CalHHS Data Exchange Framework Policy and Procedure

Subject: Privacy Standards and Security Safeguards	
Status:	**Policy: OPP-6**
Publication Date:	**Version: 1.1**

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 are important components 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.

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

III. Procedures

1. GENERAL 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 all other 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 all other 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 and all other Applicable Law.

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.

c. Each Participant shall access, use, maintain, and disclose Health and Social Services Information consistent with Applicable Law and any valid Authorization. In the event a Participant receives information about an Individual in error, the Participant, as soon as practicable, must securely destroy the information and notify the Participant that erroneously disclosed the information. In addition, the Participant must comply with any obligations the Participant may have under the Breach Notification Policy and Procedure.

2. **PRIVACY STANDARDS AND SAFEGUARDS RELATING TO BEHAVIORAL HEALTH**

a. In the event that a Participant uses, accesses, or discloses behavioral health information, Participant shall, prior to engaging in any such activity, implement appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of such information in accordance with Applicable Law, including but not limited to, 42 C.F.R. Part 2 and the California Lanterman-Petris-Short Act.

3. **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 and Applicable Law. 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.

b. Participants should use tools, resources, and technical assistance made available by the California Health and Human Services Agency to help Individual Users and/or their Personal Representatives understand the benefits of information sharing and for obtaining informed consent.

IV. Definitions

"**Authorization**" shall have the meaning and include the requirements set forth at 45 CFR § 164.508 of the HIPAA Regulations and at Cal. Civ. Code § 56.05. The term shall include all requirements for obtaining consent to disclose confidential substance abuse disorder treatment records as set forth in 42 C.F.R. Part 2, when applicable, and shall include any additional requirements under Applicable Law to disclose PHI or PII.

"**Business Associate**" shall mean an organization that is defined as a "business associate" in 45 C.F.R. § 160.103 of the HIPAA Regulations.

"**Hybrid Entity**" shall have the same meaning as set forth in 45 C.F.R. § 164.103.

"**Individual**" means a patient or a person who is the recipient of services, including Social Services.

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

V. References

VI. Related Policies and Procedures

Breach Notification Policy and Procedure

VII. Version History

	Date	Author	Comment
	July 1, 2022	CalHHS CDII	Final
	January 13, 2023	CalHHS CDII	Revised draft for public comment