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: privacyofficer@dhcs.ca.gov

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 and Relationship to Reporting Entity:

Title of Unintended Recipient:

Suspected Malicious Intent: ◯Yes ◯No

4 – DATA ELEMENTS

DEMOGRAPHIC INFORMATION (Check all that Apply)

- ☐First Name or Initial
- ☐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
- ☐Medications
- ☐(Dx) Lab Results
- ☐(CPT) Provider
- ☐TAR #
- ☐Psychotherapy Notes
- ☐Demographics
- ☐Substance Use/Alcohol Data
- ☐Mental Health Data
- ☐Other:

Please List All Data Elements Provided by DHCS:

Please List All Data Elements Verified by SSA:

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/Malware Involved? ○Yes ○No ○N/A

Was the Data Encrypted Per NIST Standards? ○Yes ○No ○N/A

Status of Data? (i.e. Recovered, Destroyed, etc.):

Was an Attestation of Nondisclosure/Destruction Obtained? ○Yes ○No

(NOTE: If Written Attestation is Not Attached It Will be Considered Verbal)

Was a police report filed? ○Yes ○No

Police Report # and Department Name:

MITIGATION SUMMARY (Example: The data was destroyed/returned, etc.)

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 Notification is Not Legally Required, Do You Still Intend to Send Written Notification (Note: Review & approval by DHCS is still required prior to dissemination of *all* notification letters.): ◯Yes ◯No

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