| | | |
|---|---|---|
| **County of Sacramento<br>Department of Health Services<br>Division of Behavioral Health Services<br>Policy and Procedure** | Policy Issuer (Unit/Program) | **QM** |
| | Policy Number | **QM-03-12** |
| | Effective Date | **01-01-2010** |
| | Revision Date | **01-04-2021** |

| | |
|---|---|
| Title:<br>**Incident Reporting and Breach Notification of Protected Health Information** | Functional Area:<br>**Confidentiality, Consent, Privacy & Security** |
| Approved By: (Signature on File) **Signed version available upon request**<br><br>**Alexandra Rechs, LMFT**<br>Program Manager, Quality Management | |

## BACKGROUND/CONTEXT:

Sacramento County Division of Behavioral Health Services (DBHS) is committed to safeguard all Personally Identifiable Information (PII) and Protected Health Information (PHI) in the possession of the county or its contractors in accordance with Federal and State laws and applicable regulatory requirements. This information, whether in physical (paper) or electronic form, documents the interaction between consumers of services and service providers. In those instances where there is any potential or actual breach of privacy and confidentiality of protected information, the DBHS policy is to take prompt and appropriate action to minimize the risk of any unintended disclosure. DBHS is required to notify the Department of Health Care Services (DHCS) Privacy Officer when a potential or actual breach occurs.

## DEFINITIONS:

**Breach –** The actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII and/or PHI, whether electronic, paper, verbal, or recorded.

**Incident –** The attempted or successful unauthorized access, use, disclosure, modification, or destruction of personally identifiable information (PII) or PHI that is under the control of the County or County's contractor, subcontractor or vendor of the County.

**Incidental Disclosure –** Use or disclosure as a secondary use or disclosure that cannot reasonably be prevented is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure. Examples: Unintentional overhearing of information/conversation containing PHI and PII; a sign-in sheet in waiting rooms; use or disclosure by employees or authorized individuals in the "same facility".

**Personally Identifiable Information (PII) –** Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. Examples of PII include, but are not limited to: Individual's name, social security number, biometric records, etc. that, alone, or when combined with other personal or identifying information may be linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

**Protected Health Information (PHI) –** Individually identifiable health information that is transmitted or maintained in any form or medium. Individually identifiable health information is health information created or received by a health care provider or health plan, its business associate, or contractor that identifies an individual and relates to the physical or mental health or condition of an individual or relates to the provision of health care to an individual or relates to the payment for health care.

Protected health information includes individually identifiable health information (with limited exceptions) in any form, including information transmitted orally, or in written or electronic form.

**Personal Representative –** Any adult that has decision-making capacity and who is willing to act on behalf of a client and has authority, by law or by agreement from the individual receiving treatment, to act in the place of the individual. This includes parents, legal guardians or properly appointed agents, like those identified in documents like Durable Power of Attorney for Healthcare, Legal Guardian, Conservator, or individuals designated by state law.

**PURPOSE:**

The purpose of this policy is to establish parameters that protect client privacy and take necessary actions in the face of any unauthorized acquisition, access, use, or disclosures of PII or PHI. The policy clarifies: (1) timely actions; (2) obligations for reporting to affected consumers; (3) mandated reporting to appropriate agencies; (4) types of required notifications in the event of breaches in PII and/or PHI.

**DETAILS:**

**A. Levels of Notification (Notice Requirements) –** Once a risk assessment has been completed, the following actions should take place:

1. **Incidental Disclosure:** The HIPAA Privacy Rule is not intended to impede customary and necessary health care communication or practices. The Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. As long as reasonable safeguards are taken to minimize the chance of incidental disclosure to others, incidental use or disclosure is permissible only to the extent that the covered entity had applied reasonable safeguards as required by § 164.530(c), and implemented the minimum necessary standard, where applicable, as required by §§ 164.502(b) and 164.514(d). *Incidental disclosures of this kind should not be reported nor should they be recorded in the Accounting of Disclosure Log.*

2. **Incident and Breach Notification Contracted Provider:** Contracted Providers are required to report incidents and breaches to DBHS as well as completing all aspects of notification directly to affected consumers and government agencies. The following steps are required:

    a) Contract providers must notify the Division of Behavioral Health Services (DBHS) Deputy HIPAA Privacy Officer and the Contract Monitor within 24 hours of the discovery of the incident or breach by phone, email or Fax.

    b) The DBHS Deputy HIPAA Privacy Officer will notify the DBHS Deputy Director of all significant breaches.

    c) DBHS Deputy HIPAA Privacy Officer will work with the contracted provider to ensure that a Privacy Incident Report (PIR), Corrective Action Plan (CAP) and Risk Analysis (RA) and all reporting to federal authorities are completed in a timely manner.

    d) Contract providers must complete a Privacy Incident Report (PIR) detailing the circumstances of the incident or breach. Do not include PII or PHI in the detailed report. The completed PIR must be sent by email/fax to the DBHS Deputy HIPAA Privacy Officer for review and submission to the DHCS Privacy Officer. The PIR can be found at the following link or a copy sent to the provider: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx

e) Contracted providers must submit a Corrective Action Plan (CAP), for every reported breach or security incident, to the DBHS Deputy HIPAA Privacy Officer for review, approval and submission to the DHCS Privacy Office.

