Data Exchange Framework
Data Sharing Agreement Policies & Procedures Subcommittee
Meeting #2

California Health & Human Services Agency

Tuesday, October 25, 2022
10:00 am – 12:30 pm

CalHHS
California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

Meeting Participation Options

Written Comments

- Participants and Subcommittee Members may submit comments and questions through the **Zoom Q&A box**; all comments will be recorded and reviewed by Subcommittee staff.
- Participants may also submit comments and questions – as well as requests to receive Data Exchange Framework updates – to CDII@chhs.ca.gov.

CalHHS California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

Meeting Participation Options

Spoken Comments

- Participants and Subcommittee Members must “raise their hand” for Zoom facilitators to unmute them to share comments; the Chair will notify participants/Members of appropriate time to volunteer feedback.

If you logged on via Zoom interface

Press “Raise Hand” in the “Reactions” button on the screen

If selected to share your comment, you will receive a request to “unmute;” please ensure you accept before speaking

If you logged on via phone-only

Press “*9” on your phone to “raise your hand”

Listen for your phone number to be called by moderator

If selected to share your comment, please ensure you are “unmuted’ on your phone by pressing “*6”

CalHHS California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

Public Comment Opportunities

- Public comment will be taken during the meeting at designated times.
- Public comment will be limited to the total amount of time allocated for public comment on particular issues.
- The Chair will call on individuals in the order in which their hands were raised.
- Individuals will be recognized for up to two minutes and are asked to state their name and organizational affiliation at the top of their statements.
- Participants are encouraged to use the Q&A box to ensure all feedback is captured or email their comments to CDII@chhs.ca.gov.

Agenda

10:00 AM	**Welcome and Roll Call** • *Courtney Hansen, Assistant Chief Counsel, CalHHS CDII*
10:05 AM	Informational Item**: Vision and Meeting Objectives** • *Courtney Hansen*
10:10 AM	Discussion Item: **Draft Language for First Set of Additional Policies & Procedures (P&Ps) in Development** • *Helen Pfister, Partner, Manatt Health*
11:10 AM	Discussion Item: **Content for Second Set of Additional P&Ps in Development** • *Rim Cothren, Independent HIE Consultant to CDII*
12:10 PM	**Public Comment**
12:25 PM	Informational Item: **Next Steps and Closing Remarks** • *Courtney Hansen*

CalHHS California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

Welcome and Roll Call

CalHHS
California Health & Human Services Agency

CENTER FOR
DATA INSIGHTS
AND INNOVATION
CALIFORNIA HEALTH &
HUMAN SERVICES AGENCY

DSA P&P Subcommittee Members (1 of 2)

Name	Title	Organization
Courtney Hansen (Chair)	**Assistant Chief Counsel**	**CDII**
Ashish Atreja	CIO and Chief Digital Health Officer	UC Davis Health
William (Bill) Barcellona	Executive Vice President for Government Affairs	America's Physician Groups (APG)
Michelle (Shelley) Brown	Attorney	Private Practice
Jason Buckner	Chief Information Officer & Chief Technology Officer	Manifest Medex
Louis Cretaro	Lead County Consultant	County Welfare Directors Association of California
Matthew Eisenberg	Medical Informatics Director for Analytics and Innovation	Stanford Health
Elaine Ekpo	Attorney	CA Dept. of State Hospitals
John Helvey	Executive Director	SacValley MedShare
Sanjay Jain	Manager, Data Analysis	Health Net
Bryan Johnson	Chief Information Security Officer	CA Dept. of Developmental Services
Diana Kaempfer-Tong	Attorney	CA Dept. of Public Health

DSA P&P Subcommittee Members (2 of 2)

Name	Title	Organization
Helen Kim	Senior Counsel	Kaiser Permanente
Steven Lane	Chief Medical Officer	Health Gorilla
Lisa Matsubara	General Counsel & VP of Policy	Planned Parenthood Affiliates of California
Deven McGraw	Lead, Data Stewardship and Data Sharing, Ciitizen Platform	Invitae
Leo Pak	Chief Technology Officer	Los Angeles Network for Enhanced Services
Eric Raffin	Chief Information Officer	San Francisco Department of Public Health
Mark Savage	Managing Director, Digital Health Strategy and Policy	Savage & Savage LLC
Tom Schwaninger	Senior Executive Advisor, Digital Ecosystem Interoperability	LA Care
Morgan Staines	Privacy Officer & Asst. Chief Counsel	CA Dept. of Health Care Services
Elizabeth Steffen	Chief Information Officer	Plumas District Hospital
Lee Tien	Legislative Director and Adams Chair for Internet Rights	Electronic Frontier Foundation
Belinda Waltman	Acting Director, Whole Person Care LA	Los Angeles County Department of Health Services
Terry Wilcox	Director of Health Information Technology/Privacy & Security Officer	Health Center Partners

Vision and Meeting Objectives

CalHHS
California Health & Human Services Agency

CENTER FOR
DATA INSIGHTS
AND INNOVATION
CALIFORNIA HEALTH &
HUMAN SERVICES AGENCY

Vision for Data Exchange in CA

Every Californian, and the health and human service providers and organizations that care for them, will have timely and secure access to usable electronic information that is needed to address their health and social needs and enable the effective and equitable delivery of services to improve their lives and wellbeing.

