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, 1/29/18	Replaces:	Distribution: All Staff

Title: **Breach of Confidentiality Reporting Process**

Approved: 1/29/18

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

Purpose

To set policy and procedures for the Stanislaus County Community Services Agency (CSA) response to breaches of customer privacy including Personal Confidential Information (PCI), and Protected Health Information (PHI) that violates federal or state privacy laws and in accordance with the California Security Breach Notification Act (California Civil Code § 1798.29).

Definition

Privacy Breach:

A Privacy breach is an unauthorized acquisition, access, use or disclosure of Protected Health Information (PHI) and/or Personal Confidential Information (PCI) that violates either state or federal privacy laws, such as the HIPAA Privacy Rule and/or the state Information Practices Act (IPA) of 1977. Privacy breaches may be either paper or electronic and may occur when information is transmitted to an unintended recipient or accessed by someone without proper authorization. Examples of paper breaches include loss or theft of paper documents containing PHI/PCI; inadvertent mailings or email to incorrect providers or beneficiaries; or misdirected paper faxes with PHI/PCI outside of the CSA. Examples of electronic breaches include stolen, unencrypted laptops, unencrypted compact discs, hard drives, Personal Computers, or thumb drives with PHI/PCI; or electronic faxes (e-fax) with PHI/PCI misdirected to persons outside of the CSA.

Privacy Rule:

The Privacy Rule is regulations implementing the Health Insurance Portability and Accountability Act (HIPAA) which set “Standards for Privacy of Individually Identifiable Health Information” found at 45 CFR Parts 160 and 164.

Protected Health Information (PHI):

Protected Health Information (PHI) is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future**.**

Personal Confidential Information (PCI):
Personal Confidential Information (PCI) is information that is not public which identifies or describes an individual including names, home addresses, home telephone numbers, Social Security Numbers, medical or employment histories, personnel records, licensing records or workers' compensation.

California Security Breach Notification Act (California Civil Code § 1798.29):
A state agency, or any person or business that owns or licenses computerized data that include personal information, must disclose any breach of security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

A breach of the security of the system is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business regardless of the medium in which the breached information is held (ie. Paper, electronic, oral, or the combination of data elements involved including non-notice triggering personal information).

1. ***Personal information*** is defined as the first name or initial and last name of an individual, in combination with one or more of the following when either the name or the data elements are not encrypted:

    - Social Security Number; or
    - Driver's license number or California ID card number; or
    - Credit card or debit card number; or
    - A financial account number with information such as PIN numbers, passwords, or authorization codes that could permit access to the account; or
    - Medical information defined as the individual's medical history, mental or physical condition, treatment or diagnosis by a health care professional (Civil Code §1798.29); or
    - Health insurance information defined as a health insurance policy or subscriber number, any unique identifier used by a health insurer used to identify the individual, or any information in an individual's application and claims history, as well as appeals records (Civil Code §1798.29).

2. A user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Policy

It is the policy of the Community Services Agency (CSA) to investigate all alleged breaches of PCI or PHI reported by its employees, staff of its business associates, and individual program beneficiaries/patients or other persons and to report such breaches as soon as practical to the Privacy Officer and Information Security Officer of the California Department of Health Care Services (DHCS). The CSA shall create procedures designed to ensure compliance with federal and state privacy laws, timely reporting and investigation, individual notifications

as required by law, mitigation of known breaches, and corrective actions to minimize future privacy breaches. Procedures shall include provisions for training staff, work process reviews, and employee sanctions for violating the content of this policy and procedures.

Procedure

CSA Incident Response Team:

The following positions comprise the CSA Incident Response Team:

- Chief Privacy Officer: Program Integrity Manager whose backup is the Civil Rights, Appeals & Quality Control Supervisor.
- Information Security Officer: Information Technology Manager or his/her designee
- Program Manager: Manager who has oversight of the Section/Unit where the breach occurred.
- Public Information Officer: CSA designated Public Information Officer (PIO).
- Legal Counsel: County Counsel as designated by the Chief County Counsel.
- Escalation Manager: The Chief Privacy or Information Security Officer will serve as the Escalation Manager based upon the nature and scope of the breach.

