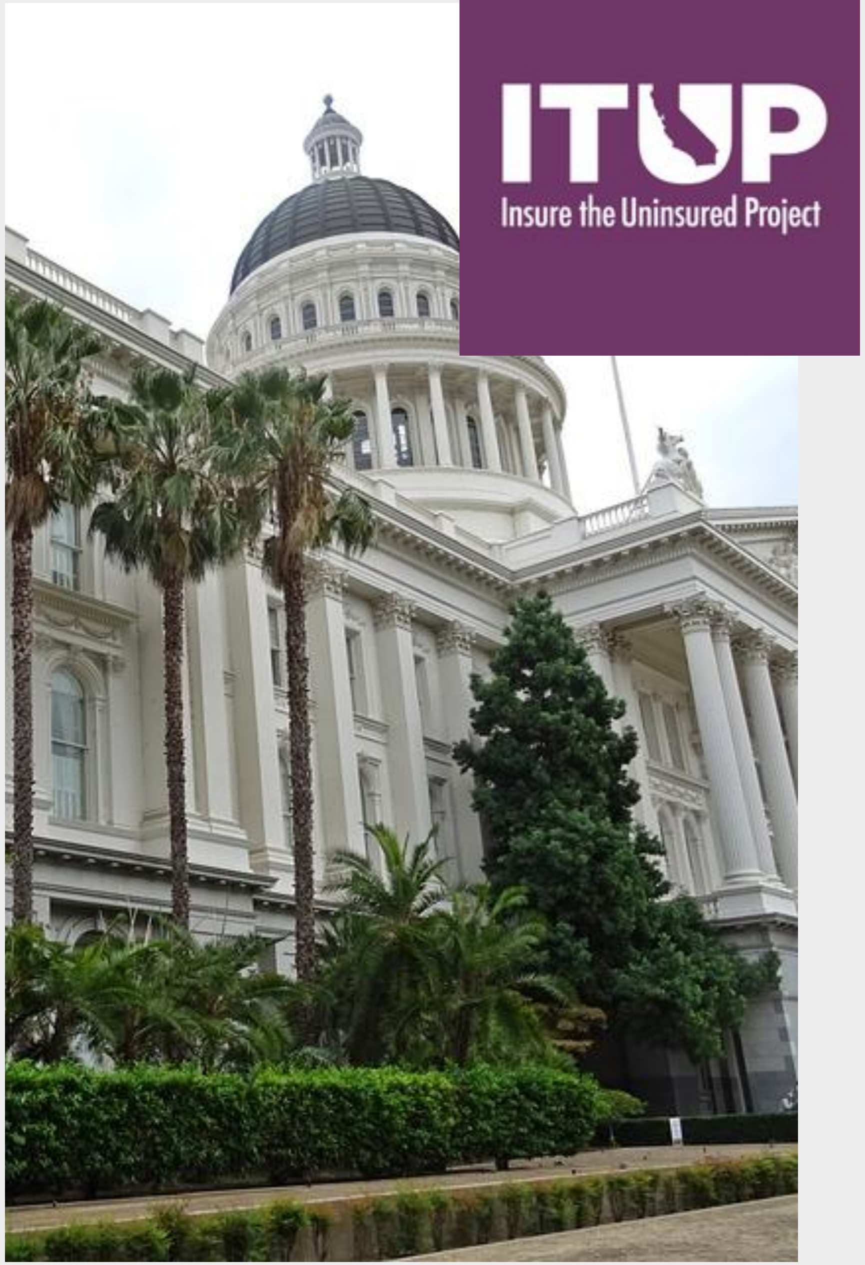
Data Exchange Framework Bootcamp

Driving Health Equity with Data Exchange



ITUP
Insure the Uninsured Project

ITUP Mission & Vision

ITUP
Insure the Uninsured Project

Mission

The mission of ITUP is to promote innovative strategies and identify workable community-informed policy solutions that expand health care access and improve the health of all Californians.

Vision

ITUP believes that all Californians should have a fair opportunity to live their healthiest lives. In pursuit of this vision, ITUP provides California policymakers, health and social care stakeholders, and advocates for equitable access to health care with timely and rigorous research and analysis, accessible explainers, and forums for discussing and developing policy options to preserve and expand health care coverage, meaningful access, and continue progress on broader state-based health reforms that will make health care more accessible, affordable, and equitable for all Californians.

ITUP Values

ITUP
Insure the Uninsured Project

ITUP Seeks a Health Care System that is:

Universal – All Californians are eligible for comprehensive health coverage and services, including primary, specialty, behavioral, oral, and vision health services, as well as services that address the social determinants of health.

Equitable – All Californians receive health care coverage, treatment, and services that address the social determinants of health regardless of health status, age, ability, income, language, race, ethnicity, gender identity, sexual orientation, immigration status, and geographic region.

Accessible – All Californians have access to coverage options and services that are available, timely, and appropriate.

Effective – Health, health care, and related services that address the social determinants of health are person-centered, value-based, coordinated, and high-quality.

Affordable – Coverage and services are affordable for consumers at the point of purchase and care; and, at the health system level for public and private purchasers

ITUP Insure the Uninsured Project

The work continues…

Understanding the impact of COVID-19

+/- Policy changes

+/- Budgets

COVERAGE

Explore Policy Solutions for the Remaining Uninsured & Underinsured

Access to Health Care Including Behavioral Health and Specialty Care

ACCESS

MODERNIZATION

Set a Vision for the Future of Health

DxF Bootcamp: Driving Health Equity with Data Sharing

Nov 2, 2023

CALIFORNIA ACADEMY OF FAMILY PHYSICIANS
STRONG MEDICINE FOR CALIFORNIA

AMERICA'S PHYSICIAN GROUPS

CALIFORNIA ASSOCIATION
CAHF
OF HEALTH FACILITIES

CAHIE
California Association of Health Information Exchanges

CALIFORNIA ASSOCIATION OF AREA AGENCIES ON AGING

ITUP
Insure the Uninsured Project

PBGH California Quality Collaborative

Consulting Supports:

BluePath HEALTH

Connecting for Better Health
Advancing data sharing to improve the health of all Californians

th transform health

Agenda

DATA EXCHANGE FRAMEWORK • CALIFORNIA HEALTH & HUMAN SERVICES •

- Welcome and Introductions
- DxF Overview - *DSA Readiness Activity*
- Impact of the DxF on Internal Operations - *DSA Compliance Activity*
- **Break – 10 Minutes**
- DxF Technical Exchange Requirements
- Technology and Data Exchange Mechanisms - *DSA Technical Exchange Activity*
- Discussion and Reflections
- Wrap Up and Conclusion

Overview and Purpose of Today's Session

DATA EXCHANGE FRAMEWORK • CALIFORNIA HEALTH & HUMAN SERVICES •

Purpose and Objectives

1. Assess DxF Readiness
2. Understand the DxF's Impact on Internal Operations and Technical Exchange Requirements
3. Examine Technology and Mechanisms to Exchange Data under the DxF
4. Identify Next Steps to Continue DxF Implementation

The Vision for Data Exchange in California

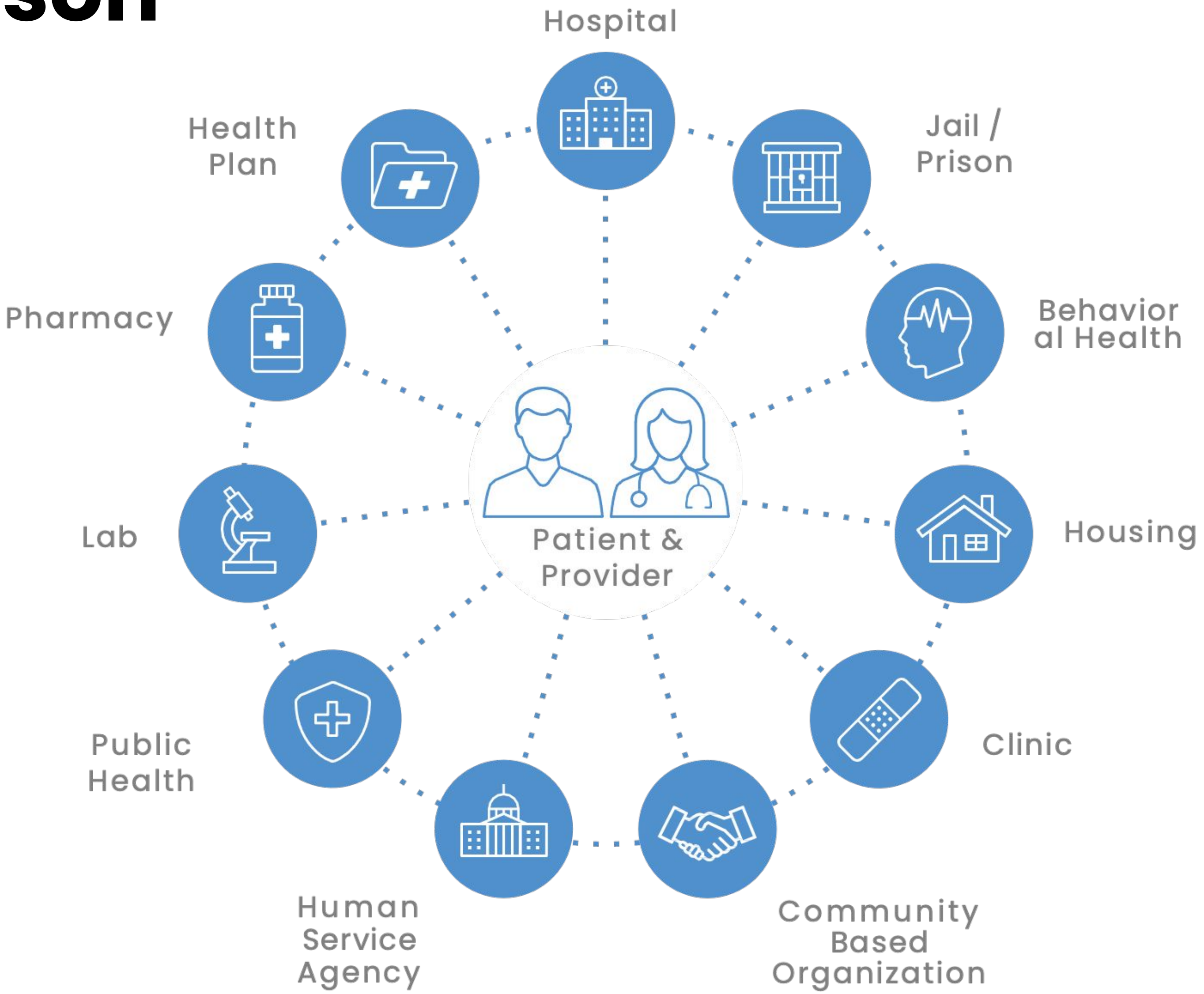
Once implemented across California, the Data Exchange Framework (DxF) will create new connections and efficiencies between health and social services providers, improving whole-person care.

