SANTA BARBARA COUNTY
DEPARTMENT OF
Behavioral Wellness
A System of Care and Recovery

Departmental Policy and Procedure

Section	Compliance	**Effective:**	10/27/2017
Sub-section	HIPAA/Privacy	**Version:**	1.0
Policy	Reporting Breaches and Security Incidents Involving PHI, PII and PI	**Last Revised:**	New policy
Policy #	11.100		
Director's Approval	Alice Gleghorn, PhD	**Date**	10/30/17
Deputy Director's Approval	Pam Fisher, PsyD	**Date**	10/27/17
Supersedes:	New policy	**Audit Date:**	10/27/2020

1. PURPOSE/SCOPE

1.1. To establish standards and procedures in accordance with the Health Information Portability and Accountability Act (HIPAA) Security Rule, the California Information Practices Act (CIPA), and all other applicable federal, state and local laws governing the protection of health information and reporting of breaches and security incidents.

2. POLICY

2.1. It is the policy of the Santa Barbara County Department of Behavioral Wellness (hereafter "the Department") to investigate potential breaches and security incidents related to the unauthorized access, use or disclosure of Protected Health Information (PHI), Personally Identifiable Information (PII), and Personal Information (PI). The Department shall comply with breach notification requirements set forth in the Department's contract with the State Department of Health Care Services (DHCS) for specialty mental health and alcohol and drug services.

3. DEFINITIONS

The following terms are limited to the purposes of this policy:

3.1. **Breach** – the acquisition, access, use, or disclosure of PHI, PII and/or PI in a manner not permitted which compromises the security or privacy of the information. A breach does not include (1) good faith acquisition, access, or use of private data by an employee, contractor, or agent of the Department, if the data is not provided to an unauthorized person; (2) incidents involving data that have been rendered unusable, unreadable, or undecipherable (e.g. through valid encryption) to unauthorized individuals; or (3) incidents involving de-identified data.

3.2. **Personal Information (PI)** – any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

3.3. **Personally Identifiable Information (PII)** – any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

3.4. **Protected Health Information (PHI)** – any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

3.5. **Security Incident** – the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI, PII and/or PI, or confidential data utilized by the Department to perform the services, functions and activities on behalf of DHCS, or interference with system operations in an information system that processes, maintains or stores PHI, PII and/or PI.

4. REPORTING VIOLATIONS

4.1. **Notification of Department Executives.** Upon discovery of a potential breach or security incident involving PHI, PII and/or PI, staff shall notify the Security Officer, the Privacy Officer, the Chief of Compliance, the Director, and any other parties requiring immediate notification.

4.2. **Initial Notification: Breach.** The Department's Privacy Officer and/or Security Officer shall notify DHCS immediately by telephone, email, or fax upon the discovery of a breach of unsecured PHI, PII and/or PI in electronic media or in any other media if the PHI, PII and/or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. A breach shall be treated as discovered by the Department as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of the Department.

4.3. **Initial Notification: Security Incident**. The Department's Privacy Officer and/or Security Officer shall notify DHCS within 24 hours by email or fax of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI, PII and/or PI or potential loss of confidential data.

1. If the suspected security incident involves Social Security Administration (SSA) data, notification must occur by email or fax within one (1) hour.

4.4. Notice shall be provided to the Information Protection Unit, Office of HIPAA Compliance.

1. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, PII and/or PI, notice shall be provided by calling the Information Protection Unit or by email at:

   Phone: (916) 445-4646
   Toll-free Number: (866) 866-0602
   Email: privacyofficer@dhcs.ca.us

2. If the incident occurs after business hours or on a weekend or holiday and involves electronic PII or PI, notice shall be provided by calling the Department Information Security Officer at:

   Phone: (916) 440-7000
   Toll-free Number: (800) 579-0874

4.5. Notice shall be made using the DHCS "Privacy Incident Report form, including all information known at the time. The Department shall use the most current version of this form, which is posted on the DHCS Information Security Officer website at http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx.

