STANISLAUS COUNTY COMMUNITY SERVICES AGENCY	Developed by/Date: Security Workgroup 4/10, 11/11	Page: 1 of 2	Number: 7.16
			Category: Administrative
	Reviewed by/Reviewed Date: Executive Committee 4/19/10, 11/7/11	Replaces:	Distribution: All Staff
Title: **Breach of Confidentiality Reporting Process**		Approved: 11/7/11	

Policy ☐ **Procedure** ☑ **Guideline** ☐

Purpose

To clearly define the two different types of breaches within the department and identify the appropriate procedures for addressing these issues consistently across the multiple programs within the Agency.

Definition

Security Breach is defined as any real or suspected **harmful event** where the security of Personal Identifiable Information (PII) could be threatened, lost, or stolen. A security breach must be reported to the breach officer to take proper action.

Examples (including, but not limited to):

- Brief case lost at airport containing case files.
- Stolen unencrypted laptop containing PII.
- Staff accessing and/or retaining customer information for personal gain with criminal intent.

Confidentiality Breach is defined as any time a customer's information is accessed or disclosed without a business need. Confidentiality breaches **do not** need to be reported to the breach officer. They do need to be reported to the manager of the staff and the Human Resources manager for disciplinary investigation and action.

Examples (including, but not limited to):

- Reviewing sister's case to see if benefits were calculated correctly.
- Giving friend a copy of their social security card from their case record.
- Reviewing case to find ex-spouse's employer.

Procedure

Security Breach Officer

Stanworks Manager IV – Primary
Stanworks Manager IV - Backup

Security Breach Process

1. The person who discovers or suspects a security breach has occurred will notify the Breach Officer or her/his back-up immediately.
2. The Breach Officer or back-up will notify the Director and appropriate Assistant Director.

3. The Breach Officer will work with those individuals involved to determine if a security breach occurred and to mitigate any further loss of PII.
4. The Security Breach Officer or back-up will notify Department of Health Care Services (DHCS) Privacy Officer and Security Officer by **email** within 24 hours of receiving notification.

    Privacy Officer
    c/o: Office of Legal Services
    Department of Health Care Services
    P.O. Box 997413, MS 0011
    Sacramento, CA 95899-7413
    Email: privacyofficer@dhcs.ca.gov
    Telephone: (916) 445-4646

    Information Security Officer
    DHCS Information Security Office
    P.O. Box 997413, MS 6400
    Sacramento, CA 95899-7413
    Email: iso@dhcs.ca.gov
    Telephone: ITSD Help Desk
    (916) 440-7000
    (800) 579-0874

5. The manager over the area where the security breach has occurred will complete the Worksheet for Reporting Loss or Potential Loss of PII within 7 working days of the incident and give it to the Breach Officer or back-up.
6. The Security Breach Officer, back-up to the Breach Officer, or the manager over the area where the security breach occurred will submit the written report to the DHCS Privacy Officer and Security Officer within 10 working days of the incident.
7. The Security Breach Officer will obtain approval from DHCS Privacy Officer for the time, manner, and content of any notification sent to individuals whose information has been breached.

<u>Confidentiality Breach Process</u>

1. Supervisor or manager made aware of the confidentiality breach will report the incident to the HR manager immediately.
2. The manager and HR manager will work together to properly investigate the incident to determine if a breach has occurred and severity of situation.
3. HR manager will recommend appropriate disciplinary action.
4. Manager will work with Assistant Director to impose appropriate discipline.