CalHHS Data Exchange Framework Policy and Procedure

Subject: Breach Notification	
Status: ~~Final~~	**Policy: OPP-3**
Publication Date: ~~July 5, 2022~~[Month Day], 2023	**Version: 1.~~0~~01**

I. Purpose

The privacy, security and integrity of Health and Social Services Information exchanged under the California Health ~~and~~& Human Services Data Exchange Framework ("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~~shall notify certain other Participants and the ~~Governance Entity~~Center for Data Insights and Innovation ("CDII") of a Breach. ~~This Policy sets~~The purpose of this policy is to set forth the procedure by which ~~a Participant and the Governance Entity~~Participants will fulfill their ~~respective~~ Breach notification obligations under the Data Sharing Agreement (the "DSA").

II. Policy

Breaches ~~are~~can be very serious events with potential for serious impact on Participants and the individuals whose Health and Social Services Information is breached. ~~Thus,~~This policy requires each Participant ~~has the obligation~~ to identify, notify, investigate and mitigate any Breach and, when detection of a Breach has occurred, to notify ~~the Governance Entity~~CDII and any Participants impacted by the Breach in accordance with the procedures herein.

This policy shall be effective as of January 31, 2024.

III. Procedures

1. OBLIGATIONS OF PARTICIPANT

a. As soon as reasonably practicable after discovering a Breach has occurred, and within any timeframes required by Applicable Law, a Participant shall notify ~~the Governance Entity~~CDII and all Participants impacted by the Breach.

b. As soon as reasonably practicable after discovering a Breach has occurred, and within any timeframes required by Applicable Law, a Participant shall provide a written report of the Breach to ~~the Governance Entity and~~ all Participants impacted by the Breach. The Participant shall supplement the information contained in the written report as it becomes available and shall cooperate with other impacted Participants. The written report should include sufficient information for the recipient of the notification to understand the nature of the Breach. For instance, such written report 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);

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.

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 Applicable Law or 45 C.F.R. § 164.412(b~~),~~) in the absence of Applicable Law, then the Participant shall delay the Breach notification for the time period specified by the law enforcement official and as required by Applicable Law. The Participant shall issue a Breach notification promptly once law enforcement determines the notification will not impede a criminal investigation.

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 in a manner not permitted by the DSA or Applicable Law. This includes both:~~

~~1. Unencrypted data that was, or is reasonably believed to have been, acquired by an unauthorized person, and~~

~~2. Encrypted data that was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or has been reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that data readable or usable.~~

All ~~other~~ capitalized terms ~~not defined herein~~ shall have the ~~same~~ meaning ~~as~~ set forth in the ~~DSA~~Data Exchange Framework Glossary of Defined Terms.

V. References

~~VI. Related Policies and Procedures~~

Subject: Breach Notification	
Status: ~~Final~~	**Policy: OPP-3**
Publication Date: ~~July 5, 2022~~[Month Day], 2023	**Version: 1.~~0~~01**

45 C.F.R. § 164.412(b)

~~VII.~~VI. Version History

No.	Date	Author	Comment
1.0	July 1, 2022	CalHHS CDII	Final
	October 24, 2023	CalHHS CDII	Amended draft for public input (administrative changes only).