The DxF is California's first-ever statewide Data Sharing Agreement (DSA) that requires the secure and appropriate exchange of health and human services information to enable providers to work together and improve an individual's health and wellbeing.

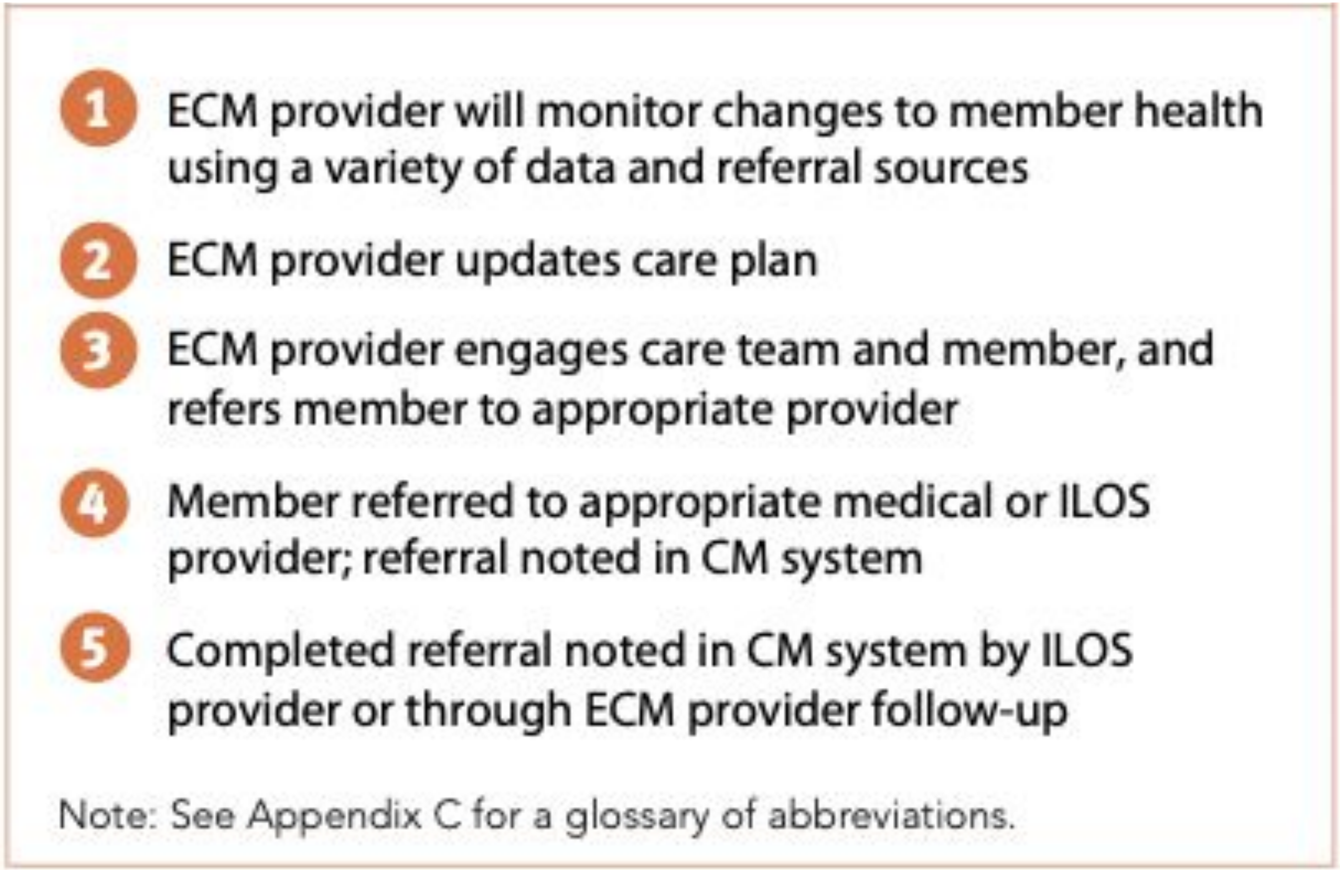
DxF Principles

1. Advance health equity
2. Make data available to drive decisions and outcomes
3. Support whole person care
4. Promote individual data access
5. Reinforce individual data privacy and security
6. Establish clear and transparent terms and conditions for data collection, exchange and use
7. Adhere to data exchange standards
8. Ensure accountability

How information exchange supports the whole person

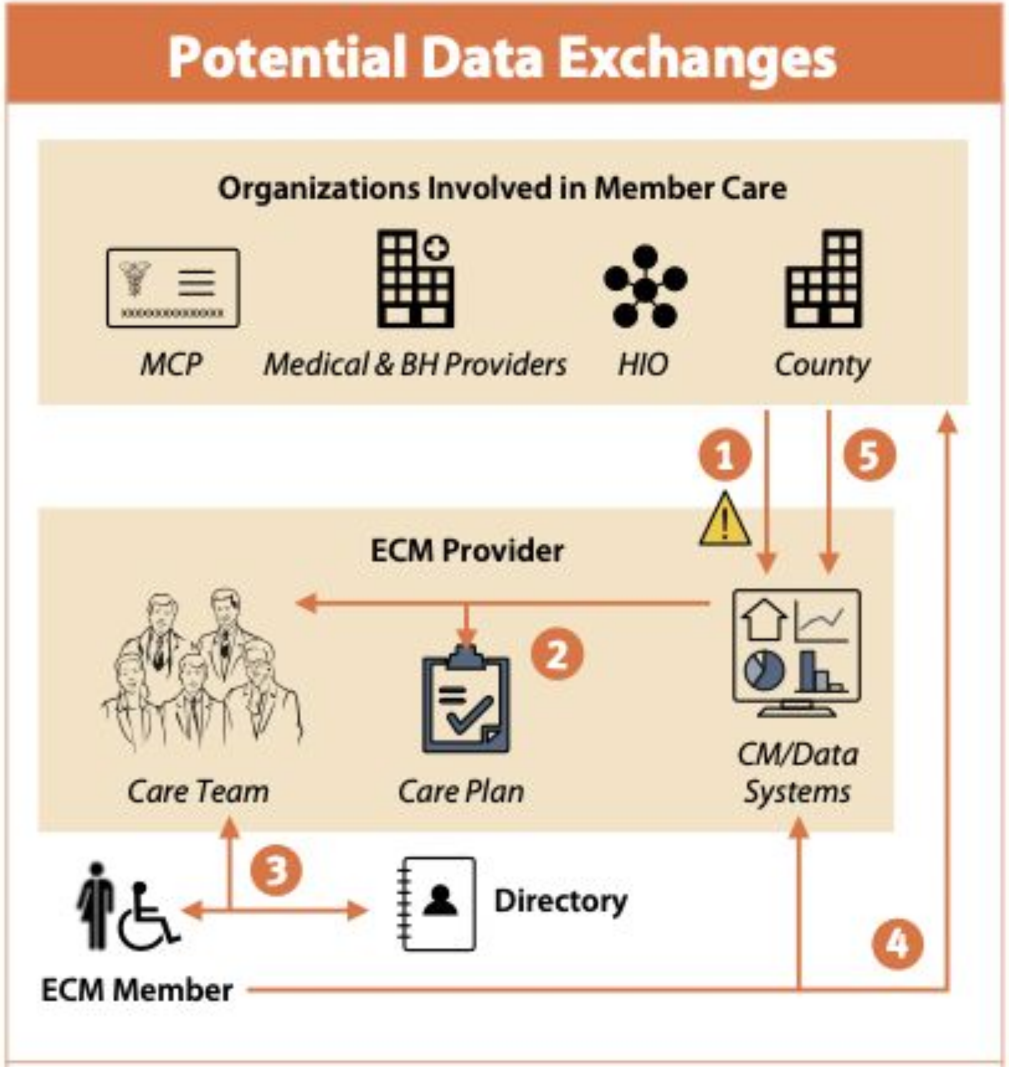


Using data exchange to advance care coordination



1. ECM provider will monitor changes to member health using a variety of data and referral sources
2. ECM provider updates care plan
3. ECM provider engages care team and member, and refers member to appropriate provider
4. Member referred to appropriate medical or ILOS provider; referral noted in CM system
5. Completed referral noted in CM system by ILOS provider or through ECM provider follow-up

Note: See Appendix C for a glossary of abbreviations.



https://www.chcf.org/wp-content/uploads/2021/04/CalAIMHealthDataSharingRoadMapECMILOS.pdf

Poll Exercise

How will the DxF benefit your organization and your community?

Scan here!

How will the DxF benefit your organization and your community?

✓ 0

Nobody has responded yet.

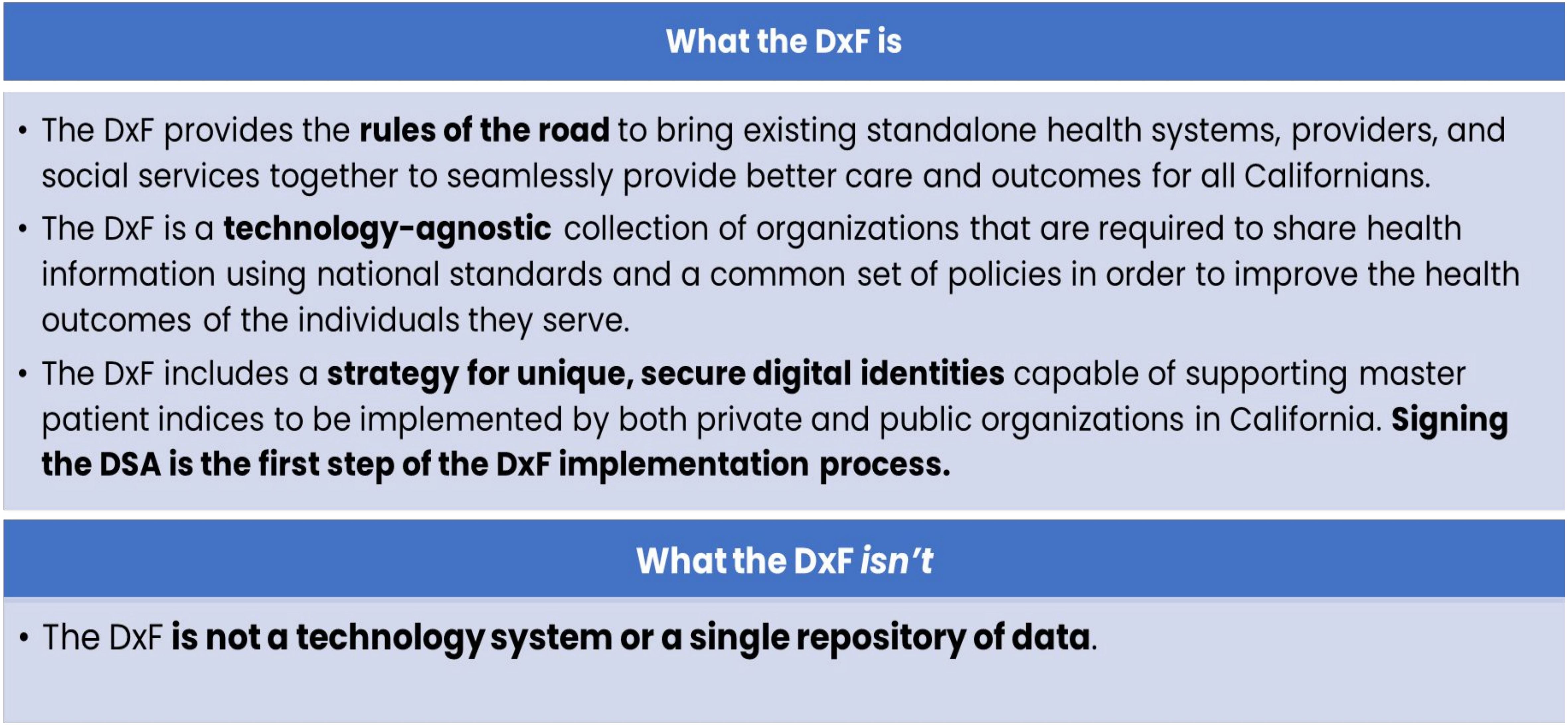
Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

