ALAMEDA COUNTY Behavioral Health Care Services	**Date Approved**: July 6, 2018 **By**: Carol F Burton Carol F. Burton, MSW, Interim Director
POLICY TITLE Privacy & Security Incident Reporting Policy	**Policy No: 1704-1-1** **Date of Original Approval**: July 25, 2013 **Date(s) of Revision(s)**: July 6, 2018

PURPOSE

This policy is to provide guidence to Alameda County Behavioral Health Care Services (ACBHCS) Mental Health and Substance Use Disorder service providers, either directly employed or otherwised contracted, for the reporting of Privacy and Security incidents that result in the potiential and actual improper or unauthorized disclosure of protected health information (PHI) in either a physical or electronic form.

AUTHORITY

- *42 CFR, Part 2*
- 45 CFR 164

SCOPE

This policy is put into place in order to maintain compliance with 45 CFR 164; SB 541; AB 211, ARRA/ HITECH ACT,and 42 CFR, Part2 in relationship to privacy incident reporting.

Privacy Incidents occurring on or after September 23, 2009 must be reported to DHHS and/or California Department of Public Health (CDPH) (immediately if 500+ individual cases; annually if fewer) and patient must be notified without unreasonable delay (but no longer than 60 days.) This policy covers all legal entities of the Alameda County Mental Health Plan (MHP) including all Business Associates in their entirety. The MHP is comprised of County staff, contractors, and interns, contracted Mental Health and Substance Use Disorder Providers and their employees.

FEDERAL vs. STATE REQUIREMENTS & RESPONSIBILITIES:

- Use the Federal Risk of Harm Threshold: For the purposes of this definition, a breach "compromises the security or privacy of the protected health information" when divulged, means it poses a significant risk of financial, reputational or other harm to the individual. (See further information below.)
- SB 541 & AB 211: State law requires health facilities as of 1/1/2009 in California to report all breaches to the CDPH.
    - Health facilities include: 24 hour care hospitals, acute psych hospitals, psychiatric health facilities, home health agencies, hospices, and primary care and specialty clinics operated by non-profit corporations.
    - Requires report to CDPH within 5 business days.

- CDPH then notifies licensing boards of any involved employees of facilities so they may discipline their licenses.
- CDPH has power to levy fines and other penalties.

POLICY

All covered entities, under the Alameda County MHP, shall report suspected, proven, or potential unauthorized disclosure of PHI to the MHP in order to mitigate harm to consumers and correct actions of it's employees, contractors, interns, volunteers, or other associated agents.

PROCEDURE

When privacy indicent occurs:

1. The Executive Director of the Contracted Agency or their designee must submit the privacy incident reporting form, (PIR), attached, at discovery to ACBHCS Privacy Officer via email: breachnotification@acgov.org or FAX: (510)639-1346.
2. The BHCS-Privacy Officer or designee will:
   a. Notify DHCS immediately by telephone and email at the discovery of a perceived breach of Medi-Cal PHI in electronic media or in any other media if the PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person or upon the discovery of a suspected security incident that involves data provided to DHCS SSA
   b. Or, notify DHCS within 24 hours by email of the discovery of a any perceived breach; incidents occurring after ACBHCS business hours will be reported to DHCS ITSD Service Desk
   c. ACBHCS will subsequently, on behalf of its subcontractors, agents, programs, will send a PIR to DHCS within 72 hours of discovery via:

Privacy Officer
E-mail: **privacyofficer@dhcs.ca.gov**
Phone: (916) 445-4646
FAX: (916) 440-7680

Information Security Officer
E-mail: **iso@dhcs.ca.gov**
Phone: (916) 440-7000 or
(800) 579-0874

i. If it falls under **federal regulations**, a risk/harm assessment will be done by the Alameda County BHCS Privacy Officer (or designee) immediately.
   1. If risk is established and the breach involves 500+ individual cases, BHCS will report to the US-DHHS by regular 1st class mail within 60 days and to media outlets. If 10 or more individuals whose information was compromised can't be

reached, BHCS will provide media or website "substituted notice".
2. BHCS will log breaches of less than 500 individual cases and will provide reports of the breaches to the US-DHHS annually, attaching the federal Breach Reporting Forms.
3. Patients must be notified within 60 days by regular 1st class mail to last known address.

United States Department of Health and Human Services
Office of Civil Rights
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, D.C. 20201
OCRPrivacy@hhs.gov
(800) 368-1019

OCR Timelines: These timelines refer to when you must notify the OCR of the breach. If the law requires you to contact the people whose information was breached, you must notify them as soon as you can – and no later than 60 days after discovering the breach.

For breaches involving the records of 500 or more people
Complete the form and send it to the OCR within 10 business days of discovering the breach.

