

# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

## I. Purpose

California Health and Safety Code § 130290 establishes that the California Health and Human Services Data Exchange Framework (“Data Exchange Framework”) will create a “common set of policies and procedures that will leverage and advance national standards for information exchange and data content, and that will govern and require the exchange of health information” among Participants. The purpose of this policy is to define recommended and required exchanges of Health and Social Services Information among Participants and the technical standards to be used in those exchanges.

## II. Policy

This policy establishes minimum technical requirements for the Access, Exchange, and Use of Health and Social Services Information. To comply with this policy, Participants must Exchange Health and Social Services Information for a Required Purpose between Participant systems in such a way that the receiving Participant’s system can Use the Health and Social Services Information without special effort on the part of the user.

This policy shall be effective January 31, 2024.

1. Request for Information is a request by a Participant for Health and Social Services Information regarding a specific Individual from one or more Participant(s) and the associated response(s) of Participant(s) to that request.

a. Requesting Participants

i. A Participant that makes a Request for Information from a Participant or Participants using a Nationwide Network or Framework must make the request using the *Integrating the Healthcare Enterprise (IHE) Cross-Community Patient Discovery (XCPD)* exchange profile for Person Matching to determine if a Participant Maintains Health and Social Services Information for an Individual, if necessary, and the *IHE Cross-Community Access (XCA)* exchange profile to retrieve Health and Social Services Information.

ii. Participants are strongly discouraged from making a Request for Information to a large or unbounded number of Participants (a.k.a., broadcast query) except if, in the professional judgment of the Participant, receipt of the information is urgent or constitutes an emergency impacting patient safety and when potential sources of Health and Social Services Information for the Individual are not known. To the extent practicable, Participants are encouraged to follow health information technology industry best practices in using health information exchange, health information networks, and health information frameworks when making Requests for Information from a large number of Participants, for example, by directing requests only to Participants within a geographic region.

b. Responding Participants

# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

i. Every Participant must accept and respond to an electronic Request for Information from another Participant.

ii. Every Participant that responds to a Request for Information from a Participant using a Nationwide Network or Framework or a point-to-point connection must support requests and responses using the *IHE Cross-Community Patient Discovery (XCPD)* exchange profile for Person Matching and the *IHE Cross-Community Access (XCA)* exchange profile to retrieve Health and Social Services Information.

iii. A Participant must respond to a Request for Information with an appropriate null response or error message if required by the technical exchange standard in use and in compliance with this policy if the Participant receiving the Request for Information cannot fulfill the request for any of the following reasons:

a. The Participant cannot determine a matching Individual for the attributes and identifiers supplied in the request,

b. The Participant determines that multiple persons may match the attributes and identifiers supplied in the request,

c. The Participant does not Maintain Health and Social Services Information for the Individual, or

d. The Participant determines that the Health and Social Services Information for the Individual cannot lawfully be shared under Applicable Law or otherwise meets an exception in the California Information Blocking Prohibitions Policy and Procedure.

c. All Participants

i. A Participant that uses an Intermediary to make a Request for Information or to respond to a Request for Information may use any open technical standard compliant with the Privacy Standards and Security Safeguards Policy and Procedure that is supported by both the Participant and the selected Intermediary. For requests or responses beyond the Intermediary's participants, the Intermediary must be able to translate the request or response into the *IHE Cross-Community Patient Discovery (XCPD)* exchange profile for Person Matching and the *IHE Cross-Community Access (XCA)* exchange profile for exchange of Health and Social Services Information.

ii. A Participant that makes a Request for Information or responds to a Request for Information using a point-to-point interface may use any open technical standard compliant with the Privacy Standards and Security Safeguards Policy and Procedure and supported by both the Participants.

# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

iii. Participants are encouraged to support Requests for Information using *Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) Release 4* conforming to the *US Core Implementation Guide*. This request and response standard may be required in future revisions of this policy.

2. Information Delivery is the delivery of Health and Social Services Information regarding a specific Individual to a specific Participant in conjunction with an Order or Referral.

a. Sending Participants

i. A Participant that creates Health and Social Services Information regarding a specific Individual in conjunction with an Order or Referral must send that Health and Social Services Information to the ordering Participant electronically via Information Delivery if the ordering Participant is technically capable of electronic receipt.

a. A sending Participant is strongly encouraged to include only that information in Information Delivery created specifically in fulfillment of the Order or Referral, (only that information necessary to communicate the diagnostic, assessment, evaluation, or consultation results produced by the sending Participant).

b. A sending Participant must communicate via Information Delivery a change in status of a previous result for the same Order or Referral, such as a transition from a preliminary result to a final result.

