



PRIVACY INCIDENT REPORTING FORM



The information reported in this form will be strictly confidential and will be used in part to determine whether a breach has occurred. **Do not include specific PHI or PI in this form.**

1- CASE IDENTIFYING INFORMATION

DHCS privacy case number:

Reporting entity:

DHCS internal Health plan County Other (specify):

Reporting entity's privacy incident case number:

Contact name:

Contact email:

Contact telephone number:

2- SUMMARY OF PRIVACY INCIDENT

Return completed form to: _____



3 - BREAKDOWN OF SUMMARY

Date(s) of privacy incident: Date of discovery: Date reported to DHCS:

Number of DHCS/CDSS program beneficiaries impacted; please specify which program(s) they belong to:

How many of the impacted beneficiaries are minors:

Title of person who caused the incident:

Title of unintended recipient:

Suspected malicious intent: Yes No

4 – DATA ELEMENTS

Demographic Information (check all that apply)

First name or initials	Last name	Address/ZIP
Date of birth	CIN or Medi-Cal #	Social security number
Driver's license	Membership #	Health plan name
Mother's maiden name	Image	Password
User name/email address		
Program name:		
Other:		

Financial Information (check all that apply)

Credit card/bank acct #	EBT card PIN #
Claims information	EBT card #
Other:	

Clinical Information (check all that apply)

Diagnosis/condition	Diagnosis codes	Procedure codes (CPT)
Medications	Lab results	Provider demographics
TAR #	Psychotherapy notes	Mental health data
Substance use/alcohol data		
Other:		

Please list all data elements provided by DHCS:

Please list all data elements verified by SSA:

Return completed form to: _____



5 - LOCATION OF DISCLOSED DATA

Laptop	Network server	Desktop computer
Portable electronic device	Email	Electronic record
Paper data	Smart phone	Hard drive
CD/DVD	USB thumb drive	Fax
Social media	Other:	

6 – SAFEGUARDS/MITIGATIONS/ACTIONS TAKEN IN RESPONSE TO EVENT

Was involved staff trained in HIPAA privacy/security within the past year: Yes No

Was malicious code or malware involved: Yes No N/A

Was the data encrypted per NIST standards: Yes No N/A

Status of the data (recovered, destroyed, etc.):

Was an attestation of nondisclosure/destruction obtained: Yes No

(NOTE: If a written attestation is not attached it will be considered verbal)

Was a police report filed: Yes No

Police report # and department name:

MITIGATION SUMMARY (*Immediate actions taken to prevent further unauthorized disclosure of data*)

Return completed form to: _____



7 - CORRECTIVE ACTION PLAN (CAP) - Please include implementation date
(A CAP is implemented in an attempt to prevent this type of privacy incident from reoccurring).

8 - DETERMINATION

Has your entity determined this to be a (check all that apply):

Federal breach

State breach

Non-breach

In the event DHCS determines a notification is not legally required, do you still intend to send written notification: Yes No

(Review & approval by DHCS is still required prior to dissemination of all notification letters)

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

[HITECH BREACH DEFINITION AND EXCEPTIONS](#)

Return completed form to: privacyofficer@dhcs.ca.gov