DxF Overview

DATA EXCHANGE FRAMEWORK • CALIFORNIA HEALTH & HUMAN SERVICES •

About the California DxF



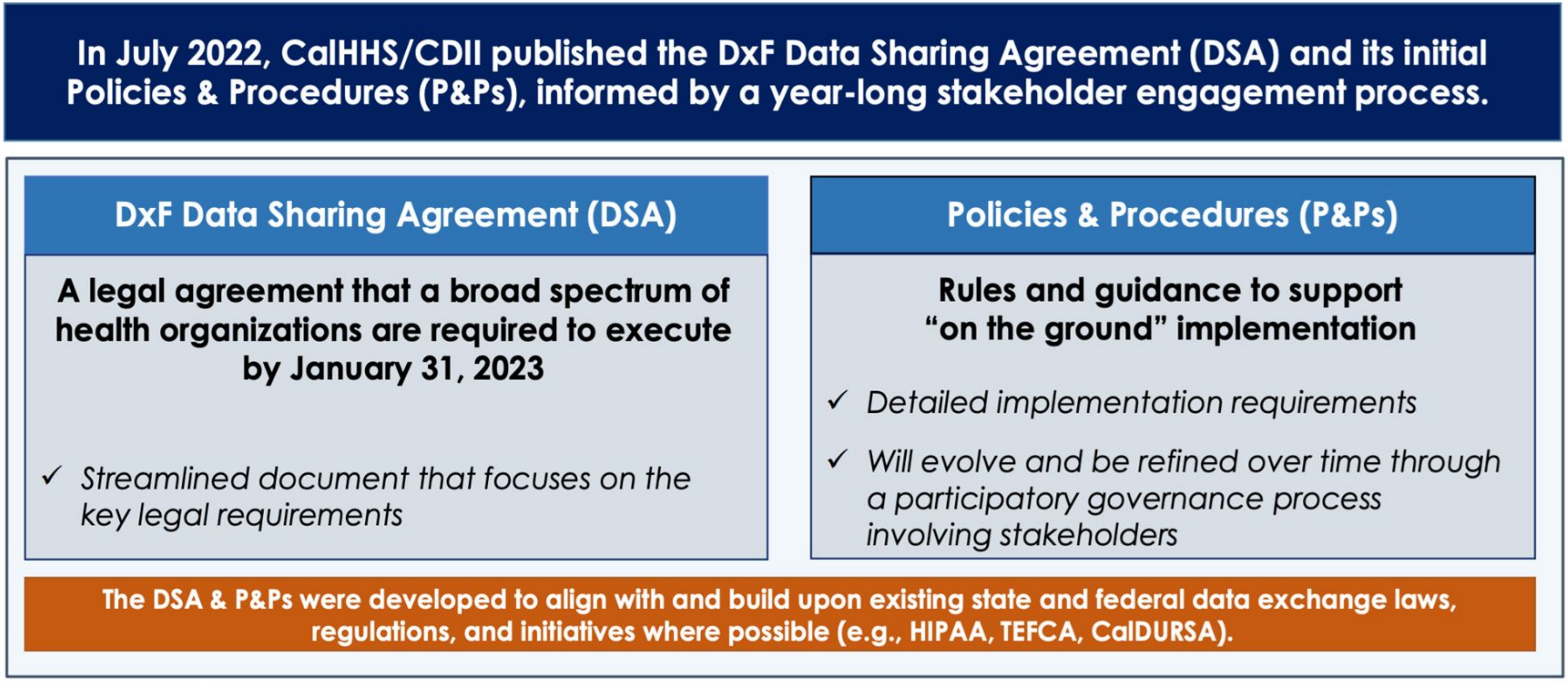
What the DxF is

- The DxF provides the **rules of the road** to bring existing standalone health systems, providers, and social services together to seamlessly provide better care and outcomes for all Californians.
- The DxF is a **technology-agnostic** collection of organizations that are required to share health information using national standards and a common set of policies in order to improve the health outcomes of the individuals they serve.
- The DxF includes a **strategy for unique, secure digital identities** capable of supporting master patient indices to be implemented by both private and public organizations in California. **Signing the DSA is the first step of the DxF implementation process.**

What the DxF *isn't*

- The DxF **is not a technology system or a single repository of data**.

What is the Data Sharing Agreement?



In July 2022, CalHHS/CDII published the DxF Data Sharing Agreement (DSA) and its initial Policies & Procedures (P&Ps), informed by a year-long stakeholder engagement process.

DxF Data Sharing Agreement (DSA)

A legal agreement that a broad spectrum of health organizations are required to execute by January 31, 2023

- ✓ *Streamlined document that focuses on the key legal requirements*

Policies & Procedures (P&Ps)

Rules and guidance to support "on the ground" implementation

- ✓ *Detailed implementation requirements*
- ✓ *Will evolve and be refined over time through a participatory governance process involving stakeholders*

The DSA & P&Ps were developed to align with and build upon existing state and federal data exchange laws, regulations, and initiatives where possible (e.g., HIPAA, TEFCA, CalDURSA).

What organizations are going to share data, and what data?

Who are Participants?

- Mandatory signatories, which are mostly health services organizations
- Non-mandatory signatories, such as community-based organizations, county agencies, and technology companies (DSA Signatory List)

What is health and social services information (HSSI)?

- "…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**." (DxF Glossary)

When do organizations need to start sharing information? (1/2)

The following were ***required to sign*** the DSA by January 31, 2023, and are ***required to begin exchanging*** information or provide access by **January 31, 2024**:

- General acute care hospitals
- Acute psychiatric hospitals (100+ beds)
- Physician organizations (e.g., Independent Practice Associations that exchange health information) and medical groups (with 25+ physicians)
- Skilled nursing facilities that currently maintain electronic records or electronic health information
- Health care service plans and disability insurers
- Clinical laboratories regulated by CDPH

When do organizations need to start sharing information? (2/2)

The following were ***required to sign*** the DSA by January 31, 2023, and are ***required to begin exchanging*** information or provide access by **January 31, 2026**:

- Physician organizations (e.g., Independent Practice Associations that exchange health information) and medical groups with >25 physicians

The following are ***not required to sign***, but if they do, are r***equired to begin exchanging*** information or provide access by **January 31, 2026**:

- Governmental organizations
- Social services organizations (including Community-Based Organizations)

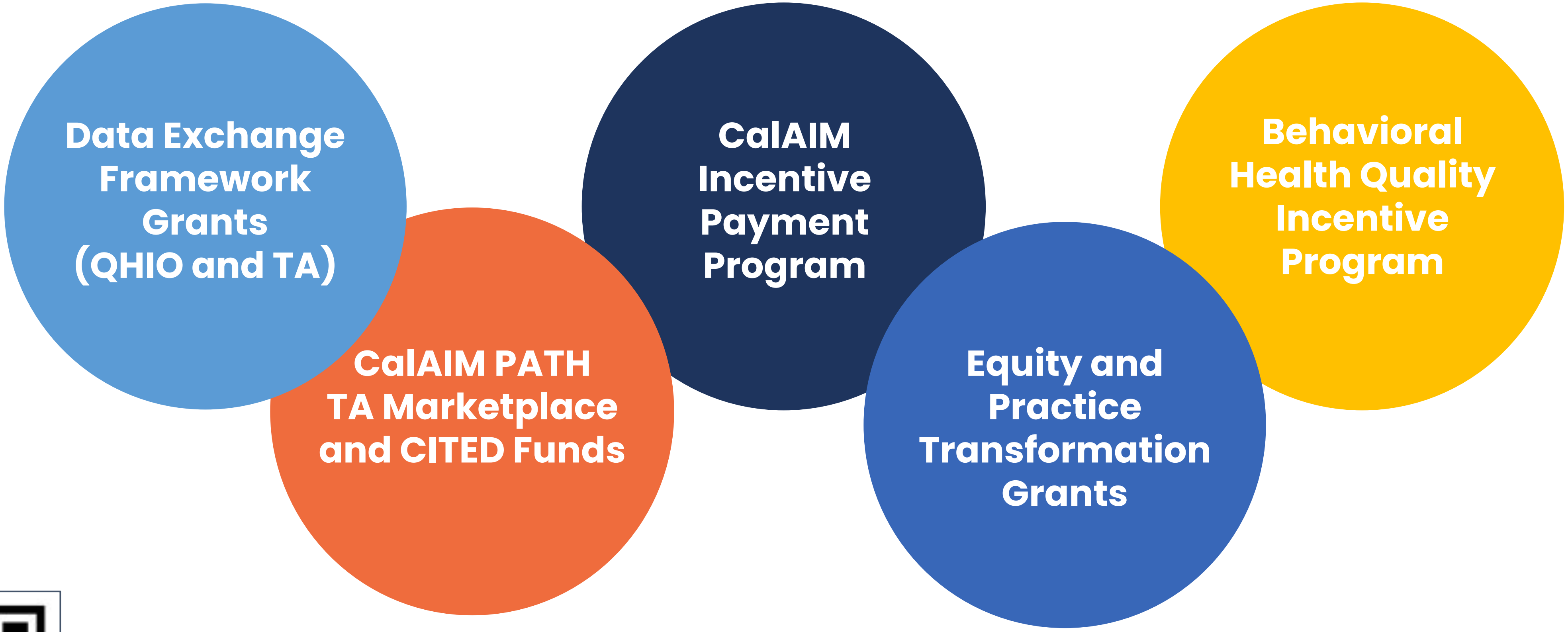
DxF Policies & Procedures (P&Ps)

CDII has published or is in the process of developing the following P&Ps:

Policy & Procedure	**Status**	**Explainers Available**
Process for Amending the DSA	Finalized	
Modifications to Policies and Procedures	Finalized	
Breach Notification	**Finalized**	**Recording | Slides**
Permitted, Required and Prohibited Purposes	**Finalized**	**Recording | Slides**
Requirement to Exchange HSSI	**CDII reviewing public comments**	
Privacy and Security Safeguards	**CDII reviewing public comments**	**Recording | Slides**
Individual Access Services	**Finalized**	**Recording | Slides**
Data Elements to Be Exchanged	**Out for public comment**	
Technical Requirements for Exchange	**Finalized**	**Slides**
California Information Blocking Prohibitions	**Finalized**	**Recording | Slides**
Qualified Health Information Organization	Finalized	
Real-Time Exchange	Finalized	

***Orange indicates P&P to be covered in today's discussion**

Funding opportunities are available to support your data sharing efforts



Data Exchange Framework Grants (QHIO and TA)

CalAIM PATH TA Marketplace and CITED Funds

CalAIM Incentive Payment Program

Equity and Practice Transformation Grants

Behavioral Health Quality Incentive Program

Join your local PATH Collaborative!