For breaches involving the records of fewer than 500 people
Complete the form and send it to the OCR by the 60th day of the calendar year following the breach. For example, if you discover a breach involving fewer than 500 people on June 30, 2009, send the form to the OCR no later than 60 days into the calendar year of 2010. If you experience two breaches like this in one calendar year – one on June 30th and another on November 1st – complete a separate form for each breach, staple them together, and send them to the OCR no later than 60 days into the calendar year of 2010.

Verify the form arrived at the OCR by using a mailing method that gives you proof of delivery. For security reasons, don't email the form.

Questions? Call the OCR at (800) 368-1019 or email OCRPrivacy@hhs.gov or send a letter to the address above.

CONTACT

BHCS Office	Current as of	Email
Quality Assurance Office- Privacy Officer Information Systems- Security Officer	July 1, 2018	BreachNotification@acgov.org

DISTRIBUTION

This policy will be distributed to the following:

- ACBHCS Staff
- ACBHCS County and Contract Providers
- Public

ISSUANCE AND REVISION HISTORY

Original Title: HIPAA Breach Reporting
Original Author: Kyree Klimist, QA Adminsitrator, ACBHCS
Original Date of Approval: 7/25/2013 by Aaron Chapman, M.D., Interim Director, ACBHCS

Date of Revision: 6/29/18

Revise Author	Reason for Revise	Date of Approval by (Name)
Donna Fone Tiffany Lynch	Change policy name; correct procedure and update to include 42 CFR	July 6, 2018 Carol Burton, ACBHCS Interim Director

DEFINITIONS

Term	Definition
Breach	A violation of one's responsibility to follow privacy policy and procedure that results in an individual's PHI being accessed by unauthorized persons
Disclosure	To release, transfer, provide access to or divulge in any way a individual's health information to authorized individuals or entities
PHI- Protected Health Information	Information that is a subset of health information, including demographic information, and: 1. Is created or received by a health-care provider, health plan, employer or health-care clearinghouse; and 2. Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and a. That identifies the individual; or b. There is a reasonable basis to believe the information can be used to identify the individual.
Privacy Incident	Any potential or actual compromise of personally identifiable information (PII) in a form that could be accessed by an

	unauthorized person
Privacy Officer	The person designated by the organization who is responsible for development and implementation of the HIPAA policies and procedures. The Privacy Officer serves as a resource to assist ACBHCS staff and contracted organizations and individual's in implementing HIPAA policies and procedures.
Security Incident	A warning or occurance of a threat or unauthorized access or disclosure to electronic information or computer security.
Security Officer	A position mandated by the HIPAA. The responsibilities of this person are to oversee implementation of the requirements mandated by the Final Security regulation and any security requirements included in the other sections of the HIPAA regulation

PRIVACY INCIDENT REPORT (PIR)

The information reported in this form will be strictly confidential. The information reported in this form will be used to review your determination of whether a breach has occurred.

*☐= Required items within 72 hours of discovery, to the extent known

† = US Health and Human Services (HHS) required information

1. SUMMARY OF PRIVACY INCIDENT *† (Please include location of the Privacy Incident, how the Privacy Incident occurred, and any information regarding the type of media and protected health information involved in the Privacy Incident.)

2. BASIC INFRMATION *†

DHCS Privacy Incident case number (this will be assigned after initial report):

Reporting entity's Privacy Incident case number (if applicable):

Date of most recent updates (today's date):

Reporting entity:	Type of Entity:	HIPAA Covered Entity?

The type of contract the reporting entity has with DHCS?

Entity that caused Privacy Incident:

HIPAA Covered Entity?

Reporting entity's relationship with the entity that caused the Privacy Incident:

Date(s) of Privacy Incident: **Dates(s) of discovery:** **Date of notice to DHCS:**

Number of individuals affected by Privacy Incident:

What was the primary job function of the person(s) known, or reasonably believed, to have improperly sent, used, accessed, or disclosed PHI/PI (include employer/employee status, and any other pertinent information)?

What was the primary job function of the person(s) who viewed or (accidentally) obtained PHI/PI (include employer, employee status, other health plan member, and any other pertinent information)?

Additional basic information:

Was this incident a Violation of your Policies and Procedures?

If yes, please explain:

3. CONTACT INFORMATION *†

Reporting entity's contact's name:

Reporting entity's contact's e-mail:

Reporting entity's contact's telephone number:

Was this incident reported to any other entities/persons(s):

If the answer to the above questions is 'yes', then list the contact information of the entity/person the report was filed with:

4. PROTECTED HEALTH INFORMATION (PHI)/PERSONALLY IDENTIFIABLE (PI)*

Does the information disclosed in the Privacy Incident provide a reasonable basis to believe it can be used to identify an individual?

Does the information disclosed in the Privacy Incident relate to the past, present, or future physical or mental health, or condition of an individual?

Does the information involved in the Privacy Incident relate to the payment or provision of health care to an individual?

