

# Cal HHS Data Exchange Framework Policy and Procedure

|   |                |
|---|----------------|
| <b>Subject: Privacy Standards and Security Safeguards</b> |                |
| <b>Status:</b>  | <b>Policy:</b> |
| <b>Effective:</b>   | <b>Version</b> |

## **I. Purpose**

The privacy, security, and integrity of PHI or PII exchanged under the California Health and Human Services Data Exchange Framework are essential. To help maintain the privacy, security and integrity of PHI or PII and promote trust among Participants, each Participant has agreed to use appropriate safeguards to protect the privacy of PHI or PII, and has agreed to maintain a secure environment that supports the exchange of PHI or PII. This Policy sets forth the procedure by which a Participant will fulfill such obligations under the Data Sharing Agreement (the “DSA”).

## **II. Policy**

Using appropriate safeguards to protect the privacy of PHI or PII and maintaining a secure environment that supports the exchange of PHI or PII is an important component to prevent unauthorized disclosure, disruption, loss, access, use, or modification of an organization’s data. Thus, each Participant has the obligation to develop and maintain appropriate safeguards to prevent unauthorized use or disclosure of PHI or PII, in a manner consistent with HIPAA Regulations, including implementing appropriate administrative, physical and technical safeguards that protect the confidentiality, integrity and availability of PHI or PII.

## **III. Procedures**

### **1. PRIVACY STANDARDS AND SAFEGUARDS**

a. To support the privacy, confidentiality and security of PHI or PII, each Participant hereby represents and warrants:

i. If the Participant is a Covered Entity or a covered component of a Hybrid Entity, the Participant does, and at all times shall, comply with the HIPAA Regulations to the extent applicable and with Applicable Law.

ii. If the Participant is a Business Associate, the Participant does, and at all times shall, comply with the provisions of its Business Associate Agreements (or for governmental entities relying upon 45 C.F.R. section 164.504(e)(3)(i)(A), its Memoranda of Understanding) and Applicable Law.

iii. Unless otherwise prohibited by Applicable Law, if the Participant is not a Covered Entity, a covered component of a Hybrid Entity or a Business Associate, the Participant shall, as a contractual standard, at all times, at a minimum, comply with the provisions of the HIPAA Regulations at 45 C.F.R. part 164, subparts C and E, as if it were acting in the capacity of a Business Associate.

b. Each Participant shall be responsible for maintaining a secure environment that supports the exchange of PHI or PII pursuant to the DSA. Each Participant, regardless of whether it, pursuant to federal law, is subject to the HIPAA Regulations, shall use appropriate

safeguards to prevent unauthorized use or disclosure of PHI or PII in a manner consistent with HIPAA Regulations, including implementing appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of PHI or PII. Participants shall also be required to comply with any Specifications or other applicable Policies and Procedures that define requirements and expectations for Participants with respect to enterprise privacy and security. Each Participant acknowledges a Participant does not become a Business Associate of another Participant by virtue of signing the DSA or exchanging PHI or PII pursuant to the DSA.

**2. POLICIES AND PROCEDURES; TRAINING**

a. Each Participant shall, pursuant to this Agreement, Applicable Law, or applicable federal and state guidance, have written privacy and security policies relating to the use and disclosure of PHI or PII that are consistent with and satisfy the requirements set forth in the HIPAA Regulations. Before granting access to PHI or PII, each Participant shall train staff, contractors, agents, employees, and workforce members, as defined under the HIPAA Regulations, who will have access to PHI or PII under this Agreement. Each Participant shall also provide refresher training consistent with each Participant’s internal privacy and security policies but no less than annually.

**IV. Definitions**

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

**V. References**

**VI. Related Policies and Procedures**

**VII. Version History**

|  | <b>Date</b>    | <b>Author</b> | <b>Comment</b>   |
|--|----------------|---------------|--|
|  | April 21, 2022 | CalHHS CDII   | Draft for DxF Data Sharing Agreement Subcommittee review           |
|  | May 12, 2022   | CalHHS CDII   | Draft for DxF Stakeholder Advisory Group review and public comment |