CDII DxF grants are available to fund your IT needs

- $47 million available from CDII for DSA signatories to fund data sharing activities
- **Two options:** Technical Assistance ("build you own") and QHIO Onboarding ("assisted pathway")
- **Currently in round 3;** no firm deadline by which to apply, but prospective applicants are encouraged to get their applications in ASAP

TA Grant

This is a flexible, **"build-your-own-solution"** pathway where Signatories identify **a range of technical and operational activities** and managed the entire process of applying for and managing funds directly.

QHIO Onboarding Grant

This is a **pre-set, "assisted" pathway** in which Signatories receive support to identify a technology solution that could fulfill their DSA requirements (i.e. **a QHIO**) and support securing and managing funding for that solution.

How to Apply Workshop Recording Available!

DSA Grants: Funding amounts depend on signatory type, technology instances, and if meet “Underserved Criteria”

- Funding amounts to take into consideration numbers of EHR/other technology instances utilized by applicant
- **Enhanced funding (2x) available** if the applicant serves underserved communities/geographies *and* did not participate in Cal-HOP

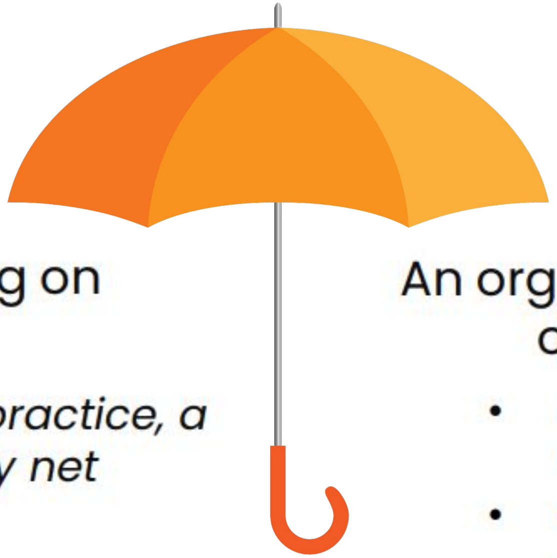
Maximum Funding Amounts by Signatory Type

Signatory Type		Funding Maximum
General Acute Care Hospitals, Acute Psychiatric Hospitals, and Skilled Nursing Facilities	**Serving Underserved Communities/Geographies *and* Did Not Receive Cal-HOP Funding**	**$100,000**
	Other	$50,000
Physician Organizations and Medical Groups	**Serving Underserved Communities/Geographies *and* Did Not Receive Cal-HOP Funding**	**$50,000**
	Other	$35,000
Health Insurance Plans	All	$25,000
Clinical Laboratories	All	$15,000
Other DSA Signatories	**Serving Underserved Communities/Geographies *and* Did Not Receive Cal-HOP Funding**	**$50,000**
	Other	$25,000

Umbrella grants are encouraged

Eligible Signatories may choose to apply on their own, or as part of an "umbrella" application with other Signatories.

An **Applicant** is the organization that submits the Application for a DSA Signatory Grant. They can be:



An eligible Signatory applying on their own behalf

Examples include a solo physician practice, a single county, or an individual safety net hospital.

An organization applying on behalf of one or multiple eligible Signatories.

- *Examples include a corporate parent, an Independent Practice Association, others.*
- *All DSA Signatories included in an Application must co-sign the Application.*

DSA Readiness Activity

DATA EXCHANGE FRAMEWORK

CALIFORNIA HEALTH & HUMAN SERVICES

Activity Objective

The following activity defines your organization in relation to:

1. Your obligations under the DxF
2. Your readiness to implement
3. Your eligibility for DxF grant funding

DSA Signing and Effective Date Considerations

1. **Does your organization need to sign the DSA under A.B. 133 (2021)?**
   - ❏ Yes (see list below)[1]
   - ❏ No
2. **Has your organization signed the DSA?[2]**
   - ❏ Yes
   - ❏ No
3. **If you have not yet signed but are interested in doing so and/or required to do so**
   a. **Who do you need to talk to about signing the DSA?** (E.g., HIT administrator, compliance, legal, etc.)?
   b. **Who at your organization has signing authority?**
   c. **Are you a subsidiary of a larger corporate entity?**
      - ❏ Yes
      - ❏ No
   d. **Are you signing the DSA on behalf of any subsidiaries?**
      - ❏ Yes
      - ❏ No
4. **If you signed the DSA, what is the compliance date by which you must begin sharing and receiving information?**
   - ❏ January 31, 2024
   - ❏ January 31, 2026

[1] Required signatories include general acute care hospitals; Acute psychiatric hospitals (100+ beds); Physician organizations (e.g., Independent Practice Associations that exchange health information) and medical groups; Skilled nursing facilities that currently maintain electronic records or electronic health information; Health care service plans and disability insurers; Clinical laboratories regulated by CDPH

[2] *See DSA signatory list.*

Initial Legal and Technology Considerations

1. **Is your organization – or parts of your organization – a HIPAA Covered Entity?[1]**
   ❏ Yes
   ❏ No

2. **Is your organization a HIPAA Business Associate of a Covered Entity?[2]**
   ❏ Yes, for these organizations: ________
   ❏ No

3. **Do you utilize a certified electronic health record (C-EHR) in your work?[3]**
   ❏ Yes
   ❏ No

[1] See OCR Covered Entity Decision Tool.
[2] See OCR Business Associate Guidance.
[3] See the ONC Health IT Certification website.

DxF Grant Eligibility Considerations

After you have signed the DSA, consider the following questions:

1. **Are you a participant of a QHIO?**[1]
   - ❑ Yes
   - ❑ No

2. **Did your organization receive funding from the Cal-HOP program?**[2]
   - ❑ Yes
   - ❑ No

3. **What are your organization’s technical or technological gaps that need to be addressed to meet your DSA requirements?**

4. **Do you serve an underserved community?**[2]
   - ❑ Yes (see the definition below)[3]
   - ❑ No

[1] See QHIO list on CDII website.

[2] See CDII grant guidance.

[3] E.g., largest facility located in zip code in bottom quartile of Health Places Index, or 30% of patient volume is on Medi-Cal, uninsured or dually eligible

Impact of the DxF on Internal Operations

DATA EXCHANGE FRAMEWORK • CALIFORNIA HEALTH & HUMAN SERVICES •

DxF P&P Related to Internal Operations

Policy & Procedure	**Status**
Process for Amending the DSA	Finalized
Modifications to Policies and Procedures	Finalized
Breach Notification	**Finalized**
Permitted, Required and Prohibited Purposes	**Finalized**
Requirement to Exchange HSSI	CDII reviewing public comments
Privacy and Security Safeguards	**CDII reviewing public comments**
Individual Access Services	Finalized
Data Elements to Be Exchanged	Out for public comment
Technical Requirements for Exchange	Finalized
California Information Blocking Prohibitions	**Finalized**
Qualified Health Information Organization	Finalized
Real-Time Exchange	Finalized

***Orange indicates P&Ps to be discussed in this section**

OPP-4 – Permitted, Required and Prohibited Purposes (1/2)

Purpose:

- To set forth the purposes for which Participants may, or are *required to,* exchange HSSI and certain restrictions on the use by Participants of HSSI obtained under the DxF.

Overview:

- *Required Purposes*:
  - DxF Participants *must* exchange and provide access to HSSI for **Treatment, Payment, Health Care Operations and Public Health Activities.**
- *Permitted and Prohibited Purposes*:
  - Except for accessing HSSI to sell or to take adverse action against an individual (e.g., limit access to medical services or discriminate), **Participants *may* exchange HSSI for any other lawful purpose.**
- *Fees*:
  - Participants **prohibited** from charging fees to other Participants for any exchange of HSSI; provided that QHIOs can still charge Participants who engage in data-sharing activities thru the QHIO.

OPP-4 – Permitted, Required and Prohibited Purposes (2/2)

Impact on Participants:

- **Required Purposes:**
  - **DxF Participants *must* exchange HSSI for Treatment, Payment, Health Care Operations, and Public Health Activities.**
    - Covered Entities under HIPAA are only required to exchange PHI for very limited purposes, and they may disclose PHI for purposes of Treatment, Payment, and Health Care Operations.
  - **Definitions for Treatment and Payment are consistent with those in HIPAA**, but the definition in this P&P and for the purposes of Required Purposes regarding **Health Care Operations encompasses only a subset of HIPAA activities**, including Quality Assessment and Improvement and population-based activities.
- **Permitted and Prohibited Purposes:**
  - Except for accessing HSSI to sell data or to take any adverse action against an individual (e.g., limit access to medical services or discriminate), **Participants *may* exchange HSSI for any other purposes.**
- **Fees:**
  - **Participants *may not* charge fees to other Participants for any exchange of HSSI**
    - QHIOs can still charge fees to Participants who engage in data-sharing activities through the QHIO.

