

CalHHS Data Exchange Framework Policy and Procedure

Subject: Privacy Standards and Security Safeguards	
Status: Final	Policy: OPP-6
Publication Date: November 15, 2023	Version: 2.0

I. Purpose

California Health and Safety Code § 130290 establishes the creation of the California Health & Human Services Data Exchange Framework (“Data Exchange Framework”), which requires certain data sharing among Participants. The privacy, security, and integrity of Health and Social Services Information Exchanged under the Data Exchange Framework are essential. To help ensure the privacy, security, and integrity of Health and Social Services Information and promote trust among Participants, each Participant shall do all of the following as described in this policy:

1. Use appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity and availability of Health and Social Services Information;
2. Use a secure environment that supports the Exchange of Health and Social Services Information;
3. Protect against unauthorized Disclosure, Access, Use, modification, or Exchange of Health and Social Services Information; and
4. Protect against any Loss or Destruction of Health and Social Services Information and any Disruption of authorized Access or Exchange of Health and Social Services Information.

The purpose of this policy is to set forth the procedure by which a Participant will fulfill such obligations under the Data Sharing Agreement (“DSA”).

II. Policy

This policy requires Participants to develop, implement, and uphold administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Health and Social Services Information. This policy requires Participants to store Health and Social Services Information in a secure environment that supports the Access, Use, or Exchange of Health and Social Services Information and prevents Loss, Destruction, or Disruption and unauthorized Disclosure, Access, Use, modification, or Exchange of Health and Social Services Information consistent with Applicable Law.

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

III. Procedures

1. GENERAL PRIVACY STANDARDS AND SAFEGUARDS

a. All Participants

i. General Privacy Requirements.

a. Each Participant shall only Access, Use, Maintain, and Disclose Health and Social Services Information consistent with Applicable Law and any valid Authorization.

CalHHS Data Exchange Framework Policy and Procedure

Subject: Privacy Standards and Security Safeguards	
Status: Final	Policy: OPP-6
Publication Date: November 15, 2023	Version: 2.0

b. A Participant that receives any Health and Social Services Information pursuant to the DSA shall comply with all Applicable Law related to such Health and Social Services Information. Such laws may include, but are not limited to, HIPAA Regulations, 42 C.F.R. Part 2, the California Consumer Privacy Act, the California Confidentiality of Medical Information Act, the Information Practices Act, the Lanterman-Petris-Short Act, the Lanterman Developmental Disabilities Services Act, and California Health and Safety Code § 11845.5. Nothing in this section requires a Participant to comply with laws that would not otherwise apply to such Participant or the Health and Social Services Information a Participant receives.

c. Participants shall only Exchange abortion or abortion-related services information or gender affirming care information in compliance with Applicable Law.

ii. De-Identification. A Participant may de-identify and use Health and Social Services Information received from another Participant under the DSA and Use or Disclose such De-Identified Health and Social Services Information so long as permitted by Applicable Law and consistent with this section. Prior to Using or Disclosing De-Identified Health and Social Services Information, a Participant shall ensure the Health and Social Services Information has been De-Identified consistent with 45 C.F.R. Part 164.514(b) or consistent with other more stringent Applicable Law. Nothing in this section requires Participants to De-Identify Health and Social Services Information prior to Exchanging with another Participant under the DSA. Participants may not sell de-identified Health and Social Services Information when that de-identified Health and Social Services Information includes information received from another Participant.

b. Participants who are Covered Entities or Business Associates under the HIPAA Regulations.

i. If the Participant is a Covered Entity or a covered component of a Hybrid Entity, the Participant shall comply with the HIPAA Regulations as applicable and all other Applicable Law.

ii. If the Participant is a Business Associate, the Participant shall comply with the privacy and security provisions of its Business Associate Agreements (or for governmental entities relying upon 45 C.F.R. § 164.504(e)(3)(i)(A), its memoranda of understanding) and all other Applicable Law.

iii. If the Participant is a Covered Entity or Business Associate, the Participant shall comply with the Policies and Procedures and shall update its Business Associate Agreements or memoranda of understanding if they conflict with the Policies and Procedures.

iv. Nothing in this section shall require a Participant to execute a Business Associate Agreement to Exchange Health and Social Services Information under the DSA if a Business Associate Agreement is not required under Applicable Law.

c. Participants who are not Covered Entities, covered components of a Hybrid Entity, or Business Associates under the HIPAA Regulations.

CalHHS Data Exchange Framework Policy and Procedure

Subject: Privacy Standards and Security Safeguards	
Status: Final	Policy: OPP-6
Publication Date: November 15, 2023	Version: 2.0

i. Protected Health Information (PHI). A Participant that is not a Covered Entity, a covered component of a Hybrid Entity, or a Business Associate shall comply with the following provisions of the HIPAA Regulations and all other Applicable Law with respect to any PHI the Participant receives as follows:

a. The Participant may only Access, Use, or Disclose PHI received from a Participant as set forth in the Permitted, Required, and Prohibited Purposes Policy and Procedure;

b. The Participant shall comply with the minimum necessary standards set forth at 45 C.F.R. §§ 164.502(b) and 164.514(d) with respect to PHI; and

c. The Participant shall comply with the verification requirements and specifications set forth at 45 C.F.R. § 164.514(h) with respect to PHI.

ii. Personally Identifiable Information (PII). This section shall only apply to PII that is not PHI. A Participant that is not a Covered Entity, a covered component of a Hybrid Entity, or a Business Associate shall comply with the following and Applicable Law with respect to any PII the Participant receives as follows:

a. The Participant may not Access, Use, or Disclose PII received from another Participant except as permitted or required by Applicable Law, or in the absence of Applicable Law, the Participant's contracts;

b. In the absence of Applicable Law, the Participant shall only Access, Use, or Disclose PII to the extent necessary to achieve the purpose of the Access, Use, or Disclosure for which the Participant received the PII; and

c. The Participant shall comply with the verification requirements and specifications set forth at 45 C.F.R. § 164.514(h)(1) and (2)(i) with respect to PII.

