



A Tradition of Stewardship
A Commitment to Service

NAPA COUNTY HEALTH AND HUMAN SERVICES AGENCY
Self Sufficiency Services Division

POLICY AND PROCEDURE:

Breach of Personally Identifiable Information

REVIEW FREQUENCY:

Every two years

POLICY # 20006-1029-15

DISTRIBUTION:

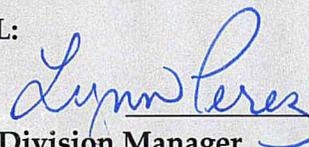
- Employment Services
- Eligibility Services
- Quality Mgmt

EFFECTIVE DATE: April 1, 2015

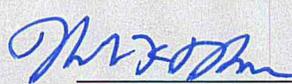
ORIGINAL DATE OF ISSUE: April 15, 2015

LAST REVISION DATE: N/A

APPROVAL:

Title and Signature	Date
APPROVAL: 	7/30/15
Division Manager	Date

APPROVAL:

	8-3-15
HHSA Director	Date

POLICY STATEMENT:

It is the policy of the Napa County Health and Human Services Agency (NCHHSA) to offer twelve (12) months of credit monitoring service at no cost, through Experian Information Solutions, Inc., to those individuals who's Personally Identifiable Information (PII) has been compromised by our Agency.

ADMINISTRATION:

- Office Assistant (OA)
- Eligibility Worker (EW)
- Employment Services Worker (ESW)
- Office Assistant Supervisor
- Eligibility Supervisor
- Employment Services Supervisor
- Analyst
- Self Sufficiency Manager
- Contractor
- Community Aide
- Screeener

DEFINITIONS:

Breach – Defined as the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control of personally identifiable information.

Compromise – Defined as to expose or make vulnerable to danger, suspicion, scandal, etc.; jeopardize.

Personally Identifiable Information (PII) – Defined as information that identifies a specific person and would allow another person to create a false identity based on that information. This includes, but is not limited to, the following information: name, address, telephone number, email address, gender, Social Security Number, date of birth, case number, and public assistance aid codes.

END OF POLICY

PROCEDURE

I. Prevention

- A. Personally Identifiable Information may only be released on an as needed basis and only to those individuals who are authorized to use such information as part of their official duties within NCHHSA
 - 1. PII is kept secure and only used for the specific official business purpose for which it was requested
 - 2. PII is not disclosed or provided to others without proper written authorization.
 - a. Client signed authorization to release information form

II. Detection

- A. PII can be compromised under several different circumstances. Circumstances include but are not limited to:
 - 1. Written documents mailed, emailed or faxed to an incorrect individual or agency
 - 2. Documents left in plain sight of other individuals
 - 3. Information released to an individual or agency without proper written authorization
 - 4. Information discussed in an area where information can be overheard by other individuals
 - 5. Lost or misplaced documents

III. Reporting Process

- A. Upon discovery that an individual's PII has been compromised the staff shall immediately report the incident to his/her supervisor. If the supervisor is not available, the staff will report the incident to their lead worker or another supervisor
 - 1. The staff will complete the Incident Report located on the HHSA Intranet, under County eForms.
 - 2. Staff will document the following information regarding the breach of PII in the C-IV journal or in the Virtual One Stop (VOS) system:
 - a. Date notified of the incident
 - b. Date incident occurred
 - c. Name of person whose information was compromised
 - d. Name of supervisor they reported incident to
 - e. Date incident report was filed
- B. If an individual reports, by phone, that he/she received a document(s) from NCHHSA that do not belong to them:
 - 1. Obtain the individual's name, phone number, and case number (if applicable) who received the document(s)
 - 2. Inform the individual that our agency takes every precaution to protect information provided to us
 - 3. Attempt to have the individual bring the document(s) to our office
 - a. Set up a specific date and time, if possible