c. A sending Participant is not required to send Health and Social Services Information that is not associated with the Order or Referral, or to continue delivering diagnostic, assessments, evaluations, or consultations results after the Order or Referral is complete.

ii. A sending Participant using a Nationwide Network or Framework for Information Delivery must support delivery using: the *IHE Cross-Enterprise Document Reliable Interchange (XDR)* or *IHE Cross-Community Document Reliable Interchange (XCDR)* exchange profiles.

iii. A sending Participant may use the *Applicability Statement for Secure Health Transport (a.k.a., Direct Secure Messaging)* for Information Delivery if supported by both Participants.

iv. A sending Participant using a point-to-point interface for Information Delivery may use any open technical standard compliant with the Privacy Standards and Security Safeguards Policy and Procedure and supported by both Participants.

v. A sending Participant is encouraged to support delivery using *HL7 Fast Healthcare Interoperability Resources (FHIR) Release 4* conforming to the *US Core*

# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

*Implementation Guide* for Information Delivery. This delivery standard may be required in future revisions of this policy.

b. Receiving Participants

i. A receiving Participant using a Nationwide Network or Framework for Information Delivery must support receipt using the *IHE Cross-Enterprise Document Reliable Interchange (XDR)* or *IHE Cross-Community Document Reliable Interchange (XCDR)* exchange profiles.

ii. A receiving Participant may use the *Applicability Statement for Secure Health Transport (a.k.a., Direct Secure Messaging)* for Information Delivery if supported by both Participants.

iii. A receiving Participant is encouraged to support receipt using *HL7 Fast Healthcare Interoperability Resources (FHIR) Release 4* conforming to the *US Core Implementation Guide* for Information Delivery. This delivery standard may be required in future revisions of this policy.

c. All Participants

i. A Participant that uses an Intermediary for Information Delivery may use any open technical standard compliant with the Privacy Standards and Security Safeguards Policy and Procedure and supported by both the Participant and the selected Intermediary. For delivery beyond the Intermediary’s participants, the Intermediary must be able to translate the delivery into the *IHE Cross-Enterprise Document Reliable Interchange (XDR)* or *IHE Cross-Enterprise Document Reliable Interchange (XCDR)* exchange profiles for Information Delivery.

ii. Nothing in this policy requires or prohibits that an Order or Referral be sent electronically.

iii. Nothing in this policy limits the delivery of Health and Social Services Information only to those Participants that create Health and Social Services Information in response to an Order or Referral.

iv. Nothing in this policy alters or limits the obligations of a Participant regarding public health reporting, technical standards for public health reporting, or other requirements for public health reporting as specified by Applicable Law.

3. Notification of Admit, Discharge, Transfer (ADT) Events is the communication of ADT Events sent by a sending Participant to a receiving Participant for specified Individuals requested by the receiving Participant.

a. Hospital and Emergency Department Participants

# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

i. Participants that are Hospitals or Emergency Departments must send Notification of ADT Events unless prohibited by Applicable Law.

ii. Participants that are Hospitals or Emergency Departments must accept requests for Notification of ADT Events from any other Participant and send Notification of ADT Events as requested using a secure method compliant with the Privacy Standards and Security Safeguards Policy and Procedure and in a format acceptable to the requesting Participant and supported by the Participant Hospital or Emergency Department.

iii. Participants that are Hospitals or Emergency Departments are required to send Notification of ADT Events to a Participant only if requested by the Participant in advance of the ADT Event. This policy does not require that a Hospital or Emergency Department, or its Intermediary, send Notifications of ADT Events for historical ADT Events that took place prior to a request for Notifications of ADT Events by another Participant.

b. Other Participants Sending Notifications of ADT Events

i. Participants that are skilled nursing facilities are encouraged to communicate admissions, discharges, and transfers to requesting Participants using the same methods as Hospitals or Emergency Departments. Skilled nursing facilities may be required to communicate admissions, discharges, and transfers in future revisions of this policy.

c. Requesting Participants

i. Any Participant may make a request for electronic Notification of ADT Events from a Hospital or Emergency Department.

ii. Participants that make requests for Notification of ADT Events must submit a roster identifying the Individuals for whom Notifications of ADT Events are requested consistent with the attributes for Person Matching or using some other method acceptable to the sending Participant.

iii. Participants that make requests for Notification of ADT Events must make the request in advance of the ADT Events. This policy does not require that a Participant send Notifications of ADT Events for historical ADT Events that took place prior to a request for Notifications of ADT Events.

d. All Participants

i. Nothing in this policy limits the responsibility of a Participant to send Notifications of ADT Events as may be required by Applicable Law.

# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

ii. Nothing in this policy limits a Participant that is a Hospital or Emergency Department from using an Intermediary to meet its obligations to accept requests for Notifications of ADT Events and/or send Notifications of ADT Events.

iii. Nothing in this policy limits the responsibility of a Hospital or Emergency Department or other Participant to execute agreements, such as a Business Associate Agreement, as required by Applicable Law prior to the exchange of Notifications of ADT Events.

4. Person Matching is the process by which a Participant ensures that exchanged Health and Social Services Information is appropriately linked to the correct real person.

a. For Requests for Information, Information Delivery, and Notifications of ADT Events, all Participants must use the following data attributes for Person Matching if Maintained by the Participant and supported by the technical exchange standard in use when specifying an Individual to match in a Request for Information, or identifying an Individual in Information Delivery or Notifications of ADT Events:

i. Name, including family name, given name(s), and middle name or initial, and including other names previously or currently used by the individual, including aliases if documented by the Participant.

ii. Date of birth

iii. Home and/or mailing address(es), including previous address(es) if known

iv. Phone number(s)

v. Email address(es)

b. Unless noted otherwise in this policy or in the Data Elements to Be Exchanged Policy and Procedure, data attributes for Person Matching must follow the guidelines and standards established by the *United States Core Data for Interoperability (USCDI) Version 2*.

c. Gender may be included among data attributes for Person Matching only if required by the technical exchange standard in use. Otherwise, gender must not be included.

i. If gender is required by the technical exchange standard in use, the attribute must likewise follow the guidelines and standards established by the USCDI Version 2 unless the Data Elements to Be Exchanged Policy and Procedure or the technical standard requires otherwise.

ii. If gender is included among the attributes for Person Matching, the recipient of the gender attribute may choose to use the attribute in Person Matching.

# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

d. Format and content of home and mailing addresses must conform to the Project US@ Technical Workgroup's *Technical Specification for Patient Addresses: Domestic and Military* published by the Office of the National Coordinator for Health Information Technology.

e. Participants must also exchange specific identifiers related to health if Maintained by the Participant and only as permitted by Applicable Law when specifying a person to match or a matched Individual in a Request for Information or identifying an Individual in Information Delivery or Notifications of ADT Events if supported by the technical exchange standard in use, including but not limited to:

i. State or federal identifiers related to health (e.g., Medi-Cal or Medicare ID).

ii. Local identifiers related to health (e.g., medical record number or plan member identification number).

f. Participants may retain and use specific identifiers related to health and Exchange them as an aid in Person Matching.

## 5. Common procedures for Request for Information, Information Delivery, Notification of ADT Events, and Person Matching

a. A Participant may Access, Maintain, Use, and further Disclose Health and Social Services Information only as permitted by Applicable Law, valid Authorization if any, and the Privacy Standards and Security Safeguards Policy and Procedure, including but not limited to Section III.1.c of the Privacy Standards and Security Safeguards Policy and Procedure.

b. Nothing in this policy permits a Participant to Request Information or Request Notifications of ADT Events, or requires a Participant to send Health and Social Services Information, including Notifications of ADT Events, other than as permitted and required in the Permitted, Required and Prohibited Purposes Policy and Procedure.

### c. Secure Exchange of Health and Social Services Information

i. Participants that use a Nationwide Network or Framework to exchange Health and Social Services Information must conform to the security model and security standards for exchanging information established by the Nationwide Network or Framework.

ii. Participants that use an Intermediary to exchange Health and Social Services Information must conform to the security standards for exchanging information required by the Intermediary and in conformance with the Privacy Standards and Security Safeguards Policy and Procedure.

# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

iii. Participants that exchange Health and Social Services Information using point-to-point connections must mutually agree to security standards that conform to the Privacy Standards and Security Safeguards Policy and Procedure.

6. Technology Updates. The Governance Entity must create an open and transparent process to review and consider new and maturing National and Federally Adopted Standards for potential inclusion in the Data Exchange Framework.

a. The process must be put in place no later than July 1, 2024.

b. The process must consider both data content standards and data exchange standards to be adopted as amendments to the Data Elements to Be Exchanged Policy and Procedure and to this policy, respectively.

c. The process must establish a regular review cadence, no less than annually.

d. The process must align with requirements of the Development of and Modifications to Policies and Procedures Policy and Procedure.

### III. Definitions

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

“**Admit, Discharge, Transfer (ADT) Event**” means, at a minimum, admission to a Hospital or Emergency Department, discharge from a Hospital or Emergency Department, or transfer from a Hospital or Emergency Department to another healthcare facility in which the admission, discharge, or transfer reflects an actual change in patient status, including cancellations of an admission, discharge, or transfer. ADT Events may include intra-facility transfers if requested by the Participant and supported by the Hospital or Emergency Department.

