

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 INFORMATION *†

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?

Return completed form to: privacyofficer@dhcs.ca.gov or fax to: (916) 440-7680

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:

Return completed form to: privacyofficer@dhcs.ca.gov or fax to: (916) 440-7680

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: privacyofficer@dhcs.ca.gov or fax to: (916) 440-7680

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:

Return completed form to: privacyofficer@dhcs.ca.gov or fax to: (916) 440-7680

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.):

Return completed form to: privacyofficer@dhcs.ca.gov or fax to: (916) 440-7680

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.

Return completed form to: privacyofficer@dhcs.ca.gov or fax to: (916) 440-7680

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 separate 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.

Return completed form to: privacyofficer@dhcs.ca.gov or fax to: (916) 440-7680