CalHHS
California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

Meeting #1 Objectives

1. Discuss **draft language for two additional P&Ps** that have been prioritized for development.

2. Discuss **concepts to inform development of other additional P&Ps** that have been prioritized for development.

CalHHS
California Health & Human Services Agency

CENTER FOR
DATA INSIGHTS
AND INNOVATION
CALIFORNIA HEALTH &
HUMAN SERVICES AGENCY

Draft Language for First Set of Additional Policies & Procedures (P&Ps) in Development

CalHHS
California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

P&P Development
Prioritized Topics

The P&Ps below have been prioritized for near-term development.

#	Prioritized Topics	Potential Contents
1	**Information Blocking**	Prohibits all Participants from undertaking any practice likely to interfere with access, exchange, or use of Health and Social Services Information (HSSI).
2	**Monitoring and Auditing**	Sets forth processes to ensure that all Participants that are required to execute the DSA do so, and that all Participants comply with their obligations under the DSA.
3	**Required Transaction Patterns and Technical Requirements for Exchange**	Sets forth data exchange patterns for the DxF and those that Participants must support, at a minimum, as well as the technical specifications Participants must adhere to for each of the Required Transaction Patterns.
4	**Real-Time Data Exchange**	Sets forth definition of 'Real Time Data Exchange' and associated obligations of Participants.
5	**Qualified HIO Designation Process**	Sets forth the process for designating an organization as a 'Qualified Health Information Organization'.

Formerly proposed as two distinct P&Ps

P&P Draft Language
Purpose of the Discussion

The goal for this section of the meeting is to obtain input on draft language for two P&Ps in development.

The topics of these P&Ps are:

- **Information Blocking**
- **Monitoring and Auditing**

Information Blocking (1)

Purpose of Proposed P&P

To support the Data Exchange Framework's commitment to facilitating the timely access, exchange, and use of Health and Social Services Information in compliance with applicable law.

This policy prohibits Participants from undertaking any practice that is likely to interfere with access, exchange, or use of Health and Social Services Information for the Required Purposes set forth in the Permitted, Required and Prohibited Purposes Policy and Procedure.

This policy shall have no impact on a Participant's obligation, if any, to comply with the Federal Information Blocking Regulations.

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

Information Blocking (2)

Overview

No Participant shall engage in Information Blocking. Practices - acts or omissions - that may constitute Information Blocking include, but are not limited to, the following:

(a) Practices that unreasonably restrict authorized access, exchange, or use of Health and Social Services Information under the DSA or Applicable Law;

(b) Implementing health information technology in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using Health and Social Services Information; and

(c) Implementing health information technology in ways that are likely to—(i) restrict the access, exchange, or use of Health and Social Services Information with respect to exporting complete information sets or in transitioning between health information technology systems; or (ii) lead to fraud, waste, or abuse, or impede innovations and advancements in Health and Social Services Information access, exchange, and use, including care delivery enabled by health information technology.

Information Blocking (3)

Exceptions to Information Blocking Prohibition

Notwithstanding the foregoing, a practice shall not be treated as Information Blocking if the Participant satisfies one of the following exceptions:

(1) Preventing Harm Exception

(2) Privacy Exception

- (a) Legally required precondition not satisfied
- (b) Respecting an individual's request not to share information
- (c) Denial of an individual's request for information

(3) Security Exception

(4) Infeasibility Exception

(5) Health IT Performance Exception

Information Blocking (4)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Preventing Harm

A Participant's practice that is likely to, or in fact does, interfere with the access, exchange, or use of Health and Social Services Information in order to prevent harm will not be considered Information Blocking when the practice meets the conditions in paragraphs (a) and (b) directly below, satisfies the conditions set forth in either paragraphs (c) or (d) directly below, and also meets the condition in paragraph (e) (if applicable) and (f) directly below.

(a) ***Reasonable belief***. The Participant engaging in the practice must hold a reasonable belief that the practice will substantially reduce a risk of harm to the individual who is the subject of the Health and Social Services Information affected by the practice or to another natural person, that would otherwise arise from the access, exchange, or use of Health and Social Services Information affected by the practice.