OPP-6 – Privacy and Security Safeguards (1/2)

Purpose:

- Require Participants to use appropriate safeguards to protect the privacy of PHI or PII

Overview:

- Requires Participants to **develop and maintain appropriate safeguards** to prevent unauthorized use or disclosure of protected health information (PHI) or personally identifiable information (PII) in a **manner consistent with HIPAA.**
- Participants that use, access or disclose **behavioral health information** must also comply with 42 CFR Part 2 (federal regulations governing the confidentiality of substance use disorder records), and California's Lanterman-Petris-Short Act (governing confidentiality of information and records obtained in the course of providing mental health services by certain entities).
- **If the Participant is not a Covered Entity or a Business Associate, the Participant must comply with HIPAA's Security Rule.**
- *See appendix for additional detail on proposed changes to this P&P*

OPP-6 – Privacy and Security Safeguards (2/2)

Impact on Participants

- **For non-Covered Entities/Business Associates:**
  - **May not use, access or disclose PHI received from other participants**
    - In normal circumstances, HIPAA protections end after a disclosure unless an agreement specifies otherwise
  - **Comply with minimum necessary standard in sharing information**
    - Under HIPAA, Covered Entities/Business Associates only need to practice minimum necessary for Payment and Operations, not Treatment purposes
  - **Comply with Security Rule**
- **All participants**
  - Must conduct trainings on an annual basis
    - HIPAA does not specify a specific cadence

OPP-10 – California Info Blocking Prohibitions (1/3)

Purpose:

- To support the DxF’s commitment to facilitating the timely access, exchange, and use of Health and Social Services Information in compliance with applicable law.

Overview:

- **Prohibits Participants from undertaking any practice that is likely to interfere with access, exchange, or use** of HSSI for the Required Purposes set forth in the Permitted, Required and Prohibited Purposes Policy and Procedure.
- **No impact on a Participant’s obligation, if any, to comply with the Federal Information Blocking Regulations.**

OPP-3 – California Info Blocking Prohibitions (2/3)

- The P&P incorporates by reference the federal information blocking exceptions under the final rule adopted by the US Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC) under the information blocking provisions of the 21st Century Cures Act.
    - **Participants deemed in compliance with the P&P if they comply with the Federal Information Blocking Regulations.**
        - *Subject to certain exceptions!*
    - P&P also notes that a Participant may rely on current and future guidance from the federal government to interpret the requirements of the Federal Information Blocking Regulations.

The Office of the National Coordinator for
Health Information Technology

OPP-3 – California Info Blocking Prohibitions (3/3)

Impact on Participants

- **A participant that is subject to the ONC Final Rule is deemed in compliance with the P&P if the participant meets an information blocking exception to the ONC Final Rule with respect to HSSI, *except* that the P&P specifically excludes the fees and licensing exceptions**
- Participants that are NOT covered actors under the ONC Final Rule are generally deemed to be in compliance with the P&P if they meet one of the ONC Final Rule exceptions to the information blocking prohibition, other than the Fees and Licensing Exceptions.
  - Note that there are also minor definitional changes to the Preventing Harm Exception and a requirement that any denial of access under the Privacy Exception be consistent with applicable law and/or the Individual Access P&P.

OPP-3- Breach Notification (1/2)

Purpose:

- Set forth the procedure Participants must follow in the event of a "Breach"

Overview:

- Requires Participants to **notify and provide written reports to "impacted" participants and the DxF Governance Entity of "Breaches"**
  - As soon as reasonably practicable after discovering the Breach has occurred, and within any timeframes required by "Applicable Law"
- **Extends Participants' data breach reporting obligations beyond current requirements** (e.g., HIPAA, Cal. Health & Safety Code, Section 1280.15, etc.)

OPP-3- Breach Notification (2/2)

Impact on Participants:

- Extends Participants’ data breach reporting obligations beyond current requirements (e.g., HIPAA, Cal. Health & Safety Code, Section 1280.15, etc.)
- **Differences with HIPAA:**
  - □ **The HIPAA definition contains the following exceptions:** (i) Any unintentional acquisition, access, or use of PHI by a workforce member if in good faith, (ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, or (iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
  - □ **Requires reporting of breaches where data affected hasn’t been compromised,** with no provisions related to the conduction of risk analyses unlike in HIPAA and Cal. Health & Safety Code, Section 1280.15, which do not require reporting if a risk analysis concludes there is a low probability that data was not compromised.
  - □ **Requires breach reporting of social service information by including HSSI in the breach definition,** whereas there is no current requirement under federal or state law to report breaches of social service information.
  - □ **Under this P&P, Participants have expanded breach reporting obligations which requires them to notify and provide written reports to “impacted” Participants and the DxF Governance Entity.**

DSA Compliance Activity

DATA EXCHANGE FRAMEWORK

CALIFORNIA HEALTH & HUMAN SERVICES

Activity Objective

Review areas for internal updates to comply with the following P&Ps:

- Breach Notification
- Permitted, Required and Prohibited Purposes
- Privacy and Security Safeguards
- California Information Blocking Prohibitions

Purposes / Privacy and Security P&P Considerations

1. **Do you have internal policies and procedures related to privacy and security?**
   - ❑ Yes
   - ❑ No

2. **Do your internal P&Ps include the requirement to share data with other DSA participants for all treatment, payment and operations purposes, as specified (beyond HIPAA requirements)?**
   - ❑ Yes
   - ❑ No

3. **Do your internal P&Ps cover HSSI – beyond just PHI or specific data types?**
   - ❑ Yes
   - ❑ No

4. **For non-Covered Entities/Business Associates: Do your P&Ps include methods for preventing the re-use or disclosure of PHI received under the DSA?**
   - ❑ Yes
   - ❑ No

Information Blocking P&P Considerations

1. **Do your internal P&Ps contain sections on information blocking?**
   - ❏ Yes
   - ❏ No

2. **Is your organization a health IT developer or actor subject to the federal information blocking rule?**
   - ❏ Yes
   - ❏ No

   a. **If yes, do your P&Ps account for DSA exclusion of the fees and licensing exceptions to the federal rule?**
      - ❏ Yes
      - ❏ No

   b. **If yes, do your P&Ps account for the DSA changes to the preventing harm exception related to "professional relationships"?**
      - ❏ Yes
      - ❏ No

Breach Notification P&P Considerations

1. **Does your organization have a breach notification P&P?**
   ❑ Yes
   ❑ No

2. **Is your organization subject to HIPAA?**
   ❑ Yes
   ❑ No

   a. **If yes, do your P&Ps account for DSA removal of certain exceptions to breach notification?**
      ❑ Yes
      ❑ No

   b. **If yes, do your P&Ps account for the DSA exclusion of risk analyses provision?**
      ❑ Yes
      ❑ No

Break
10 Minutes

DATA EXCHANGE FRAMEWORK

CALIFORNIA HEALTH & HUMAN SERVICES

DxF Technical Exchange Requirements

P&Ps Related to Technical Exchange Requirements

Policy & Procedure	**Status**
Process for Amending the DSA	Finalized
Modifications to Policies and Procedures	Finalized
Breach Notification	Finalized
Permitted, Required and Prohibited Purposes	Finalized
Requirement to Exchange HSSI	**CDII reviewing public comments**
Privacy and Security Safeguards	CDII reviewing public comments
Individual Access Services	**Finalized**
Data Elements to Be Exchanged	**Out for public comment**
Technical Requirements for Exchange	**Finalized**
California Information Blocking Prohibitions	Finalized
Qualified Health Information Organization	Finalized
Real-Time Exchange	Finalized

***Orange indicates P&Ps to be discussed in this section**

OPP-5 – Requirement to Exchange HSSI (1/2)

Purpose:

Set forth Participants' responsibilities to respond to requests for HSSI, and to exchange HSSI.

Overview:

- **All Participants must *respond* to requests for HSSI made by other Participants**
  - by providing the information in accordance with the law, OR
  - by providing a clear written response that states the HSSI is not available, cannot be exchanged under Applicable Law, or is not required to be shared under the DSA
  - as soon as reasonably practicable
- Clarifies that the DxF is intended to be technology agnostic – meaning it does not prescribe a method of data exchange.
- Certain health care entities (with limited exceptions) must begin sharing by 1/31/2024
  - Excepted health care entities, governmental organizations and social services organizations have until 1/31/2026

The term "**Health and Social Services Information**" encompasses not just protected health information (PHI) subject to HIPAA, but also any personal information as defined by California law (PI). *The definition also extends to "de-identified data, anonymized data, pseudonymized data, metadata, digital identities, and schema."*

OPP-5 – Requirement to Exchange HSSI (2/2)

Impact on Participants

- **Imposes new requirement that all Participants respond to requests**
  - Under current law, no such requirement
  - Under national networks (e.g., Carequality), participants are encouraged to respond but not required to do so
- Clarifies 1/31/2024 and 1/31/2026 deadlines to begin sharing information

OPP-8 - Data Elements to Be Exchanged (1/2)

Purpose:

- Set forth the information that Participants must either make available or exchange.

Overview:

- **For health care providers, county health facilities, and public health agencies, all Electronic Health Information (EHI)** as defined in the federal information blocking rules (45 CFR 171.102) – i.e., the entire designated record set, other than—
  - Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
- **For health plans, all data required to be shared under the CMS Interoperability rule**, which includes but is not limited to all adjudicated claims, encounter and clinical data
- Participant is required to provide access to or exchange of HSSI if and only if it has access to, control over, and authority to share the data.

OPP-8 – Data Elements to Be Exchanged (2/2)

Impact on Participants

- Providers required to share all EHI in their possession–that is, all the electronic PHI they have
- Plans are required to share not just claims and encounter data, but also clinical data in their possession
    - These requirements may differ from existing contributions made by these entities to HIEs today (e.g., CCDA, ADT and claims/encounter feeds)

OPP-9 – Technical Requirements (1/3)

Purpose:

- To describe 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 data exchange patterns.

Overview:

- *Key Terms*:
  - Order or Referral
  - Request for Information
  - Response
- *Request for Information*:
  - Requires requesting Participants to **make a request for HSSI using IHE XCPD exchange profile for person matching** to determine if a Participant maintains HSSI on the Individual
  - Participants must accept and respond to an electronic Request for Information from another Participant either with an appropriate null response or error message OR using IHE XCPD exchange profile
  - **Strongly discourages Participants from making 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, when potential sources of HSSI for the Individual are not known

OPP-9 – Technical Requirements (2/3)

Overview (cont'd):

- ***Information Delivery*:**
  - Governs the delivery of HSSI regarding a specific Individual to a specific Participant in conjunction with an Order or Referral.
- ***Notification of Admit, Discharge, Transfer (ADT) Events:***
  - Sets out specific requirements for the communication of ADT Events sent by a sending Participant to a receiving Participant for specified Individuals requested by the receiving Participant.
    - Participants that are **Hospitals or EDs must send Notification of ADT Events** unless prohibited by Applicable Law and must accept requests for Notification of ADT Events from any other Participant and send using a secure method compliant with the Privacy Standards and Security Safeguards P&P.
    - SNF Participants are encouraged to communicate admissions, discharges, and transfers to requesting Participants using the same methods as Hospitals or EDs. SNFs may be required to communicate admissions, discharges, and transfers in future revisions of this policy.
- ***Person Matching*:**
  - Sets out the process by which a Participant ensures that exchanged Health and Social Services Information is appropriately linked to the correct real person.

