
	Date Approved: <u> 7/25/13 </u> By: <u></u> Aaron Chapman, MD Interim Mental Health Director
POLICY: HIPAA Breach Reporting	Date Revised: <u> 6/15/13 </u> Policy No.: _____

POLICY: HIPAA Breach Reporting

The following policy is put into place in order to maintain compliance with 45 CFR 164; SB 541; AB 211 and the ARRA/ HITECH ACT, in relationship to HIPAA breach reporting.

All confidentiality breaches 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.)

DEFINITION:

Breach: The acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted under the above mentioned laws and regulations, which compromises the security or privacy of the protected health information.

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.

DEFINITIONS:

Breach: The acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted under the above mentioned laws and regulations, which compromises the security or privacy of the protected health information.

Exceptions to the need to report a Breach (Further details in Title 45 CFR 164, subpart E):

- Mistaken access by an employee:
 - Any unintentional acquisition, access or use of PHI by a workforce member or person, acting under the authority of a Business Associate (BA) or Covered Entity (CE), if it was

- Mistaken disclosure between two employees: Any inadvertent disclosure by a person who is authorized to access that PHI at a covered entity or business associate to another person authorized to access PHI at the same CE or BA or Organized Health Care Arrangement (OHCA) in which the CE participates, and the information received is not further used or disclosed in a manner not permitted under subpart E (the Privacy Rule).
 - Near Miss:
 - A disclosure of PHI where a CE or BA has a good faith belief that an un-authorized person to whom the disclosure was made would not reasonably be able to retain such information, eg. sending some PHI in the mail to the wrong address where the mail is returned unopened to the post office as undeliverable, or eg. a nurse mistakenly hands discharge papers to the wrong patient, quickly realizes the mistake and recovers the PHI before the patient has time to read it.
 - Federal Risk of Harm Threshold: As of March 23, 2013, the “harm threshold” was replaced with a more objective standard: Section 164.402 states: (Unless an explicit exception) a breach is an acquisition, access, use or disclosures in violation of the Privacy Rule is presumed to be a breach unless the Covered Entity or Business Associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
 - i. Nature and extent of the PHI, types of identifiers and likelihood of re-identification
 - ii. The person who used the PHI or to whom it was disclosed
 - iii. Whether it was actually acquired previewed; and,
 - iv. The extent to which the risk was mitigate
 - Covered Entity must do the assessment in the case of every potential reportable breach
 - Records of the risk assessment must be kept for Six (6) years
- Considerations: (also see “Breach Risk Assessment-Attachment 1”):
1. Who used or received the PHI in violation of the Rule (eg. if the recipient also must comply with federal privacy laws there is less risk of harm than if others got it.)
 2. Were immediate steps taken to mitigate the harm? (Did the recipient provide satisfactory assurances that the PHI will not be further disclosed and has been destroyed?)
 3. What type of PHI was involved? (If only a hospital patient’s name was released, with no other information, may be no significant risk of harm. But if it is a specialty hospital or treatment program that might be different.)
 4. Was a limited data set used or disclosed? (If re-identification risk is so small because the 16 identifiers (below), zip codes and dates of birth are excluded and therefore there is no significant risk of harm, then no breach.)
 1. Names
 2. Postal address information, other than town or city, State, and zip code
 3. Telephone numbers
 4. Fax numbers
 5. Electronic mail addresses
 6. Social security numbers
 7. Medical record numbers
 8. Health plan beneficiary numbers
 9. Account numbers
 10. Certificate/license numbers
 11. Vehicle identifiers and serial numbers, including license plate numbers
 12. Device identifiers and serial numbers
 13. Web Universal Resource Locators (URLs)

14. Internet Protocol (IP) address numbers
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.

PROCEDURE:

When a breach is identified:

1. The Executive Director of the Provider Agency or their designee must submit the privacy incident reporting form, (PIR), at discovery to ACBH Privacy Officer via email: breachnotification@acgov.org or FAX: (510)639-1346.
2. The ACBH-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 ACBH business hours will be reported to DHCS ITSD Service Desk
 - c. ACBH 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 ACBH Privacy Officer (or designee) immediately. (See above “Considerations”)
 1. If risk is established and the breach involves 500+ individual cases, ACBH 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, ACBH will provide media or website “substituted notice”.
 2. ACBH 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.