(b) ***Practice breadth***. The practice must be no broader than necessary to substantially reduce the risk of harm that the practice is implemented to reduce.

Information Blocking (5)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Preventing Harm

(c) ***Type of risk and type of harm (professional judgment)***. The risk of harm must be determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior relationship with the individual whose Health and Social Services Information is affected by the determination; and the type of harm must be one of the following:

(1) The request for access is made by the individual's legal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such legal representative is reasonably likely to cause substantial harm to the individual or another person.

(2) The Health and Social Services Information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.

(3) The licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.

(d) ***Type of risk and type of harm (misidentification or mismatch)***. The risk of harm must arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual whose Health and Social Services Information is affected by the determination or another person.

Information Blocking (6)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Preventing Harm

(e) ***Individual right to request review of individualized determination of risk of harm***. If access is denied on a ground permitted in accordance with paragraph (c) above, the individual has the right to have the denial (i) reviewed by a licensed health care professional who is designated by the Participant to act as a reviewing official and who did not participate in the original decision to deny; or (ii) reviewed and reversed in accordance with any other applicable Federal, State, or tribal law. The Participant must provide or deny access in accordance with the determination of the reviewing official.

Information Blocking (7)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Preventing Harm

(f) ***Practice implemented based on an organizational policy or a determination specific to the facts and circumstances.*** The practice must be consistent with an organizational policy that meets paragraph (f)(1) below or, in the absence of an organizational policy applicable to the practice or to its use in particular circumstances, the practice must be based on a determination that meets paragraph (f)(2) below.

(1) An organizational policy must:

(i) Be in writing;

(ii) Be based on relevant clinical, technical, and other appropriate expertise;

(iii) Be implemented in a consistent and non-discriminatory manner; and

(iv) Conform each practice to the conditions in paragraphs (a) and (b) above, as well as the conditions in paragraphs (c) through (f) above that are applicable to the practice and its use.

(2) A determination must:

(i) Be based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use; and

(ii) Be based on expertise relevant to implementing the practice consistent with the conditions in paragraphs (a) and (b) above, as well as the conditions in paragraphs (c) through (e) above that are applicable to the Practice and its use in particular circumstances.

Information Blocking (8)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Privacy

A Participant's practice of not fulfilling a request to access, exchange, or use Health and Social Services Information in order to protect an Individual's privacy will not be considered Information Blocking when the practice meets all of the requirements of at least one of the sub-exceptions in paragraphs (a) through (c) directly below.

(a) ***Sub-exception - State or Federal preconditions not satisfied***. To qualify for the exception on the basis that state or federal law requires one or more preconditions for providing access, exchange, or use of Health and Social Services Information that have not been satisfied, the following requirements must be met:

(1) The Participant's practice is tailored to the applicable precondition not satisfied, is implemented in a consistent and non-discriminatory manner, and either:

(i) Conforms to the Participant's organizational policies and procedures that: (A) are in writing; (B) specify the criteria to be used by the Participant to determine when the precondition would be satisfied and, as applicable, the steps that the Participant will take to satisfy the precondition; and (C) are implemented by the Participant, including by providing training on the policies and procedures; or

(ii) Are documented by the Participant, on a case-by-case basis, identifying the criteria used by the Participant to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met.

Information Blocking (9)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Privacy

(2) If the precondition relies on the provision of a consent or Authorization from the individual subject of the Health and Social Services Information and the Participant has received a version of such a consent or Authorization that does not satisfy all elements of the precondition required under applicable law, the Participant must:

(i) Use reasonable efforts within its control to provide the individual with a consent or Authorization form that satisfies all required elements of the precondition or provide other reasonable assistance to the individual to satisfy all required elements of the precondition; and

(ii) Not improperly encourage or induce the individual to withhold the consent or Authorization.

(3) For purposes of determining whether the Participant's privacy policies and procedures and actions satisfy the requirements of paragraphs (a)(1)(i) and (a)(2) directly above when the Participant's operations are subject to multiple laws which have inconsistent preconditions, the Participant shall be deemed to satisfy the requirements of the paragraphs if the Participant has adopted uniform privacy policies and procedures to address the more restrictive preconditions.