OPP-9 – Technical Requirements (3/3)

Impact on Participants

- **Creates new legal obligation to adhere to technical requirements that otherwise don’t exist in statute or regulation (exception for ADTs, see below)**
  - However, the IHE profiles mentioned align with those required in the federal Trusted Exchange Framework and Common Agreement (TEFCA), and those used in national networks like Carequality
- **Expansion of ADT requirements beyond those required by Medicare Conditions of Participation**
  - Participants that are Hospitals or EDs must send Notification of ADT Events unless prohibited by Applicable Law and must accept requests for Notification of ADT Events from any other Participant and send using a secure method compliant with the Privacy Standards and Security Safeguards P&P.
  - SNF Participants are encouraged to communicate admissions, discharges, and transfers to requesting Participants using the same methods as Hospitals or EDs. SNFs may be required to communicate admissions, discharges, and transfers in future revisions of this policy.

OPP-7 – Individual Access Services (1/2)

Purpose:

- To require Participants to provide individuals with access to their PHI or PII.

Overview:

- To the extent permitted by applicable law, an individual or their Personal Representative **has a right of access to inspect and obtain a copy of PHI or PII** about the individual, for as long as the PHI or PII is maintained by a Participant, and once the Participant has verified the identity of the individual.
  - Participants must give individuals the option of using electronic means (e.g., email or secure web portal) or other means determined by Governance Entity to assert access rights
- Participants must respond to a request by individual to add self-reported HSSI to the individual's health records, and must have a process to correct inaccurate information and for reconciling discrepancies in such records to ensure accuracy.
- If a Participant doesn't maintain the PHI or PHI that is requested and the Participant knows where the requested information is maintained, the Participant must inform the individual or their Personal Representative. Participants may also deny request if permitted by law.

OPP-7 – Individual Access Services (2/2)

Impact on Participants

- **Expands the scope of individual access beyond HIPAA and Cal. Health & Safety Code 123100 *et seq.* by asserting that an Individual or their Personal Representative has a right of access to inspect and obtain a copy of an Individual's HSSI, not just their PHI.** This applies if the information is maintained by the Participant and once the requestor's identity has been verified as consistent with HIPAA, 45 C.F.R. § 164.514(h), and other Applicable Law. Additionally, Participants must:
    - Allow the option of using electronic means to *access an Individual's information*, whereas HIPAA allows covered entities to offer electronic means *for requests*.
    - Respond to requests to add self-reported HSSI, which is unique from current law, and have a process to correct inaccurate information.
    - Inform requestors where requested HSSI is maintained if they do not maintain it and know where the requested information is accessible.
- In line with current law, this P&P does not prohibit charging fees for copying/inspecting records. It does however prohibit charging other Participants fees to exchange HSSI.

Technology and Data Exchange Mechanisms

DATA EXCHANGE FRAMEWORK

CALIFORNIA HEALTH & HUMAN SERVICES

What is data sharing?

Data sharing allows patients and the organizations that provide or pay for their care to appropriately access and securely share a patient's vital medical information electronically.

Common legal obligations

Defined technical specifications

Optimal participant directory within catchment area

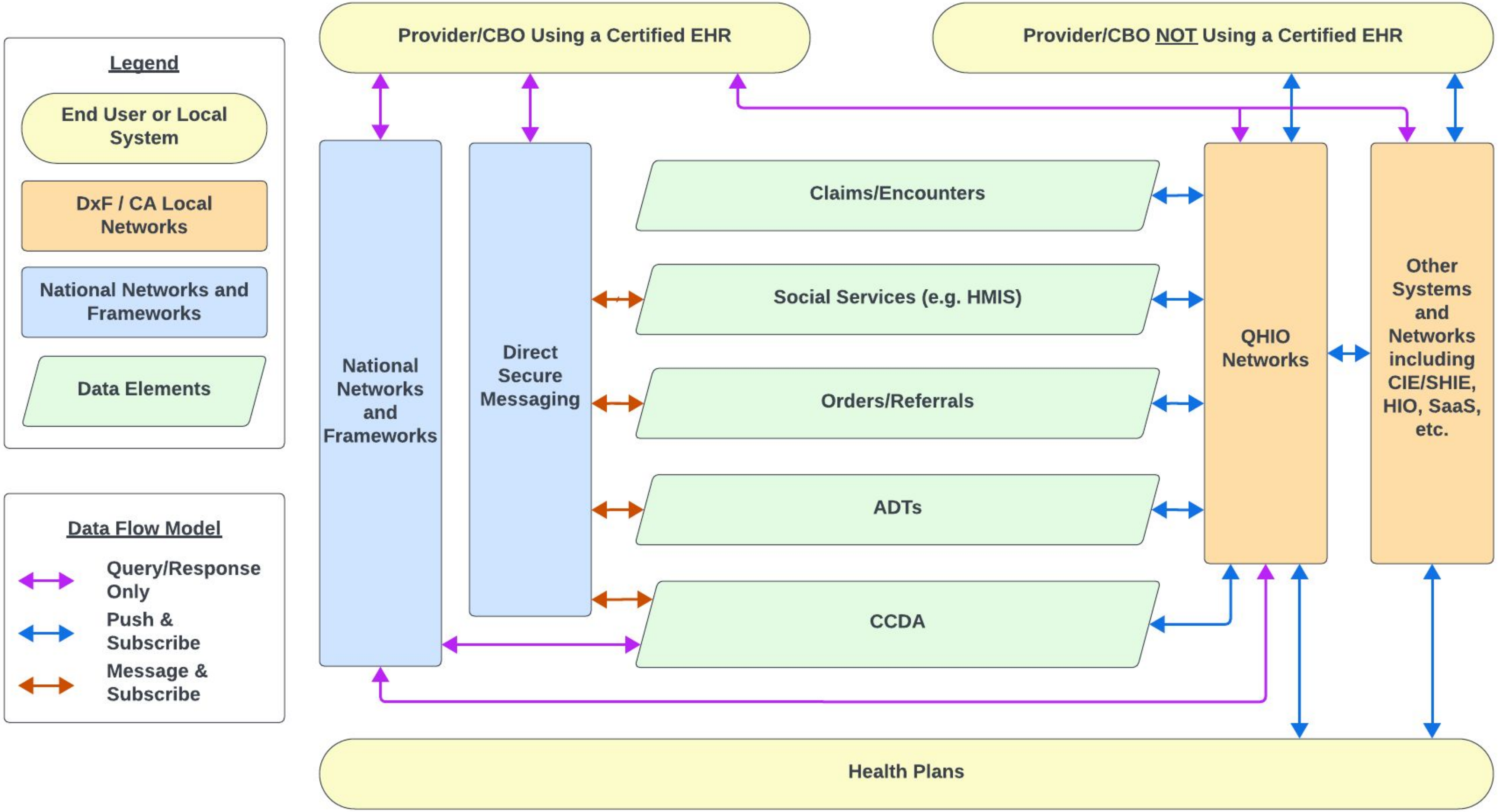
Three key forms of data sharing:

- **Directed Exchange**: Ability to send and receive secure information electronically between care providers to support coordinated care
- **Query-based Exchange**: ability for providers to find and/or request information on a patient from other providers, often for unplanned care
- **Consumer Mediated Exchange**: ability for patients to aggregate and control the use of their health information among providers

Data Sharing Methods and Value

Methods	Definition	Use Case Sample & Value
Query - Response	Communication or information exchange that may occur in real-time in which the query sender requests specific information/data from another entity, the responder **(often through automation)**, and receives the appropriate data requested.	Provider X requires a summary of care for 'new' Patient 1 to establish an understanding of their health history. **Real-time access to data as needed and comprehensive access to information.**
Message - Subscribe	Communication or information exchange that **occurs asynchronously via a message** requesting information from the sender, with **manual intervention** by the responder prior to the data being sent to the requestor.	Provider X requires a procedure summary for Patient 1 who recently visited the Provider Y at a hospital. Summary was unavailable when attempting a query-response through national network and using this method to get the data. **Request and receive data as needed with known delay.**
Push - Subscribe	Communication or information exchange that **occurs proactively** for a providers patients based on an established roster of information to be shared **when an patient event occurs.**	Provider X establishes a patient roster with Entity 1 allowing for proactive data sharing for anyone on a list of patients when a given event occurs. **e.g. ADT events.** Data access via push when patients have a healthcare event that requires provider awareness and/or follow-up.

What can data exchange look like under the DxF?


Legend
End User or Local System
DxF / CA Local Networks
National Networks and Frameworks
Data Elements
Data Flow Model
Query/Response Only
Push & Subscribe
Message & Subscribe
Provider/CBO Using a Certified EHR
Provider/CBO NOT Using a Certified EHR
National Networks and Frameworks
Direct Secure Messaging
Claims/Encounters
Social Services (e.g. HMIS)
Orders/Referrals
ADTs
CCDA
QHIO Networks
Other Systems and Networks including CIE/SHIE, HIO, SaaS, etc.
Health Plans

Operationalizing HSSI: Data Elements To Consider

- Claims / Encounters
- Social Services
- Orders / Referrals
- ADTs
- CCDA

Clinical Data Per USCDI V.2

Patient Demographics	Medications
Clinical Notes	Patient Goals
Clinical Tests	Laboratory data
Encounter Information	Smoking Status
Care Team Member(s)	Assessment and Plan of Treatment
Provenance	Problems
Allergies and Intolerances	Procedures
Immunizations	Vital Signs
Diagnostic Imaging	Unique Device Identifiers for a patient’s implantable Devices(s)

Networks and Systems (1/2)

- Is connectivity through a National Network or Framework enough?
- How do I meet the real-time requirements within the DSA?
- How do CIEs factor into my HSSI data needs and where do I access it and how do I store or use that data?
- Some large enterprise EHRs may be able to cover a lot of requests within their brand, via their own network for exchange and national network capabilities but Participants may have further gaps to address

National Networks and Frameworks

Direct Secure Messaging

Other Systems and Networks (Including CIE/SHIE, HIO, SaaS, etc)

QHIO Networks

Many DxF Participants will need to connect in multiple manners with different solutions

Networks and Systems (2/2)

