/updated Security Risk Analysis
- ☐ Provided individuals with free credit monitoring
- ☐ Revised policies and procedures
- ☐ Sanctioned workforce members involved (including termination)
- ☐ Took steps to mitigate harm
- ☐ Trained or retrained workforce members
- ☐ Other (describe): _____

APPENDIX K: APPROACHES TO RESPONDING TO CONSUMER CONCERNS ABOUT DATA SHARING

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
Approaches to Responding to Consumer Concerns about Data Sharing

- Explain importance of data sharing
    - Helps streamline the application and intake process, especially if consumer is working with other providers who use HMIS
    - Important documents can be saved into electronic file so the same information doesn't have to be collected again
    - Helps to not miss out on housing opportunities –we can notify you of temporary and permanent housing opportunities
    - HMIS allows linking people to valuable resources by matching information with the eligibility criteria for resources such as benefits linkage, rental assistance, shelters, street outreach, housing navigation, veteran services, health services, and runaway homeless youth services.
- Explain privacy and security; everyone gets retrained every year
- Explain de-identified/aggregate data is reported and used
    - Provides statistical and demographic information necessary to continue receiving funding for services and housing for people experiencing homelessness
    - Helps us understand the needs of our community to identify gaps and services that would benefit our community further
    - Helps us identify and make the case for more housing, more services, and more funding for the community
- Role play with a colleague
- Options if client doesn't want some/all data shared
    - Enter the maximum amount of data approved by the consumer
    - Create an anonymous client record
    - Document and indicate the reasons the consumer refused to sign

APPENDIX L: HMIS CHO CORRECTIVE ACTION PLAN TEMPLATE

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
HMIS Agency Corrective Action Plan

Date of Notification: _____

Agency: _____

Executive Director/HMIS Lead for Agency: _____

Email: _____

Phone: _____

Itemized Violation(s)	Applicable Documents
1.	
2.	
3.	
4.	

Itemized Corrective Measures	Expected Completion Date
1.	
2.	
3.	
4.	

HMIS Resources to Support Corrective Measures: _____

_____

_____

_____

_____ _____

Agency Administrator/Director Signature Date

_____ _____

CoC HMIS Coordinator Signature Date

APPENDIX M: HMIS GRIEVANCE FORM

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
HMIS Grievance Form

How to File a GRIEVANCE about our Privacy Practices

If you feel a violation of your rights as an HMIS client has occurred or disagree with a decision made about your "Protected HMIS Information" you may complete this form. Complete this form only after you have exhausted the applicable agency's grievance procedures. **It is against the law for any agency to take retaliatory action against you if you file this grievance. You can expect a response within 30 days via the method of your choice.**

The form can be submitted electronically via DocuSign (click here), by secure email to santacruz@bitfocus.com, or mailed or delivered in person at:

Housing for Health Partnership HMIS
County of Santa Cruz Human Services Housing for Health Division
1000 Emeline Ave., Santa Cruz, CA 95060

Date of offense: _____

_____	_____
Name of individual who violated your privacy rights	Name of agency who violated your privacy rights

Brief description of grievance – what happened:

Best way to contact you:

Your name: _____

Your phone: _____

Your mailing address: _____

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, and to better understand the needs of people served. Only information considered to be appropriate is collected.

CoC Grievance Response Date: _____

Recommendation to Agency:

APPENDIX N: HMIS CLIENT REVOCATION OF CONSENT TO RELEASE INFORMATION

Watsonville/Santa Cruz City & County Continuum of Care (CoC)
HMIS client revocation of consent to release information

I, _____, hereby revoke permission for this agency to share my personal information in the Watsonville/Santa Cruz CoC HMIS. I understand that my information will remain in HMIS as part of the non-identifying data collected on services provided within the CoC.

I understand that information that has already been entered remains in the system. By canceling my agreement for participation in HMIS, my personal information that has been saved will be restricted.

I further understand that any information entered and/or shared under my previously agree-to-consent form will continue to be shared and this Client Revocation of Consent only applies to information entered into the system from this day forward.

I also understand that the disclosure of my non-identifying information may be required in some instances, such as for the reporting of aggregate numbers to entities that provide funding to this agency.

The Watsonville/Santa Cruz CoC HMIS System Administrator and this agency are hereby released from any legal responsibility or liability for the release, use or disclosure of information I authorized previously.

Agency Name: _____

Agency Representative: _____

Phone Number: _____

Client's Full Name: _____

SSN/Client's HMIS ID Number:_____

_____ _____

Client Signature Date

This form can be submitted electronically via DocuSign (click here), by secure email to santacruz@bitfocus.com, mailed or delivered in person at:

Housing for Health Partnership HMIS
County of Santa Cruz Human Services Housing for Health Division
1000 Emeline Ave., Santa Cruz, Ca 95060