Information Blocking (10)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Privacy

(b) ***Sub-exception - respecting an individual's request not to share information***. Unless otherwise required by law, a Participant may elect not to provide access, exchange, or use of an individual's Health and Social Services Information if the following requirements are met:

(1) The individual requests that the Participant not provide such access, exchange, or use of Health and Social Services Information without any improper encouragement or inducement of the request by the Participant;

(2) The Participant documents the request within a reasonable time period;

(3) The Participant's practice is implemented in a consistent and non-discriminatory manner; and

(4) The Participant may terminate an individual's request for a restriction to not provide such access, exchange, or use of the individual's Health and Social Services Information only if:

(i) The individual agrees to the termination in writing or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented by the Participant; or

(iii) The Participant informs the individual that it is terminating its agreement to not provide such access, exchange, or use of the individual's Health and Social Services Information except that such termination is:

(A) Not effective to the extent prohibited by applicable federal or state law; and

(B) Only applicable to Health and Social Services Information created or received after the Participant has so informed the individual of the termination.

Information Blocking (11)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Privacy

(c) ***Sub-exception - denial of an individual's request for their PHI or PII.*** A Participant may elect not to provide an individual the right of access to inspect and obtain a copy of PHI or PII about the individual under the circumstances set forth directly below or in the *Preventing Harm* exception set forth above.

(1) A Participant may deny the individual access in the following circumstances.

(i) The PHI or PII constitutes (A) psychotherapy notes; or (B) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

(ii) The PHI or PII is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, or any equivalent state law, and the denial of access under any such law would meet the requirements of that law.

(iii) The PHI or PII was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

Information Blocking (12)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Security

A Participant's practice that is likely to interfere with the access, exchange, or use of Health and Social Services Information in order to protect the security of Health and Social Services Information will not be considered Information Blocking when the practice meets the conditions in paragraphs (a) through (c) of this section, and in addition meets either the condition in paragraph (d) of this section or the condition in paragraph (e) of this section.

(a) The practice must be directly related to safeguarding the confidentiality, integrity, and availability of Health and Social Services Information.

(b) The practice must be tailored to the specific security risk being addressed.

(c) The practice must be implemented in a consistent and non-discriminatory manner.

(d) If the practice implements an organizational security policy, the policy must -

(1) Be in writing;

(2) Have been prepared on the basis of, and be directly responsive to, security risks identified and assessed by or on behalf of the Participant;

(3) Align with one or more applicable consensus-based standards or best practice guidance; and

(4) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

(e) If the practice does not implement an organizational security policy, the Participant must have made a determination in each case, based on the particularized facts and circumstances, that:

(1) The practice is necessary to mitigate the security risk to Health and Social Services Information; and

(2) There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with access, exchange or use of Health and Social Services Information.

Information Blocking (13)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Infeasibility

A Participant's practice of not fulfilling a request to access, exchange, or use Health and Social Services Information due to the infeasibility of the request will not be considered Information Blocking when the practice meets one of the conditions in paragraph (a) below and meets the requirements in paragraph (b) below.

(a) ***Conditions***

(1) Uncontrollable events. The Participant cannot fulfill the request for access, exchange, or use of Health and Social Services Information due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.

(2) Segmentation. The Participant cannot fulfill the request for access, exchange, or use of Health and Social Services Information because the Participant cannot unambiguously segment the requested Health and Social Services Information from Health and Social Services Information that:

(i) Cannot be made available due to an individual's preference or because the Health and Social Services Information cannot be made available by law; or;

(ii) May be withheld in accordance with this policy or in accordance with federal or state law.

Information Blocking (14)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Infeasibility

(3) Infeasible under the circumstances.

(i) The Participant demonstrates, prior to responding to the request pursuant to paragraph (b) of this section, through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of the following factors that led to its determination that complying with the request would be infeasible under the circumstances:

(A) The type of Health and Social Services Information and the purposes for which it may be needed;

(B) The cost to the Participant of complying with the request in the manner requested;

(C) The financial and technical resources available to the Participant;

(D) Whether the Participant's practice is non-discriminatory and the Participant provides the same access, exchange, or use of Health and Social Services Information to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

(E) Whether the Participant owns or has control over a predominant technology, platform, health information exchange, or health information network through which Health and Social Services Information is accessed or exchanged; and

(F) Why the Participant was unable to provide access, exchange, or use of Health and Social Services Information consistent with this Policy and Procedure, including consideration of whether the Participant would be able to fulfill the request in an alternative manner than the one requested.

Information Blocking (15)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Infeasibility

(ii) In determining whether the circumstances were infeasible under paragraph (a)(3)(i) above, it shall not be considered whether the manner requested would have:

(A) Facilitated competition with the Participant.

(B) Prevented the Participant from charging a fee or resulted in a reduced fee.

(b) ***Responding to requests.*** If a Participant does not fulfill a request for access, exchange, or use of Health and Social Services Information for any of the reasons provided in paragraph (a) above, the Participant must, within ten (10) business days of receipt of the request, provide to the requestor in writing the reason(s) why the request is infeasible.