Responsibilities:

In the event of a privacy breach, CSA staff should do the following:

Staff Discovering Breach:

- Immediately report the breach to your immediate supervisor.
- If your supervisor is not available, report the breach to any other supervisor or manager.
- Explain how the breach came to your attention.
- Explain the circumstances of how the breach occurred if known.
- Provide as much factual information as possible (names, dates, times, circumstances, etc).

Supervisor Responsibilities:

- Once you are apprised of a breach, verify whether in fact the circumstances meet the definition of a privacy breach. You may consult with your manager and/or the Program Integrity Manager for assistance.
- Take immediate steps to recover the media that contains PCI/PHI and to mitigate any further breaches.
- Gather as many facts as possible to identify who, what, when, where, why, and how of the incident.
- Identify the parties by case number only. DO NOT INCLUDE NAMES
- Draft an email to the Program Integrity Manager as soon as possible, but no later than 10:00 AM the next business day informing him/her of the involved parties, date the

breach was first noticed, date the breach actually occurred, and the nature of the breach.
- The Program Integrity Manager will reply to your email with an assigned agency investigation number (ie. 17-01) *This number is not the number assigned by the DHCS.
- Conference with your manager to decide who will conduct the privacy breach investigation and email the Program Integrity Manager the information.
- Complete the Privacy Incident Report and forward it to the Program Integrity Manager by 10:00 AM on or before the fifth business day following discovery of the breach. For example, if a breach is discovered on Monday, the PIR should be completed by 10:00 AM the following Monday. Do not count weekend days or county recognized holidays.
- The Privacy Incident Report (PIR) should be completed in accordance with the example attached to this policy.

Manager Responsibilities:

- Provide oversight to ensure privacy breach policy and procedures are correctly followed. You may consult the Program Integrity Manager for assistance.
- Assume the Supervisor Responsibilities listed above in the event a supervisor is responsible for the breach.
- Coordinate the privacy breach investigation if it involves multiple customers and/or staff.
- Review work processes and procedures to help formulate an appropriate Corrective Action Plan (CAP) aimed at mitigating future privacy breaches.
- Conference with the Human Resources Manager and Assistant Director to determine appropriate disciplinary action to include, but not limited to training and/or sanctions.
- Execute appropriate CAP that may include any combination of changes in work processes or procedures, additional training, and/or employee sanctions.
- Ensure the CAP and completed dates are reflected in the PIR.
- Draft an email to the Program Integrity Manager as soon as possible, but no later than 10:00 AM on the next business day once the CAP is completed.

Program Integrity Manager Responsibilities:

- Facilitate communication and oversight of this policy and procedures.
- Offer guidance and assistance to supervisors and/or managers to identify, investigate, and report privacy breach incidents.
- Liaison and report breaches to the Privacy Officer and/or Information Security Officer of the California Department of Health Care Services (DHCS) as required by law.
- Examine the nature and scope of the breach and consult with the DHCS to ensure the CSA takes appropriate courses of action.
- Track investigations, issue report numbers, prepare customer notices, and file all documentation of the breach as required by the DHCS.
- Conference with managers and the CSA leadership to identify the patterns and frequency of privacy breaches and offer suggestions for corrective actions.

- Assess and update privacy breach training as necessary to comply with changes in the law.

Sources

- State of California, California Information Security Office: *Requirements to Respond to Incidents Involving a Breach of Personal Information* (SIMM 5340-C, March 2017).
- State of California, Department of Health Care Services: *Privacy Policies and Procedures* (April 2013).
- *State of California Civil Code §§ 1798 et seq.* (California Legislative Information, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29).

Community Services Employees needing to report a Privacy Incident can find the Privacy Incident Report and Privacy Incident Report Instructions located at Ollie>Admin>Human Resources>Employee Forms