“**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**” means and includes the requirements set forth at 45 CFR § 164.508 of the HIPAA Regulations and at Cal. Civ. Code §§ 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, when applicable, and shall include any additional requirements under Applicable Law to disclose PHI or PII.

“**Business Associate Agreement**” means a contract, agreement, or other arrangement that satisfies the requirements of 45 C.F.R. § 164.504(e), as applicable. With regard to



# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

Governmental Participants, a Business Associate Agreement may be a memorandum of understanding that satisfies the requirements of 45 C.F.R. § 164.504(e)(3).

“**Disclose**” or “**Disclosure**” means the release, transfer, provision of access to, or divulging in any manner of Health and Social Services Information outside the entity holding Health and Social Services 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 its Policies and Procedures.

“**Health and Social Services Information**” means any and all individually identifiable 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 PHI; and (c) information related to the provision of social services. Health and Social Services Information may include PHI, PII, and digital identities.

“**Hospital or Emergency Department**” means any emergency services or inpatient services setting, including but not limited to general acute care hospitals, acute psychiatric hospitals, and emergency departments, including standalone emergency departments and observation units.

“**Individual**” means the person that is the subject of Health and Social Services Information being Accessed, Used, Disclosed or Exchanged.

“**Information Delivery**” means the delivery of Health and Social Services Information regarding a specific Individual to a specific Participant in conjunction with an Order or Referral.

“**Intermediary**” means a health information exchange network, health information organization, or technology vendor that assists a Participant in the Exchange of Health and Social Services Information and adheres to the standards and policies established by the DSA and its Policies and Procedures as applicable to the services provided to the Participant. Examples might include nationwide networks or frameworks, vendors that provide applicable services, health information organizations including Qualified HIOs, or community information exchanges.

“**Maintain**” means that the entity has access to the data, control over the data, and the authority to make the data available, as defined for payers in the CMS Interoperability and Patient Access Final Rule but applied to entities beyond payers.

# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

“**National and Federally Adopted Standards**” means standards specifically included by the US Department of Health and Human Services in a published version of the Standards Version Advancement Process.

“**Nationwide Network or Framework**” means any vendor-agnostic health information network or health information exchange framework with nationwide scope, including coverage in California, available to some or all Participants for the exchange of Health and Social Services Information that may or may not have signed the DSA. Examples include, but are not limited to, eHealth Exchange, CommonWell Health Alliance, Carequality, DirectTrust, or Trusted Exchange Framework.

“**Notification of ADT Events**” means the message sent from a sending Participant to a receiving Participant with details of an ADT Event, including, at a minimum, the identity of the Individual who is the subject of the event, the Hospital or Emergency Department associated with the event, the event date and time, and the diagnosis or chief complaint associated with the event.

“**Order or Referral**” means any request, electronic or otherwise, placed by a health professional for diagnostic services, including but not limited to requests for diagnostic clinical laboratory and radiology services, or for assessment, evaluation, or consultation services from another health or social services professional.

“**Participant(s)**” means an organization that is a signatory to the Data Sharing Agreement, including any identified subordinate entities of that signatory.

“**Person Matching**” means the process by which a Participant ensures that exchanged electronic Health and Social Services Information is appropriately linked to the correct real person.

“**Request for Information**” means a request by a Participant for Health and Social Services Information regarding a specific Individual from one or more Participant(s) and the associated response(s) of Participant(s) to that request.

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

## IV. References

[Applicability Statement for Secure Health Transport, Version 1.2 \(a.k.a., Direct Secure Messaging\)](#) or later

[California Health and Human Services, Data Exchange Framework, Strategy for Digital Identities](#)

California Information Blocking Prohibitions Policy and Procedure

Data Elements to Be Exchanged Policy and Procedure

# CalHHS Data Exchange Framework Policy and Procedure

<b>Subject: Technical Requirements for Exchange</b>	
<b>Status: Final</b>	<b>Policy: OPP-9</b>
<b>Publication Date: June 26, 2023</b>	<b>Version: 1.0</b>

Development of and Modifications to Policies and Procedures Policy and Procedure

[HL7 Fast Health Information Resources \(FHIR\) Release 4 Version 4.0.1](#) or later

[IHE IT Infrastructure \(ITI\) Technical Framework, Volume 2](#)

Permitted, Required, and Prohibited Purposes Policy and Procedure

Privacy Standards and Security Safeguards Policy and Procedure

[Standards Version Advancement Process](#)

[Technical Specification for Patient Addresses: Domestic and Military](#)

[United States Core Data for Interoperability \(USCDI\) Version 2](#)

[US Core Implementation Guide Version 5.0.1 - STU5 Release US](#) or later

## V. Version History

No.	Date	Author	Comment
1.0	June 26, 2023	CalHHS CDII	Final