Information Blocking (16)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Health and Social Services IT Performance

A Participant's practice that is implemented to maintain or improve health and/or social services IT (referred to collectively herein as "health IT") performance and that is likely to interfere with the access, exchange, or use of Health and Social Services Information will not be considered Information Blocking when the practice meets a condition in paragraph (a), (b), or (c) below, as applicable to the particular practice and the reason for its implementation.

(a) Maintenance and improvements to health IT. When the Participant implements a practice that makes health IT under the Participant's control temporarily unavailable, or temporarily degrades the performance of health IT, in order to perform maintenance or improvements to the health IT, the Participant's practice must be –

(1) Implemented for a period of time no longer than necessary to complete the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;

(2) Implemented in a consistent and non-discriminatory manner; and

(3) If the unavailability or degradation is initiated by a health IT developer of certified health IT, health information exchange, or health information network:

(i) Planned. Consistent with existing service level agreements between the individual or entity to whom the health IT developer of certified health IT, health information exchange, or health information network supplied the health IT; or

(ii) Unplanned. Consistent with existing service level agreements between the individual or entity; or agreed to by the individual or entity to whom the health IT developer of certified health IT, health information exchange, or health information network supplied the health IT.

Information Blocking (17)

Preventing Harm		Protect Privacy		Security Risk		Infeasibility		Health IT

Exceptions – Health IT Performance

(b) Practices that prevent harm. If the unavailability of health IT for maintenance or improvements is initiated by a Participant in response to a risk of harm to an Individual or another person, the Participant does not need to satisfy the requirements of this Health IT Performance exception, but must comply with all requirements of the Preventing Harm exception set forth above at all relevant times to qualify for an exception.

(c) Security-related practices. If the unavailability of health IT for maintenance or improvements is initiated by a Participant in response to a security risk to Health and Social Services Information, the Participant does not need to satisfy the requirements of this Health IT Performance exception, but must comply with all requirements of the Security exception as set forth above at all relevant times to qualify for an exception.

Monitoring and Auditing (1)

Purpose of Proposed P&P

To set forth the monitoring and auditing processes the Governance Entity will utilize in order to verify Participants' compliance with their obligations as set forth in the California Health and Safety Code and the Data Sharing Agreement ("DSA").

Obligations of the Governance Entity

(a) The Governance Entity shall engage in any monitoring activities it deems necessary in order to verify that entities set forth in California Health and Safety Code section 130290 have executed the DSA.

(b) The Governance Entity shall engage in any monitoring and auditing activities that it deems necessary in order to verify that Participants are in compliance with their obligations under the DSA.

Monitoring and Auditing (2)

Obligations of the Governance Entity

(c) The Governance Entity's responsibilities for monitoring Participants' compliance with the DSA shall include, but not necessarily be limited to, the following:

1. Verifying that Participants are exchanging Health and Social Services Information as set forth in the Permitted, Required, and Prohibited Purposes Policy and Procedure and the Requirement to Exchange Policy and Procedure.
2. Verifying that Participants are using appropriate safeguards to protect the privacy of PHI or PII as set forth in the Privacy Standards and Security Safeguards Policy and Procedure.
3. Verifying that Participants provide Individual Users bidirectional access to their PHI or PII in accordance with the Individual Access Services Policy and Procedure.
4. Verifying that Participants are not engaging in Information Blocking as set forth in the Information Blocking Policy and Procedure.

(d) The Governance Entity shall establish a complaint process that enables any individual or entity to file a complaint with the Governance Entity if a Participant is not in compliance with its obligations under the DSA. The Governance Entity shall publicly make available information detailing how individuals or entities may submit complaints and the Governance Entity's process for investigating such complaints.

Monitoring and Auditing (3)

Obligations of the Participants

(a) All Participants shall, with advance written notice and during regular business hours, make their internal practices, books, and records relating to compliance with the DSA available to the Governance Entity for purposes of determining the Participant's compliance with the DSA.

(b) If a Participant engages in the exchange of Health and Social Services Information through execution of an agreement with a Qualified HIO, the Participant shall attest, on an annual basis and in a manner set forth by the Governance Entity, that the Participant has entered into such an agreement and that the Participant is exchanging Health and Social Services Information in accordance with all applicable requirements set forth in the DSA.

(c) If a Participant engages in the exchange of Health and Social Services Information through execution of an agreement with an entity other than a Qualified HIO, the Participant shall attest, on an annual basis and in a manner set forth by the Governance Entity, that it is exchanging Health and Social Services Information in accordance with all applicable requirements set forth in the DSA.