4. If the individual is unable to bring the document(s) to our office that same day, arrange a time on that same day (no later than the following morning) for a Community Aid or any available staff to pick up the document(s) from the individual
 5. Ask the individual if they have read through the documents
 6. Do not ask the individual to read through the documents
 7. The staff person will document the following information regarding the breach of PII in the C-IV journal or in the VOS system:
 - a. Date notified of the incident
 - b. Date incident occurred
 - c. Name of person whose information was compromised
 - d. Name of supervisor they reported incident to
 - e. Date incident report was filed
- C. If an individual reports, in person, that he/she received a document(s) from NCHHSA that do not belong to them:
1. Obtain the individual's name, phone number, and case number (if applicable) who received the document(s)
 2. Inform the individual that our agency takes every precaution to protect information provided to us
 3. Ask the individual to please wait and speak to a Supervisor
 - a. Call a Supervisor immediately
 4. Ask the individual if they have read through the documents
 5. The staff person will document the following information regarding the breach of PII in the C-IV journal or in the VOS system:
 - a. Date notified of the incident
 - b. Date incident occurred
 - c. Name of person whose information was compromised
 - d. Name of supervisor they reported incident to
 - e. Date incident report was filed

IV. Initiating Credit Monitoring Service

- A. Supervisor will contact the assigned Analyst the same day the incident report is filed and will provide a copy of the incident report
 1. The Deputy Director of Self Sufficiency Services Division (SSSD) and/or the County Privacy and Security Officer will review the facts of the incident to determine whether or not there was breach of PII and if the individual(s) will be offered credit monitoring services
 - a. If it is determined there was no breach of PII, no further action is needed
 - b. If it is determined there was a breach of PII, and credit monitoring services are necessary the Deputy Director of SSSD will advise the assigned Analyst
 - c. Assigned Analyst will notify the unit Eligibility Supervisor to make initial contact with the client whose PII was breached
- B. Assigned Analyst will prepare the First Contact letter to the individual whose PII was compromised
 1. Letter to be signed by the Deputy Director of SSSD or a Self Sufficiency Manager

2. Assigned Analyst will notify the unit Eligibility Supervisor that the First Contact letter was sent to the individual
3. Assigned Analyst will document, in C-IV or in VOS, the date letter was mailed
- C. One week after the First Contact letter is mailed, the assigned Analyst will prepare the Experian Activation letter to the individual whose Personally Identifiable Information was compromised
 1. Assigned Analyst will order activation codes from Experian as needed by completing the Experian Protection Products Order form
 2. Expiration date of the activate code will be included in the letter to the individual
 3. Letter to be signed by the Deputy Director of SSSD or a Program Manager
 4. Assigned Analyst will document, in C-IV or in VOS, the date letter was mailed
 5. Electronic copy of the letter to be sent to the Napa County Privacy and Security Officer
- D. Assigned Analyst will enter the following information into a tracking spreadsheet
 1. Date of incident
 2. Name of person whose information was compromised
 3. Case number
 4. Name of the person who reported the incident
 5. Supervisor's name that filed the Incident Report
 6. Date Incident Report was submitted
 7. Date the First Contact letter was sent to the individual
 8. Date assigned Analyst notified unit Eligibility Supervisor that First Contact letter was sent
 9. Date the Experian Activation letter was sent to the individual
 10. Experian Code provided to the individual
 11. Date the Experian Code expires
 12. Date invoice sent to Fiscal for payment

V. Requesting payment from Fiscal

- A. Once an individual has activated a code, Experian will invoice NCHHSA.
 1. Experian will not invoice NCHHSA, if a code is not activated
- B. The assigned Analyst will approve the invoice and forward to Fiscal for payment

REFERENCES:

Confidentiality Policy and Procedure # 2000600-1000-13

FORMS:

Incident Report (County eForm)
 First contact letter
 Experian form letter

CONTACT PERSON(S):

Vickie Ruise, Staff Services Analyst

END OF PROCEDURE

REVISION HISTORY:

Revision	Date	Description of Change	Requested By
1.0	4/15/2015	Procedure Created. Released into 60 day working draft	V. Ruise, SSA