f) DHCS Privacy Office will assign a Case Number to be used with all further communication.

g) If a letter of breach notification to the effected beneficiaries/consumers is required, the contracted provider will send a draft letter to the DBHS Deputy HIPAA Privacy Officer for review, approval and submission to the DHCS Privacy Office. The DBHS HIPAA Privacy Officer will provide guidance for the appropriate letter format.

h) DHCS Privacy Office will approve or require additional corrections to the draft notification letter. Once approved, the contract provider will send the letter of notification to the effected beneficiaries/consumers.

i) Contracted provider must provide evidence of notification to all affected parties with a redacted copy of the notification sent-out to effected beneficiaries/consumers. Notification is sent to DBHS Deputy HIPAA Privacy Office.

j) DHCS Deputy Privacy Officer may require that the contracted provider submit a Risk Assessment.

k) Contract Provider will be notified when the case is closed.

l) Based on the following size of breaches, notification by the Contract Provider to the U.S. Secretary of Health and Human Services is also required.

   i. **Less than 500:** For breaches that affect fewer than 500 individuals, a covered entity must provide the Secretary with notice *annually*. All notifications of breaches occurring in a calendar year must be submitted within 60 days of the end of the calendar year in which the breaches occurred. This notice must be submitted electronically by following the link below http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html and completing all information required on the breach notification form. A separate form must be completed for every breach that has occurred during the calendar year. The Contract Provider must provide a copy of the breach report to the County DBHS Privacy Officer.

   ii. **More than 500:** If a breach affects 500 or more individuals, a covered entity must provide the Secretary with notice of the breach without unreasonable delay and in no case later than 60 days from discovery of the breach. This notice must be submitted electronically by following the link below and completing all information required on the breach notification form. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

   iii. If a covered entity that has submitted a breach notification form to the Secretary discovers additional information to report, the covered entity may submit an additional form, checking the appropriate box to signal that it is an updated submission.

   iv. Contract provider will provide a copy of the report to the DHCS Deputy HIPAA Privacy Officer.

**3. Incident or Breach Notification County Operated Clinic or other County Operations:**

a. County Operated Clinics or other county operations must immediately advise their respective Program Manager/Supervisor of any incident or breach. The Program Manager/Supervisor will notify the County of Sacramento Office of Compliance and DBHS Deputy HIPAA Privacy Officer. County Program Manager/Supervisor must also follow HIPAA privacy and security incident reporting protocol.

   i. Report to DTech Service Desk online at https://jira.saccounty.net/servicedesk/customer/portal/24 or via phone at 874-5555. A tracking number will be assigned for all further communications.

   ii. Complete a First Report of Incident form at http://inside.compliance.saccounty.net/Pages/IncidentReporting.aspx. Send the completed First Report of Incident form to the Office of Compliance via Email: HIPAAOffice@saccounty.net.

   iii. Complete a Corrective Action Plan (CAP).

   iv. The Office of Compliance will complete a Risk Analysis (RA).

b. County Office of Compliance will work with Division Compliance Officer and Deputy HIPAA Privacy Officer to ensure that the PIR, if applicable, CAP and RA and all reporting to federal authorities are completed in a timely manner.

c. DBHS Deputy HIPAA Privacy Officer will report the incident to DHCS, if applicable, and will work with the provider to ensure all reporting is completed in a timely manner.

d. DBHS Deputy HIPAA Privacy Officer will notify the DBHS Deputy Director of all significant breaches.

e. Clinic Manager/Program Manager must submit a draft letter of notification that a breach occurred, if required. The Office of Compliance will provide guidance, review and approve the letter of notification to be sent to the effected beneficiaries/consumers.

f. County operated clinic or operations must provide evidence of notification to all effected beneficiaries/consumers with a redacted copy of the notification that was mailed to the effected beneficiaries/consumers.

**B. Risk Assessment –** An acquisition, access, use or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.

2. The unauthorized person who used the protected health information or to whom the disclosure was made.

3. Whether the PHI was actually acquired or viewed.

4. The extent to which the risk to the protected health information has been mitigated.

**REFERENCE(S)/ATTACHMENTS:**

- California Civil Code §1798.29
- Welfare & Institution Code 5328
- 42 USC §1320d
- HIPAA 45 CFR Part 160 and Part 164, subparts A and E
- 42 U.S.C. §1320d-6(a)(2)

**RELATED POLICIES:**

- County of Sacramento HIPAA Privacy Rule and Security Rule Policies and Procedures http://inside.compliance.saccounty.net/Documents/2018%20HIPAA%20Privacy%20Rule%20P&Ps.pdf
- Office Of Compliance HIPAA First Report of Incident form. http://inside.compliance.saccounty.net/Documents/First%20Report%20of%20HIPAA%20Incident%20Form-FILLABLE%20v.2.pdf

**DISTRIBUTION:**

| Enter X | DL Name | Enter X | DL Name |
|---|---|---|---|
| X | Behavioral Health Staff Adult | X | Specific grant/specialty resource |
| X | Behavioral Health Staff Child | | |
| X | Mental Health Treatment Center | | |
| X | Adult Contract Providers | | |
| X | Children's Contract Providers | | |
| X | Substance Use and Prevention Treatment | | |

**CONTACT INFORMATION:**

- Quality Management Information QMInformation@SacCounty.net