Monitoring and Auditing (4)

Obligations of the Participants

(d) If a Participant engages in the exchange of Health and Social Services Information through use of the Participant's own technology, the Participant shall attest, on an annual basis and in a manner set forth by the Governance Entity, that it is exchanging Health and Social Services Information in accordance with all applicable requirements set forth in the DSA. Additionally, the Participant shall, upon request by the Governance Entity, provide written demonstration of its compliance with the DSA.

Confidential Information

(a) As set forth in the DSA, to the extent that a Participant provides access to or discloses Confidential Participant Information to the Governance Entity in connection with the Governance Entity's monitoring and auditing activities, the Governance Entity shall hold such information in confidence and shall not redisclose such information to any person or entity except as required by Applicable Law.

Public Comment Process

CalHHS invites stakeholder input on draft P&Ps in upcoming periods of public comment.

Public Comment Process

CalHHS will release P&Ps for public comment as they are developed. The first set of P&Ps will be released for comment in **mid-November** following discussion at the November 3rd IAC meeting. The first two P&Ps that will be released address the following topics:

- Information Blocking
- Monitoring and Auditing

Members of the public will be encouraged to use a provided template when providing comments to ensure accurate and efficient collection and review of comments. More information will be communicated to stakeholders and made available on the CalHHS DxF website.

CalHHS
California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

Content for Second Set of Additional P&Ps in Development

CalHHS
California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

P&P Draft Concepts
Purpose of the Discussion

The goal for this section of the meeting is to obtain input on draft concepts for two P&Ps in development.

The topics of these P&Ps are:

- **Required Transaction Patterns and Technical Requirements for Exchange**
- **Real-Time Data Exchange**

Technical Requirements for Exchange (1)

Purpose of Proposed P&P

To identify and advance common Specifications that are to be leveraged by Participants to provide access to and exchange of electronic Health and Social Services Information

- The *Data Elements to Be Exchanged* P&P identifies the Specifications for minimum data content for Health and Social Services Information.
- This P&P identifies the common technical Specifications for exchange of Health and Social Services Information.

Definitions (From DSA)

1. **Health and Social Services Information** shall mean any and all information received, stored, processed, generated, used, transferred, disclosed, made accessible, or shared… including but not limited to… information related to the provision of health care services… and information related to the provision of social services. Health and Social Services Information may include PHI, PII, de-identified data, anonymized data, pseudonymized data, metadata, digital identities, and schema.
2. **Specifications** shall mean the specifications… to establish (i) minimum data content required for particular data exchange use cases and (ii) technical and security requirements to enable the Participants to exchange Health and Social Services Information. Specifications may include, but are not limited to, specific network standards, services, and policies.

Definitions (From Relevant P&Ps)

3. **National and Federally Adopted Standards** shall mean standards published by the US Department of Health and Human Services in the Standards Version Advancement Process.

Technical Requirements for Exchange (2)

Approach

Establish a set of principles in identifying Transaction Patterns and exchange Specifications:

1. Advance Transaction Patterns in alignment with federal regulation and national initiatives
2. Specify National and Federally-Adopted Standards for use by Participants to accomplish exchange Transaction Patterns
3. Leverage standards and capabilities of national initiatives, qualified HIOs, and nationwide networks
4. Share information that informs Participants
    - Results in response to an order or request for services
    - Notification of a health event for a patient, member, or client
5. Avoid sending information that has not been requested
    - Care summaries for every transition
    - Details beyond the notification of an event
6. Request information from Participants likely to have the information sought
    - Information on a new patient/member/client from the referring physician, plan, attributed physician
    - Information flowing from receipt of an event notification from the Participant producing the notification
7. Use broadcasts sparingly
    - Reserve broadcasts for urgent or emergency situations
    - Avoid broadcasts for common events or unrestricted geographies

Questions

Are these the right principles to drive P&P development?

CalHHS California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

Technical Requirements for Exchange (3)

Overview

Identified Transaction Patterns include:

1. Targeted Information Delivery – delivering results in response to an order or request for health care or social services
   Required by TEFCA, supported (but not widely implemented) by nationwide networks and HIOs
2. Requested Notification – notifying Participants of events for patients/members/clients requested by them
   Required of hospitals by CMS Interoperability and Patient Access final rule, supported by many HIOs, not supported by nationwide networks
3. Targeted Requests for Information – requesting information from a Participant likely to have the information sought
   Required by TEFCA, supported and widely implemented by nationwide networks and HIOs
4. Broadcast Requests for Information – requesting information from a group when Participants likely to have it are unknown
   Required by TEFCA, supported and widely implemented by nationwide networks and HIOs

Notes

"Transaction Patterns" are the interactions between Participants undertaken to provide exchange of Health and Social Services Information to meet a defined business need or use case.

