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 Protected Health Information ("PHI") and/or Personally Identifiable Information ("PII") 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 PHI and/or PII and promote trust among Participants, each Participant shall do all of the following as described in this policy:

1. Use appropriate safeguards to protect the privacy and security of PHI and/or PII;

2. Maintain a secure environment that supports the Exchange of PHI and/or PII;

3. Protect against unauthorized Disclosure, Access, Use, disruption or modification of PHI and/or PII; and

4. Protect against any loss of PHI and/or PII.

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 maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI and/or PII and a secure environment that supports the Access, Use, or Exchange of PHI and/or PII and prevents unauthorized Disclosure, disruption, loss, Access, Use, or modification of Health and Social Services Information consistent with Applicable Law and this policy.

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.

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

(ii) If a Participant receives any PHI and/or PII pursuant to the DSA, the receiving Participant shall comply with all Applicable Law with respect to such PHI

and/or PII. Such laws may include, but are not limited to, 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 section 11845.5.

ii. De-Identification. A Participant shall De-Identify any PHI and/or PII received from another Participant consistent with the provisions of 45 C.F.R. part 164.514(b) prior to Using or Disclosing de-identified or anonymized information.

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 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.

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

i. 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 at all times, at a minimum, comply with the following provisions of the HIPAA Regulations and all other Applicable Law with respect to any PHI and/or PII the Participant receives under the DSA:

(i) The Participant may not Use or Disclose PHI and/or PII received from a Participant except as set forth in 45 C.F.R. section 164.502(a)(1)(i) through (v), including with a valid Authorization, or as otherwise permitted by Applicable Law;

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

(iii) The Participant shall comply with the verification requirements and specifications set forth at 45 C.F.R. section 165.514(h).

2. GENERAL SECURITY STANDARDS AND SAFEGUARDS

a. Each Participant shall develop, implement and maintain appropriate administrative, physical, and technical safeguards and controls that protect the confidentiality, integrity, and availability of Health and Social Services Information and a secure environment that supports the Exchange of PHI and/or PII and protects against any unauthorized Disclosure, Access, or Use and disruption, loss, or modification of PHI and/or PII. Each Participant, regardless of

whether it, pursuant to federal law, is subject to the HIPAA Regulations, shall use appropriate safeguards to prevent unauthorized Disclosure, Access, or Use and disruption, loss, or modification of PHI and/or PII.

i. 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.

ii. 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 such PHI and/or PII, as follows:

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

b. Secure Destruction. In the event a Participant discovers that it has received PHI and/or PII about an Individual in error, it 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 section 11845.5, California Lanterman-Petris-Short Act (*see* Cal. Welf. & Inst. Code § 5328, et seq.)., Lanterman Development Disabilities Services Act (*see* Cal. Welf. & Inst. Code § 4400 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.) (the "Behavioral Health Laws and Regulations") 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, including but not limited to, the Behavioral Health Laws and Regulations.

4. POLICIES AND PROCEDURES; TRAINING

a. Participants shall have written privacy and security policies and procedures to support Access, Use, Disclosure of PHI and/or PII and prevent disruption, modification or loss of PHI and/or PII that are consistent with and satisfy the requirements set forth in Applicable Law and/or this policy. Before granting Access to PHI and/or PII, each Participant shall properly train staff, contractors, agents, employees, and other members of the Workforce. At minimum, each Participant shall implement information security training and privacy training. Among other things, privacy trainings shall address Applicable Law governing the Health and Social Services Information that the Participant will be Accessing, Using or Disclosing under the DSA. Each

Participant shall also provide refresher training consistent with each Participant's internal privacy and security policies but no less than annually. Participants shall maintain records of trainings for at least three (3) years, or such longer period as may be required by Applicable Law.

IV. Definitions

"**Access**" means the ability or means necessary to make Health and Social Services Information available for Exchange or Use.

"**Applicable Law**" means all federal, state, local, or tribal laws and regulations then in effect and applicable to the subject matter herein. For the avoidance of doubt, federal government entities are only subject to federal law.