2. GENERAL SECURITY STANDARDS AND SAFEGUARDS

a. Each Participant, regardless of whether it is subject to the HIPAA Regulations, shall develop, implement, and uphold appropriate administrative, physical, and technical safeguards and controls that:

i. Protects the confidentiality, integrity, and availability of Health and Social Services Information;

ii. Establishes a secure environment that supports the Exchange of Health and Social Services Information; and

iii. Protects against any Loss, Destruction, or Disruption and unauthorized Disclosure, Access, Use, modification, or Exchange of Health and Social Services Information.

CalHHS Data Exchange Framework Policy and Procedure

Subject: Privacy Standards and Security Safeguards	
Status: Final	Policy: OPP-6
Publication Date: November 15, 2023	Version: 2.0

a. If the Participant is a Covered Entity, Business Associate, or a covered component of a Hybrid Entity, the Participant shall comply with the HIPAA Security Rule and all other Applicable Law.

b. A Participant who is not a Covered Entity, Business Associate, or covered component of a Hybrid Entity shall at all times, at a minimum, comply with the following provisions of the HIPAA Regulations and all other Applicable Law with respect to the Health and Social Services Information, as follows:

(i) The Participant shall implement appropriate standards and administrative, physical, and technical safeguards consistent with 45 C.F.R. §§ 164.306, 164.308, 164.310, and 164.312.

b. **Secure Destruction.** In the event a Participant discovers that it has received Health and Social Services Information about an Individual in error, the receiving Participant must, as soon as practicable, Securely Destroy the information and notify the Participant that erroneously Disclosed the information. In addition, both Participants shall comply with any obligations they may have under the Breach Notification Policy and Procedure and any Applicable Law.

3. **PRIVACY STANDARDS AND SAFEGUARDS RELATING TO SPECIALLY PROTECTED BEHAVIORAL HEALTH INFORMATION**

a. Participants that Use, Access, or Disclose behavioral health information that is subject to special protection under Applicable Law, including but not limited to 42 C.F.R. Part 2, California Health and Safety Code § 11845.5, California Lanterman-Petris-Short Act (*see* Cal. Welf. & Inst. Code § 5328 et seq.), Lanterman Developmental Disabilities Services Act (*see* Cal. Welf. & Inst. Code § 4514 et seq.), and to the extent applicable to outpatient behavioral health information, the California Confidentiality of Medical Information Act (*see* Cal. Civ. Code § 56 et seq.) shall implement appropriate administrative, physical, and technical safeguards and controls that protect the confidentiality, integrity, and availability of such information in accordance with Applicable Law. Participants shall also comply with all Applicable Law that applies to specially protected Health and Social Services Information.

4. **POLICIES AND PROCEDURES; TRAINING**

a. **Policies and Procedures.** Participants shall have written privacy and security policies and procedures to support Access, Use and Disclosure of Health and Social Services Information and prevent Loss, Destruction, Disruption, or unauthorized Disclosure, Access, Use, modification, or Exchange of Health and Social Services Information that are consistent with and satisfy the requirements set forth in Applicable Law and/or this policy. Participants shall review and update their privacy and security policies and procedures as needed, and no less than annually.

b. **Training.** Before granting Access to Health and Social Services Information each Participant shall properly train staff, contractors, agents, employees, and other members of the Workforce. At minimum, each Participant shall implement appropriate roles-based information security training and privacy training. Among other things, privacy trainings shall address

CalHHS Data Exchange Framework Policy and Procedure

Subject: Privacy Standards and Security Safeguards	
Status: Final	Policy: OPP-6
Publication Date: November 15, 2023	Version: 2.0

Applicable Law governing the Health and Social Services Information that the Participant will be Accessing, Using or Disclosing. Each Participant shall also provide refresher training consistent with each Participant’s internal privacy and security policies but no less than annually.

c. Record Retention. Participants shall store records of trainings for at least six (6) years, or such longer period as may be required by Applicable Law.

d. Participants may use tools and resources made available by the California Health & Human Services Agency to help Individual Users and/or their Personal Representatives understand information sharing requirements under Applicable Law, including when Authorization from an Individual is required to share Health and Social Services Information.

IV. Definitions

All capitalized terms shall have the meaning set forth in the Data Exchange Framework Glossary of Defined Terms.

V. References

42 C.F.R. Part 2

45 C.F.R. Parts 160 and 164

Breach Notification Policy and Procedure

Permitted, Required, and Prohibited Purposes Policy and Procedure

California Confidentiality of Medical Information Act

California Health and Safety Code § 130290

California Health and Safety Code § 11845.5

Lanterman Development Disabilities Services Act

California Lanterman-Petris-Short Act

[HHS FAQ 575: What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?](#)

CalHHS Data Exchange Framework Policy and Procedure

Subject: Privacy Standards and Security Safeguards	
Status: Final	Policy: OPP-6
Publication Date: November 15, 2023	Version: 2.0

VI. Resources

[California Hospital Association Consent Manual \(2021\)](#)

[State Health Information Guidance \(SHIG\)](#)

VII. Version History

No.	Date	Author	Comment
1.0	July 1, 2022	CalHHS CDII	Final
2.0	November 15, 2023	CalHHS CDII	Final. Amended in response to public comment and stakeholder feedback and to make administrative changes to clarify use of certain terms and ensure consistency with the DxF Glossary of Defined Terms.