"Nationwide networks" may include eHealth Exchange, Carequality, and the CommonWell Alliance. For individual-to-individual exchange, DirectTrust might also be included as a nationwide network. TEFCA would be included once QHINs are identified and exchange begins.

Technical Requirements for Exchange (4)

Overview

1. Targeted Information Delivery – delivering results in response to an order or request for services
   Required by TEFCA, supported (but not widely implemented) by nationwide networks and HIOs
   - Any Participant may choose to send electronic Information to another Participant via this Transaction Pattern.
   - Participants using nationwide networks or point-to-point connections, including QHIOs, must use IHE XDR reliable document delivery profiles to send Information.
   - Participants that create Information as result of an order or requested service delivery are strongly encouraged to send Information via this Transaction Pattern.
   - The sending Participant must ensure that the recipient is authorized to receive the information sent.
   - All Participants are encouraged to support receipt of Information via a QHIO or nationwide network.

Notes

"Information" in the above and subsequent slides applies to all Health and/or Social Services Information as defined in the DSA.

QHIOs must meet additional requirements listed in the applicable P&Ps.

Questions

Should Participants that create Information as a result of orders or requested service delivery (e.g., radiology reports, consults) be required to support this Transaction Pattern and the IHE XDR document delivery standard?

Should FHIR be specified as an optional Specification to be used as an alternative to IHE profiles? It is not well supported by HIOs or nationwide networks.

Technical Requirements for Exchange (5)

Overview

2. Requested Notification – notifying Participants of events for patients/members/clients requested by them
   Required of hospitals by CMS, supported by many HIOs, not supported by nationwide networks

- Acute care hospital Participants must respond to requests for notifications of admission, transfer, and discharge events.
- QHIOs receiving notifications must exchange received notifications with all other QHIOs. QHIOs may only retain notifications if authorized to do so.
- Acute care hospitals and QHIOs must use HL7 v2.x ADT messages to send/exchange notifications.
- Any Participant may request notifications by submitting a roster of patients/members/clients for whom to receive notifications. A Participant requesting notifications must be authorized to receive them.
- Acute care hospitals and QHIOs must accept requests for notifications from any authorized Participant.
- QHIOs may offer any method to deliver notifications to requesting Participants. Notifications must include the identity of the Participant submitting the notification and the digital identity of the person to facilitate subsequent request of Information.

Notes

QHIOs must be authorized to retain notifications they receive, e.g., because a participant has a relationship with the individual or because a QHIO has a request to deliver notifications for the individual and the individual is identified on a roster.

Questions

Should the role of QHIOs be expanded in this Transaction Pattern?

Should the P&P list specific delivery standards or content requirements for QHIOs to use in delivering notifications to Participants?

Technical Requirements for Exchange (6)

Overview

3. Targeted Requests for Information – requesting information from a Participant likely to have the information sought
   Required by TEFCA, supported and widely implemented by nationwide networks and HIOs
4. Broadcast Requests for Information – requesting information from a group when Participants likely to have it are unknown
   Required by TEFCA, supported and widely implemented by nationwide networks and HIOs

- Any Participant may make a request for Information via these related Transaction Patterns.
- Participants using nationwide networks or point-to-point connections, including QHIOs, must use IHE XCPD and XCA query-based document exchange delivery profiles to exchange Information.
- Every Participant must respond to a valid authorized request for Information via a QHIO or nationwide network.
- QHIOs must be able to request Information and respond to requests from all other QHIOs and a nationwide network.
- A Participant that makes a request for Information must be authorized to receive the Information requested.
- Participants are encouraged to use a Notification as a trigger for a targeted request via this Transaction Pattern.
- Participants are strongly discouraged from broadcast requests except for emergency use cases.

Questions

Should FHIR be specified as an optional Specification to be used as an alternative to IHE profiles? It is not well supported by HIOs or nationwide networks.

Should broadcast requests be regulated more strongly than “strongly discouraged”?

Real-Time Data Exchange (1)

Purpose of Proposed P&P

AB 133 states that the CalHHS DxF 'will be designed to enable and require real-time access to, or exchange of, health information among health care providers and payers…'. The purpose of this P&P is to define 'real-time' and associated obligations for signatories.

Background

In general, few existing data sharing agreements and frameworks define concepts of timeliness or provide significant guidance on timeliness requirements.