"**Authorization**" shall have the meaning and include the requirements set forth at 45 C.F.R. § 164.508 of the HIPAA Regulations and at Cal. Civ. Code §§ 56.05, 56.11, and 56.21. 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. §§ 2.31 and 2.33, when applicable, and shall include any additional requirements under Applicable Law to disclose PHI or PII.

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

"Covered Entity" shall have the meaning set forth at 45 C.F.R. § 160.103 and shall also include the following as these terms are defined in California Civil Code § 56.05: "provider of health care," "health care service plan," and "licensed health care professional."

"**De-identify**" means health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual, as the term is used in 45 C.F.R. § 165.514.

"Disclose" or "Disclosure" means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

"**Exchange**" means the transmittal of Health and Social Services Information between and among different technologies, systems, platforms, or networks.

"Governance Entity" means the entity within the California Health and Human Services Agency established to oversee the California Data Exchange Framework, the DSA and the Policies and Procedures.

"Health and Social Services Information" means any and all information received, stored, processed, generated, used, transferred, disclosed, made accessible, or shared pursuant to the DSA, including but not limited to: (a) data elements as set forth in the applicable Policy and Procedure; (b) information related to the provision of health care services, including but not limited to Protected Health Information (PHI); and (c) information related to the provision of social services. Health and Social Services Information may include PHI, Personally Identifiable Information (PII),

de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), anonymized data, pseudonymized data, metadata, digital identities, and schema.

"HIPAA Regulations" means the standards for privacy of individually identifiable health information, the security standards for the protection of electronic protected health information and the breach notification rule (45 C.F.R. Parts 160 and 164) promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as in effect and as may be amended, modified, or renumbered**.**

"**HIPAA Security Rule**" means the security standards for the protection of electronic protected health information (45 C.F.R. Part 164, Subpart C) promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as in effect and as may be amended, modified, or renumbered.

"**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.

"Participant(s)" means each health care organization as set forth in California Health and Safety Code § 130290(f) and any other person or organization that is a signatory to the DSA. Participants may include, but are not limited to, a health information network, a community information exchange, a laboratory, a health system, a health information technology (IT) developer, a community-based organization, a payer, a government agency, a research institute, or a Social Services Organization.

"**Personal Representative,**" means a person who, under Applicable Law, has authority to make health care decisions on behalf of an Individual as set forth in 45 C.F.R. § 164.502(g) and Health and Safety Code 123105(e).

"Personally Identifiable Information" or "PII" shall have the same meaning as "Personal Information" set forth in Section 1798.140(v) of the California Civil Code, but shall be limited to PII Exchanged pursuant to the DSA.

"Policies and Procedures" means the policies and procedures adopted by the Governance Entity pursuant to the DSA.

"Protected Health Information" or "PHI" means "protected health information" as set forth at 45 C.F.R. § 160.103 of the HIPAA Regulations and "medical information" as set forth at Civil Code § 56.05.

"**Securely Destroy**" means consistent with Applicable Law and with generally accepted industry standards.

"Social Services" means the delivery of items, resources, and/or services to address social determinants of health and social drivers of health, including but not limited to housing, foster care, nutrition, access to food, transportation, employment, and other social needs.

"Social Services Organization" means a person or entity whose primary business purpose is to provide Social Services to individuals. Social Services Organizations can include but are not limited to government entities (including multi-department health and human services agencies), community-based organizations, nonprofits, and private entities.

"**Use**" means the ability for Health and Social Services Information, once Accessed or Exchanged, to be understood and acted upon.

"**Workforce**" means employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for a Participant, is under the direct control of the Participant, whether or not they are paid by the Participant.

V. References

42 C.F.R. Part 2

45 C.F.R. Parts160 and 164

California Civil Code § 56.05

California Civil Code § 1798.140(v)

California Confidentiality of Medical Information Act

California Health and Safety Code § 130290(f)

California Health and Safety Code § 11845.5

Lanterman Development Disabilities Services Act

California Lanterman-Petris-Short Act

VI. Related Policies and Procedures

Breach Notification Policy and Procedure

VII. Version History

	Date	Author	Comment
	July 1, 2022	CalHHS CDII	Final
	June 2, 2023	CalHHS CDII	Amended draft for IAC and DSA P&P Subcommittee review