Network/ System	Capabilities	Examples	Limitations
National Networks and Frameworks	• Access to clinical records in external systems • Centered on certified EHRs	• Carequality • CommonWell Health Alliance • TEFCA (not yet live)	• Limited to CCDAs at this time; no ADT, claims, social services data • Largely limited to Treatment purposes
Direct Secure Messaging	• Enables a push mechanism (sender-initiated) for exchanging encrypted health information among clinicians, patients, and organizations via the Internet	• DirectTrust	• Data Integrity Issues • Lack of standardization or message handling • May increase clinician burden with more manual processes
QHIO Networks	• Aggregation of health and social services information across participants • Centered on all DSA signatories	• See list on slide 66	• DSA P&Ps largely focused on health care organizations; additional guidance needed to support social services
Other HIOs and CIE/SHIEs	• Aggregation of health and social services information to varying degrees, depending on community/customer needs • Related to vendor/ 2-1-1/ other specific entity/constituency	• Alameda SHIE • Epic Care Everywhere • 2-1-1 San Diego CIE	• Often limited to use of vendor solution/ specific community • Only CIEs typically contain social service data
Certified EHR	• An electronic system that meets certain criteria, with ability to build and maintain a longitudinal patient record	• Epic • Cerner • NextGen • Allscripts	• Variability of national network standards used

QHIOs must be able to meet the following Criteria:

1. Currently engaged in health information exchange
2. Must maintain privacy and security of PHI and PII
3. Must provide patient identity management and matching
4. Must participate in Carequality, CommonWell Health Alliance, or eHealth Exchange national networks
5. Must exchange information with other QHIOs and via the nationwide network(s) and framework(s) in which they participate
6. Must receive, process, and forward HL7 v2.5.1 Admit, Discharge, Transfer (ADT) event notifications

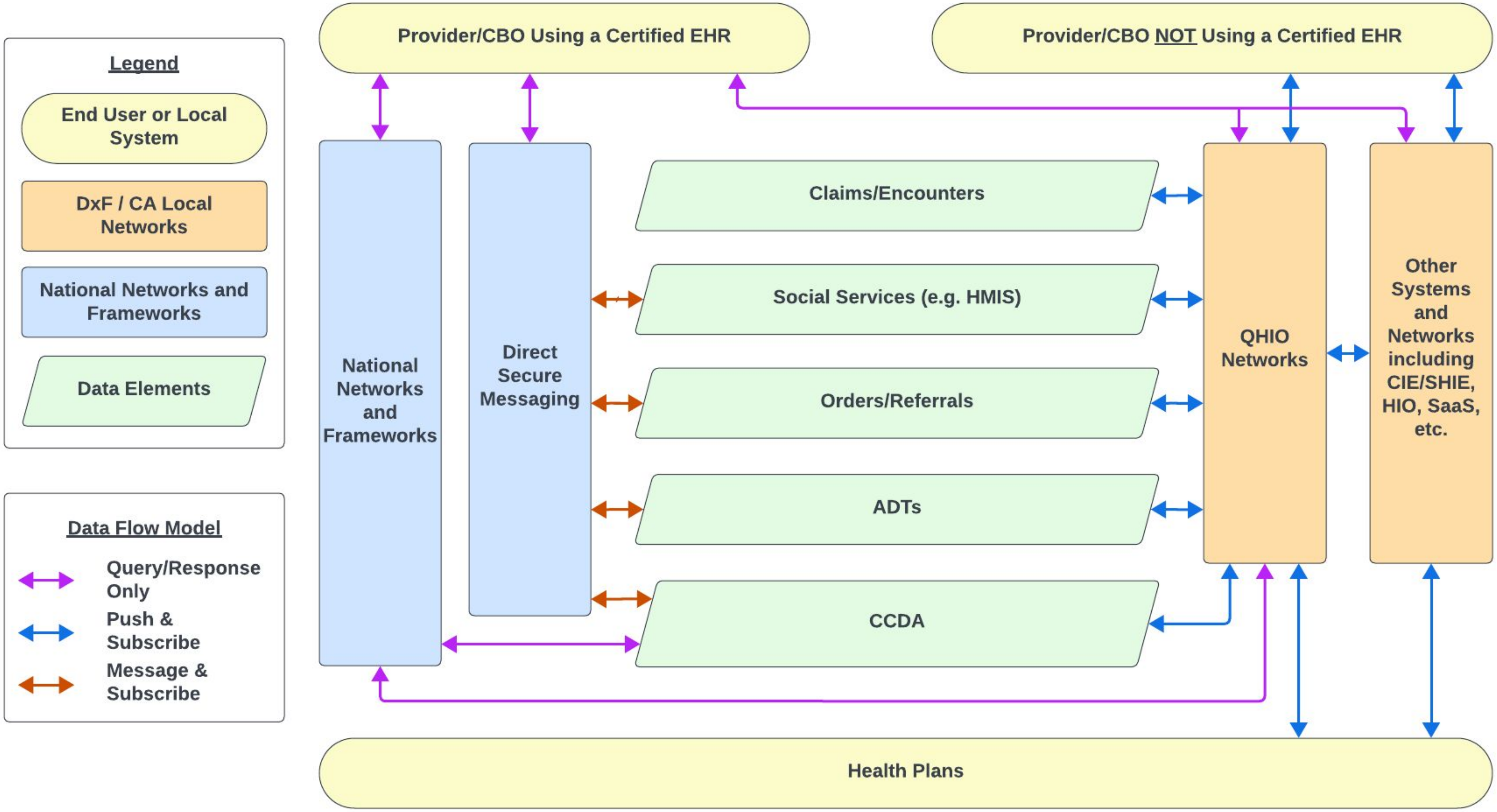
Designated DxF QHIOs

Nine organizations designated as qualified health information organizations (QHIOs) to assist Participants in meeting their DxF obligations:

- **Applied Research Works, Inc. (Cozeva)**
- **Health Gorilla, Inc.**
- **Long Health, Inc.**
- **Los Angeles Network for Enhanced Services (LANES)**
- **Manifest MedEx**
- **Orange County Partners in Health – Health Information Exchange (OCPH-HIE)**
- **SacValley MedShare**
- **San Diego Health Connect**
- **Serving Communities Health Information Organization (SCHIO)**

DATA EXCHANGE FRAMEWORK • CALIFORNIA HEALTH & HUMAN SERVICES

What can data exchange look like under the DxF?



Legend

End User or Local System

DxF / CA Local Networks

National Networks and Frameworks

Data Elements

Data Flow Model

Query/Response Only

Push & Subscribe

Message & Subscribe

Provider/CBO Using a Certified EHR

Provider/CBO NOT Using a Certified EHR

National Networks and Frameworks

Direct Secure Messaging

Claims/Encounters

Social Services (e.g. HMIS)

Orders/Referrals

ADTs

CCDA

QHIO Networks

Other Systems and Networks including CIE/SHIE, HIO, SaaS, etc.

Health Plans

Technical Exchange Activity

DATA EXCHANGE FRAMEWORK

CALIFORNIA HEALTH & HUMAN SERVICES

Activity Objective

Consider how your organization may approach data exchange under the DxF by examining the following questions:

- What data do I share now?
- What data do I need to share?
- How do I currently share data and how could I share data?
- Who do I need data from? How do/will I get that data?

Technology considerations for your organization

Complete this exercise for each solution you are using today to collect data.

1. **What system(s) are you using to collect HSSI?**
2. **What data are collected?**
3. **How are you sharing (sending and receiving) different types of HSSI?**
   - ❏ Claims:
   - ❏ Encounters:
   - ❏ CCDA:
   - ❏ Other:
4. **With whom do you share data?**
   - ❏ Health plan:
   - ❏ Hospital:
   - ❏ Other provider:
   - ❏ CBO:
   - ❏ Other:
5. **What data would you like to be receiving, and from whom?**
6. **What data would you like to be sending, and to whom?**
7. **What mechanisms are available to receive or send such data?**

Technology considerations for your community

1. **What resources are available in your community today?**
   - ❏ Community Information Exchange:
   - ❏ Health Information Organization:
   - ❏ QHIO :
   - ❏ 2-1-1:
   - ❏ Closed Loop Referral System:
   - ❏ ADT Network:
   - ❏ Other:
2. **What specific issues related to these resources do you need more information on to make an informed decisions about whether to take advantage of or participate in these resources?**
   - ❏ Onboarding process
   - ❏ Workflow
   - ❏ Data Governance
   - ❏ Cost
   - ❏ Availability
   - ❏ Other
3. **What other resources not mentioned here are required for your community to meet your DSA needs?**

Discussion and Reflections

DATA EXCHANGE FRAMEWORK

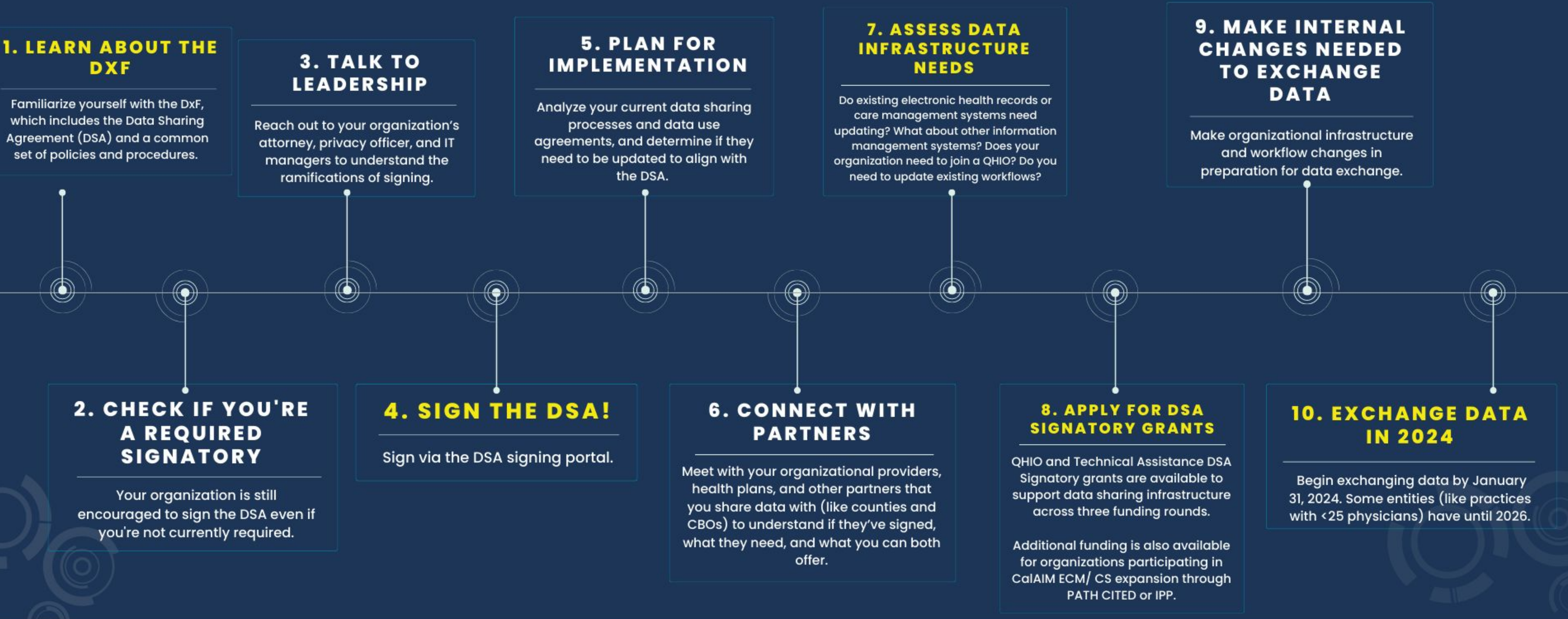
CALIFORNIA HEALTH & HUMAN SERVICES

THE JOURNEY OF DATA SHARING:

How to Sign & Implement the Data Exchange Framework in 10 Steps

DEVELOPED BY THE MULTI-ASSOCIATION DXF EDUCATION INITIATIVE

visit our website for additional resources!