- Some agreements require timely exchange (specifically for targeted requests for health information) but do not further define what is meant by "timely"
  - ***Example:*** *"When acting as a Submitter, each Participant...hereby represents that at the time of transmission, the Message Content it provides is... provided in a timely manner and in accordance with the Performance and Service Specifications and Operating Policies and Procedures."* (eHealth Exchange DURSA)
- The Interoperability and Patient Access Final Rule states that hospitals must send event notifications to providers **at the time of** an individual's admission (to ED or inpatient facilities) and **immediately prior to, or at the time of,** discharge/transfer
  - *CMS interprets "immediately" to be at the time of discharge or transfer and without any intentional delays.* (CMS FAQs)

CalHHS California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

Real-Time Data Exchange (2)

Background

The Interoperability and Patient Access Final Rule also requires that plans make certain types of data available in a patient access API within one business day of receipt

- *Plans must make available in a Patient Access API, at a minimum: adjudicated claims; encounters with capitated providers; provider remittances; enrollee cost-sharing; and clinical data, including laboratory results (where maintained by the impacted payer).*
- *Data must be made available no later than one (1) business day after a claim is adjudicated or encounter data are received.*

- Networks specify specific reporting timelines for urgent communications (i.e., reporting an adverse security event).
  - ***Example:*** *CTEN requires participants to report breaches "as soon as reasonably practicable", but no later than 24 hours after determining that a breach has occurred.*

Real-Time Data Exchange (3)

Discussion Questions:

- **What factors should be considered to inform an operationalizable definition of "real-time"?**
- **Should the definition of real-time vary by transaction pattern?**
  - Targeted health information delivery
  - Requested notifications
  - Targeted or broadcast requests for health information
- **How quickly would data need to be available/exchanged to meaningfully inform delivery of care services?**

Update to the DSA

CalHHS is making a necessary change to the Data Exchange Framework's DSA.

What's Being Changed

The DSA is an agreement between the entities that will be required to exchange data in accordance with the Agreement and its P&Ps. As such, the DSA will be revised to remove CalHHS as a signatory. See the change below (noted in red):

1. PARTIES

(a) This Single Data Sharing Agreement is made between the ~~California Health and Human Services Agency and~~ Participants (defined below) who are required to or elect to exchange Health and Social Services Information (defined below) within the State of California in accordance with this Agreement (defined below).

What is Not Changing

CalHHS Departments will still be expected to sign the DSA and exchange data with other public and private participants in accordance with the Agreement. This change does not change or diminish CalHHS's role and responsibility to oversee the DxF and ensure successful implementation.

An updated DSA will be posted to the CalHHS DxF website after the November 3rd meeting of the Implementation Advisory Committee (IAC).

CalHHS California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

Signing the DSA

CDII anticipates both mandatory and voluntary signatories may begin executing the DSA in November. All mandatory signatories are required by AB-133 to execute the DSA by 1/31/2023.

- CDII is creating a web-based self-service application to sign the DSA electronically. Organizations wishing to execute the DSA will need to determine:
  - Who is authorized to sign the DSA within your organization.
  - What facilities or subordinate entities are included in the DSA; a signatory may sign on behalf of multiple facilities/entities if authorized.
  - Information about the individual signing, their organization, their contact information, and all subordinate entities will need to be listed on the DSA prior to signing.
- The link to the application will be posted on the CalHHS DxF website.
- Mandatory signatories should be reviewing the DSA now to plan for executing it by 1/31/2023 and complying with its provisions and associated P&Ps.
  - Organizations may not negotiate changes to the DSA prior to execution.
  - Organizations should continue to monitor development of P&Ps through the coming months.

CalHHS California Health & Human Services Agency

CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

Public Comment Period

CalHHS
California Health & Human Services Agency

CENTER FOR
DATA INSIGHTS
AND INNOVATION
CALIFORNIA HEALTH &
HUMAN SERVICES AGENCY

Next Steps and Closing Remarks

CalHHS
California Health & Human Services Agency

CENTER FOR
DATA INSIGHTS
AND INNOVATION
CALIFORNIA HEALTH &
HUMAN SERVICES AGENCY

Next Steps

CalHHS will:

- Post a summary of today's meeting.
- Consider feedback from Subcommittee Members on the development of the DSA P&Ps.
- Draft language for P&Ps that are prioritized for development.

Members will:

- Provide additional feedback on today's topics to CDII.
- Participate in the upcoming period of public comment.

Meeting Schedule

DSA P&P Subcommittee Meetings	Date
DSA P&P SC Meeting #2	October 25, 2022, 10:00 AM to 12:30 PM
DSA P&P SC Meeting #3	December 15, 2022, 9:00 AM to 11:30 AM
DSA P&P SC Meeting #4	January 26, 2023, 9:00 AM to 11:30 AM
DSA P&P SC Meeting #5	March 9, 2023, 9:00 AM to 11:30 AM

For more information or questions on Subcommittee meeting logistics, please email CDII (CDII@chhs.ca.gov).