5. TYPE OF PRIVACY INCIDENT *†

- ☐ Improper Disposal
- ☐ Theft
- ☐ Loss
- ☐ Unauthorized Disclosure
- ☐ Mis-Sent
- ☐ Hacking/IT Incident
- ☐ Unauthorized Use/Access
- ☐ Unknown
- ☐ Other

If other, please explain:

6. TYPE OF PROTECTED INFORMATION INVOLVED *†

DEMOGRAPHIC INFORMATION

- ☐ First Name or Initial
- ☐ Last Name
- ☐ Address/Zip
- ☐ CIN or Medi-Cal #
- ☐ Date of Birth
- ☐ Social Security Number
- ☐ Driver's License
- ☐ Membership #
- ☐ Health Plan Name
- ☐ User Name/Email Address with Password
- ☐ Other

Return Completed Form to: BreachNotification@acgov.org or Fax 510-639-1346

If other type of protected information, please explain:

FINANCIAL INFORMATION

☐ Credit Card/Bank Acct# ☐ Claims Information ☐ Other

If other, please explain:

CLINICAL INFORMATION

☐ Diagnosis/Condition ☐ Medications ☐ Psychotherapy notes

☐ Mental Health Data ☐ Lab Results ☐ Substance Use/Alcohol Data

☐ Other

If other, please explain:

Please list all the data elements originally obtained from DHCS:

Please list all the data elements originally obtained from or verified by the Social Security Administration:

7. LOCATION OF INFORMATION DISCLOSED IN PRIVACY INCIDENT *†

☐ Laptop ☐ Network Server ☐ Desktop Computer

☐ Portable Electronic Device ☐ Email ☐ Electronic Record

☐ Paper Data ☐ Smart Phone ☐ Hard Drive

☐ CD/DVD ☐ PDA ☐ Tape/DLT/DASD

☐ USB Thumb Drive ☐ Fax ☐ Other

If other, please explain: if network server please provide the name of the server and who owns it:

8. APPLICABLE SAFEGUARDS IN PLACE PRIOR TO PRIVACY INCIDENT *†

☐ Strong Authentication ☐ Packet Filtering ☐ Anti-Virus Software

☐ Secure Browser Sessions ☐ Biometrics ☐ Encrypted Wireless

☐ Physical Security ☐ Firewalls ☐ Logical Access Control

☐ Data Leak Protection ☐ Encrypted ☐ Intrusion Detection

Was staff involved in Privacy Incident trained in HIPAA information Security and Privacy within the past year?

Additional information regarding safeguards:

9. MALICIOUS CODE/MALWARE TYPE

☐ Worm ☐ Buffer Overflow ☐ Virus

☐ Trojan ☐ Denial of Service (DOS) ☐ Other

If other, please explain:

10. DATA AND RECOVERY *

Were any DHCS systems involved?

Was data encrypted per NIST standards?

Was data recovered?

If data was recovered, specify what, when, and who has it now:

If not recovered, explain (still missing/shredded/under investigation):

Discuss the impact of Privacy Incident (potential misuse of data, identity theft, etc.):

11. DHCS PROGRAM DATA

How many DHCS Program beneficiaries' PHI or PI were impacted by the Privacy Incident? *

Did this Privacy Incident involve a minor (<18 yrs.)?

Was PHI or PI in question utilized in the administration of the Medi-Cal Program?

12. SUPPLEMENTARY DESCRIPTION OF PRIVACY INCIDENT † (Please include any supplementary information regarding the Privacy Incident)

13. ACTIONS TAKEN IN RESPONSE TO PRIVACY INCIDENT †

Describe mitigation plan and status (if necessary attach separately):

Investigation status (i.e. completed, estimated completion date, etc.):

Status of member notification letter (if applicable):

Describe Corrective Action Plan (CAP) and status (attach CAP separately if needed):

Note: A CAP is implemented in an attempt to prevent this type of Privacy Incident from reoccurring.

Enter the CAP completion/implementation date (Or the date it is scheduled):

14. BREACH DEFINITIONS AND EXCEPTIONS

Did Privacy Incident fall under one of the three exclusions?

If an exclusion, please explain circumstances.

15. BREACH DETERMINATION †

Has your entity determined this to be a Federal Breach?

Has your entity determined this to be a State Breach?

An incident is presumed to be a breach. If you have evidence under 45 CFR 164.402(2)(1)(i),(ii),(iii),(iv), please provide the evidence and the HIPAA provision that applies to find that a breach does not exist below.

This may be submitted in a seperate document. If this is the case please enter "Attached" below.

16. BREACH REPORTING (if applicable) †

Date of Federal breach reporting to OCR (if applicable).

If you did not enter a date above, remember that it is your responsibility to report breaches as required by Federal regulation.

Date of State breach reporting to Attorney General's office (if applicable).

If you did not enter a date above, remember that it is your responsibility to report breaches as required by State Law.