1. LEARN ABOUT THE DXF

Familiarize yourself with the DxF, which includes the Data Sharing Agreement (DSA) and a common set of policies and procedures.

2. CHECK IF YOU'RE A REQUIRED SIGNATORY

Your organization is still encouraged to sign the DSA even if you're not currently required.

3. TALK TO LEADERSHIP

Reach out to your organization's attorney, privacy officer, and IT managers to understand the ramifications of signing.

4. SIGN THE DSA!

Sign via the DSA signing portal.

5. PLAN FOR IMPLEMENTATION

Analyze your current data sharing processes and data use agreements, and determine if they need to be updated to align with the DSA.

6. CONNECT WITH PARTNERS

Meet with your organizational providers, health plans, and other partners that you share data with (like counties and CBOs) to understand if they've signed, what they need, and what you can both offer.

7. ASSESS DATA INFRASTRUCTURE NEEDS

Do existing electronic health records or care management systems need updating? What about other information management systems? Does your organization need to join a QHIO? Do you need to update existing workflows?

8. APPLY FOR DSA SIGNATORY GRANTS

QHIO and Technical Assistance DSA Signatory grants are available to support data sharing infrastructure across three funding rounds.

Additional funding is also available for organizations participating in CalAIM ECM/ CS expansion through PATH CITED or IPP.

9. MAKE INTERNAL CHANGES NEEDED TO EXCHANGE DATA

Make organizational infrastructure and workflow changes in preparation for data exchange.

10. EXCHANGE DATA IN 2024

Begin exchanging data by January 31, 2024. Some entities (like practices with <25 physicians) have until 2026.

What are your next steps with DxF implementation?

1. Are there others in your organization or networks you will engage based on today’s work? If so, who are they?

2. What are your next steps within your organization in implementing the DxF?

3. How will you think differently about local, regional, state, and national exchange?

Reflections

- How will the DxF benefit your organization and your community?

- What are your ideas for next steps for going live with the DxF coming out of today's session?

Wrap Up and Conclusion

DATA EXCHANGE FRAMEWORK

CALIFORNIA HEALTH & HUMAN SERVICES

Stay updated

- To receive updates on the Data Exchange Framework, email CDII@chhs.ca.gov

- For more resources and office hours, check out the DxF Multi-Association Education Initiative Info Hub

- Sign up for Connecting for Better Health's Round-Up

Connecting for Better Health

Advancing data sharing to improve the health of all Californians

Resources

Question inbox: dxfeducation@connectingforbetterhealth.com

CDII LinkedIn/Twitter handles and hashtags:

- CalHHS Center for Data Insights and Innovation/ @Cal_HHS @CDIIgov #DxF

Follow Consultant Groups on LinkedIn/Twitter:

- BluePath Health/@bluepathhealth
- Connecting for Better Health (C4BH)/ @Connecting4H
- Transform Health, LLC/ @transformhc

Follow Associations on LinkedIn/Twitter:

- America's Physician Groups (APG)/@AmerPhysGrps
- California Academy of Family Physicians (CAFP)/@cafp_familydocs
- California Association of Health Facilities (CAHF)/ @CAHFupdates
- California Association of Health Information Exchanges (CAHIE)/ @info_cahie
- California Association of Area Agencies on Aging (C4A)/ @C4A_Sacramento
- Purchaser Business Group on Health (PBGH)/ @PBGHealth

ITUP
Insure the Uninsured Project

Thank You!

Follow ITUP on Social Media!

𝕏 @itup

in @InsuretheUninsuredProject

f @InsuretheUninsuredProject

⌂ www.itup.org

Appendix

DATA EXCHANGE FRAMEWORK

CALIFORNIA HEALTH & HUMAN SERVICES

CalAIM PATH CITED funding enables the transition, expansion, and development of ECM and Community Supports capacity and infrastructure

IT Sample Uses

Allowable Use Category	Sample Activities	Sample Line Items
Modifying, purchasing and/or developing the necessary clinical, referral, billing, data reporting or other infrastructure and IT systems, to support integration into CalAIM: IT/Data System Hardware and Equipment Software (including associated licenses) Implementation Support Planning Other	- Supporting health information exchange between entities responsible for providing ECM and/or Community Supports services - Supporting the implementation of a closed-loop referral system - Enhancing existing systems to support core monitoring/data reporting needs - Transitioning former WPC Pilot infrastructure for integration into ECM/Community Supports and other managed care contracted services - Modifying existing IT systems to support the provision of ECM services to Justice-Involved individuals post-release	- New EHR system *Please note: Applicants should only request funding for the percentage of the IT system that will be used for Medi-Cal members eligible for ECM/Community Supports*

EPT Payments Program Overview

Program Component	Intended Practices	Application	Purpose/Deliverable
Initial Planning Incentive Payments $25M over 1 year MCP Incentive Program	**Small/medium-sized independent practices (1-50 providers)** that might not otherwise be able to participate in Provider Directed Payment Program; **MCPs choose practices**	Practices **work with contracted MCPs** (no formal application to DHCS)	**Began July 2023** To help smaller providers develop practice transformation plans and apply for Provider Directed Payment Program
Provider Directed Payment Program $650M ($200M for preparing practices for value-based payment) over 5 years Directed Payment Program	**Primary care of any size or setting:** primary care Pediatrics, Family Medicine or Internal Medicine; primary care OB/GYN; and/or behavioral health providers providing integrated behavioral health services in a primary care setting	Formal Application Reviewed by MCPs with Final Approval from DHCS	**First Cohort in January 2024** Payments for **delivery system transformation activities,** required and optional
Statewide Learning Collaborative $25M for program duration Structure still being determined	**All practices in Provider Directed Payment Program**	N/A	Provide **support to practices with practice transformation**; will be largely modeled on PHMI materials

EPT Required Technology & Data Activities

Population Health and Quality Improvement Governance

Dashboards and Business Intelligence

Data and Quality Reporting Gaps

New/Upgraded EHR and/or Population Health Management Tool

Data Exchange

P&P – *Draft* Privacy and Security Safeguards

Amended proposed revisions from CDII

Purpose:

- Describes privacy standards and security safeguards Participants must comply with in connection with the exchange of HSSI under the DSA.

Overview:

- Each Participant may only access, use, maintain and disclose HSSI "consistent with Applicable Law and any valid Authorization" and must implement administrative, physical, and technical safeguards to protect HSSI.

Key Updates *(as of 8/21/23)*:

1. Non-Covered Entities' and Business Associates' privacy and security obligations;
2. Standards for De-Identification under the DSA;
3. Record retention requirements related to privacy and security trainings; and
4. Defined terms, including "Securely Destroy," "Loss," "Disruption," and "Destruction."

P&P – *Draft* Privacy and Security Safeguards

Amended proposed revisions from CDII

Applicable law:

- Reminds Participants of more stringent privacy laws beyond HIPAA and CMIA, including
  - 42 C.F.R. Part 2
  - California Consumer Privacy Act
  - California Confidentiality of Medical Information Act
  - Information Practices Act
  - Lanterman-Petris-Short Act & Lanterman Developmental Disabilities Services Act
  - California Health and Safety Code section 11845.5

De-identification:

- Participants must de-identify any PHI or PII received from another Participant in accordance with 45 C.F.R. section 164.514(b) or other more stringent law prior to using or disclosing it (except when exchanging HSSI with another Participant)

P&P – *Draft* Privacy and Security Safeguards

Amended proposed revisions from CDII

Privacy Requirements:

- HIPAA Covered Entities, Business Associates and hybrid entities:
    - Must comply with HIPAA as applicable, and all other Applicable Laws
    - Need to review/update BAAs if conflict with DxF P&Ps

- Non-Covered Entities/Business Associates:
    - With respect to PHI:
        - May not Access, Use or Disclose PHI received from a Covered Entity/Business Associate Participant, except as set forth in 45 CFR section 164.502(a)(1)(i) through (v), including with a valid Authorization;
        - Comply with minimum necessary standards (45 CFR sections 164.502(b) and 164.514(d)); and
        - Comply with HIPAA's verification requirements (45 CFR section 165.514(h)).

P&P – *Draft* Privacy and Security Safeguards

Amended proposed revisions from CDII

Privacy Requirements:

- Non-Covered Entities/Business Associates:
  - With respect to PII:
    - May not Access, Use or Disclose PII received from a Participant, except as contractually permitted or permitted by Applicable Law
    - Only Access, Use, or Disclose PII to extent necessary to achieve intended purpose; and
    - Comply with HIPAA's verification requirements (45 CFR section 165.514(h)).

P&P – *Draft* Privacy and Security Safeguards

Amended proposed revisions from CDII

Security Requirements:

- HIPAA Covered Entities, Business Associates and hybrid entities:
    - Must comply with HIPAA Security Rule, and all other Applicable Laws
    - Need to review/update BAAs if conflict with DxF P&Ps
- Non-Covered Entities/Business Associates:
    - Implement appropriate administrative, physical, and technical safeguards consistent with 45 C.F.R. sections 164.306, 164.308, 164.310, and 164.312, respectively.

P&P – *Draft* Privacy and Security Safeguards

Amended proposed revisions from CDII

Secure Destruction:

- In the event Participant discovers it has received HSSI from another in error, it must "Securely Destroy" the info as soon as possible and notify the disclosing Participant (and both must comply with breach notification requirements, as applicable)

P&Ps; Trainings:

- Participants must have written privacy and security policies and procedures to support Access, Use, Disclosure of PHI and/or PII and prevent Loss, Destruction, Disruption or unauthorized uses/disclosures
- Participants must properly train staff, contractors, agents, employees, and other workforce members before granting access to HSSI
  - Refresher trainings "no less than annually"
- Store records of trainings for at least 6 years