4.6. Upon discovery of a breach or suspected security incident, intrusion, or unauthorized access, use or disclosure of PHI, PII and/or PI, the Department's Privacy Office and/or Security Officer shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
2. Any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

4.7. **Investigation and Investigation Report.** The Department shall immediately investigate suspected security incidents, breaches, unauthorized access, use or disclosure of PHI, PII and/or PI. Within 72 hours of the discovery, the Department shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Information Protection Unit (for breaches) or the DHCS Information Security Officer (for security incidents).

4.8. **Complete Report.** The Department shall provide a complete report of the investigation to the DHCS Program Contract Manager and the Information Protection Unit within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or

disclosure. If DHCS requests information in addition to that listed on the "Privacy Incident Report" form, the Department shall make reasonable efforts to provide DHCS with such information. If, because of the circumstances of the incident, the Department needs more than ten (10) working days from the discovery to submit a complete report, DHCS may grant a reasonable extension of time, in which case the Department shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. DHCS will review and approve the determination of whether a breach occurred and whether individual notifications and a corrective action plan are required.

4.9. **Responsibility of Reporting of Breaches: PHI.** If the cause of the breach of PHI is attributable to the Department or its agents, subcontractors or vendors, the Department is responsible for all required reporting of the breach as specified in 42 USC Section 17932 and its implementing regulations, including notification to media outlets and to the Secretary (after obtaining prior written approval of DHCS). If a breach of unsecured PHI involved more than 500 residents of the State of California or under its jurisdiction, the Department shall first notify DHCS, then the Secretary of the breach immediately upon discovery of the breach. If a breach involves more than 500 California residents, the Department shall also provide, after obtaining written prior approval of DHCS, notice to the Attorney General of the State of California, Privacy Enforcement Section. If the Department has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to DHCS in addition to the Department, the Department shall notify DHCS, and DHCS and the Department may take appropriate action to prevent duplicate reporting.

4.10. **Responsibility of Notification of Affected Individuals: PHI.** If the cause of a breach of PHI is attributable to the Department or its agents, subcontractors or vendors and notification of the affected individuals is required under state or federal law, the Department shall bear all costs of such notifications as well as any costs associated with the breach. In addition, DHCS reserves the right to require the Department to notify such affected individuals, which notifications shall comply with the requirements set forth in 42 USC Section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days after discovery of the breach. The DHCS Privacy Officer shall approve the time, manner and content of any such notification and their review and approval must be obtained before the notification are made. DHCS will provide its review and approval expeditiously and without unreasonable delay.

4.11. **Responsibility of Reporting of Breaches: PII and PI.** If the cause of the breach of PII or PI is attributable to the Department or its agents, subcontractors or vendors, the Department is responsible for all required reporting of the breach as specified in CIPA Section 1798.29 and as may be required under the Information Exchange Agreement

(IEA) with DHCS. The Department shall bear all costs of required notifications to individuals as well as any costs associated with the breach. The DHCS Privacy Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. DHCS will provide its review and approval expeditiously and without unreasonable delay. If the Department has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to DHCS in addition to the Department, the Department shall notify DHCS, and DHCS and the Department may take appropriate action to prevent duplicate reporting.

ASSISTANCE

Celeste Andersen, JD, Chief of Compliance

Marshall Ramsey, Division Chief of Information Technology/Security Officer

Yvonia Newby, Privacy Officer

REFERENCE

Code of Federal Regulations – Notification in the Case of Breach of Unsecured Protected Health Information
Title 45, Part 164, Subpart D

Code of Federal Regulations – Confidentiality of Substance Use Disorder Patient Records
Title 42, Part 2

California Civil Code - California Information Practices Act
Title 1.8, Section 1798

State County Contract/Department of Health Care Services (DHCS)
Exhibits G-1, 3-D, 13(a-e) and G-2, 3-B, 9(a-g)

RELATED POLICIES

Violations of HIPAA/CMIA

REVISION RECORD

DATE	VERSION	REVISION DESCRIPTION

Culturally and Linguistically Competent Policies

The Department of Behavioral Wellness is committed to the tenets of cultural competency and understands that culturally and linguistically appropriate services are respectful of and responsive to the health beliefs, practices and needs of diverse individuals. All policies and procedures are intended to reflect the integration of diversity and cultural literacy throughout the Department. To the fullest extent possible, information, services and treatments will be provided (in verbal and/or written form) in the individual's preferred language or mode of communication (i.e. assistive devices for blind/deaf).