Cal HHS Data Exchange Framework Policy and Procedure

Subject: Breach Notification	
Status:	**Policy:**
Effective:	**Version**

I. Purpose

The privacy, security, and integrity of Health and Social Services Information exchanged under the California Health and Human Services Data Exchange Framework are essential. To help maintain the privacy, security and integrity of Health and Social Services Information and promote trust among Participants, each Participant has agreed to notify certain other Participants and the Governance Entity of a Breach. This Policy sets forth the procedure by which a Participant and the Governance Entity will fulfill their respective Breach notification obligations under the Data Sharing Agreement (the "DSA").

II. Policy

Breaches are very serious events with potential for serious impact on Participants and the individuals whose Health and Social Services Information is breached. Thus, each Participant has the obligation to identify, notify, investigate and mitigate any known Breach or potential Breach, and when detection of a potential Breach has occurred, to notify the Governance Entity and any affected Participants of the potential Breach in accordance with the procedures herein.

III. Procedures

1. OBLIGATIONS OF PARTICIPANT

a. As soon as reasonably practicable, but no later than two (2) calendar days after determining that a Breach has occurred, a Participant shall provide notification of the Breach to the Governance Entity and all affected Participants. In addition, as soon as reasonably practicable, but no later than ten (10) calendar days after determining that a Breach has occurred, a Participant shall provide notification of the Breach to other affected individuals and/or entities. The Participant shall supplement the information contained in the notification as it becomes available and cooperate with other impacted Participants. The notification should include sufficient information for the recipient of the notification to understand the nature of the Breach. For instance, such notification should include, to the extent available, the following information:

i. One or two sentence description of the Breach;

ii. Description of the roles of the people involved in the Breach (e.g. employees, service providers, unauthorized persons, etc.);

iii. The type of Health and Social Services Information Breached;

iv. Participants likely impacted by the Breach;

v. Number of individuals or records impacted/estimated to be impacted by the Breach;

vi. Actions taken by the Participant to mitigate the Breach;

vii. Current status of the Breach (under investigation or resolved); and

viii. Corrective action taken and steps planned to be taken to prevent a similar Breach.

b. Notwithstanding the above, Participants agree that within twenty-four (24) hours following the discovery of a Breach that may involve a Participant that is a Governmental Participant, Participants shall provide notification to all Governmental Participants that are likely impacted by the Breach in accordance with the procedures and contacts provided by such Governmental Participant.

c. Notwithstanding the above, if a Participant is notified, in writing or by oral statement by any law enforcement official or by any other governmental agency (e.g. Federal Trade Commission), that a Breach notification would impede a criminal investigation or cause damage to national security, and the statement has been documented consistent with 45 C.F.R. part 164.412(b), then the Participant shall delay the Breach notification for the time period specified by the law enforcement official and as permitted by Applicable Law.

d. This Agreement shall not relieve Participants from any other Breach reporting requirements under Applicable Law including those relating to consumer notifications.

IV. Definitions

"Breach" shall mean the unauthorized acquisition, access, disclosure, or use of Health and Social Services Information. The following activities shall not constitute a "Breach":

1. Any acquisition, access, disclosure, or use of Health and Social Services Information that is encrypted in a manner that conforms with the National Institute of Standards and Technology (NIST) standards specified in Special Publication (SP) 800-57 (as revised from time to time) or a separate methodology specified by the Secretary of the United States Secretary of Health and Human services in guidance issued pursuant to section 13402(h)(2) of Public Law 111-5;

2. Any acquisition, access, disclosure, or use of Health and Social Services Information for a legitimate business need and for a purpose either required or authorized by California Civil Code section 56 et seq. or any other Applicable Law that governs the lawful access, use, or disclosure of Health and Social Services Information; or

3. Any good faith acquisition, access, disclosure, or use of Health and Social Services Information by an employee or agent of a Participant for the purposes of this Agreement provided that the Health and Social Services Information is not used or subject to further unauthorized disclosure consistent with California Civil Code sections 1798.29 and 1798.82;

4. With regard to Governmental Participants, a disclosure of Health and Social Services Information that is required by law or permitted by California Civil Code section 1798.24 or other Applicable Law; or

5. Any other acquisition, access, use or disclosure of Health and Social Services Information set forth in 45 CFR § 164.402(1) and (2).

All other capitalized terms not defined herein shall have the same meeting as set forth in the DSA.

V. References

VI. Related Policies and Procedures

VII. Version History

	Date	Author	Comment
	April 21, 2022	CalHHS CDII	Draft for DxF Data Sharing Agreement Subcommittee review