



**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:

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

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): _____