



DATA EXCHANGE FRAMEWORK IMPLEMENTATION TOOLKIT

Multi-Association DxF Education Initiative

December 2023



Consulting Partners



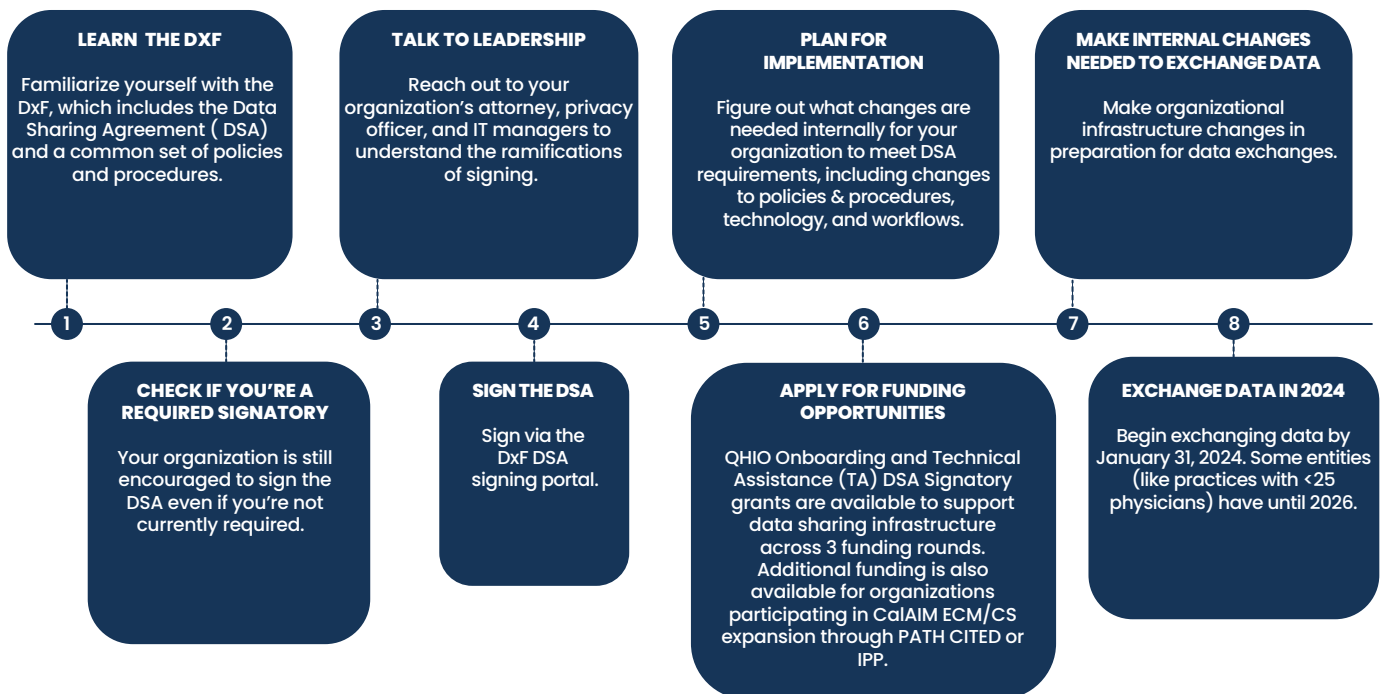
Table of Contents

How to Use This Toolkit	1
Overview	2
Step 1: Understand the Data Exchange Framework (DxF)	4
Step 2: Check if You're a Required Signatory	6
Step 3: Talk to Leadership	8
Step 4: Sign the Data Sharing Agreement (DSA)	9
Step 5: Plan for Implementation	11
Step 6: Apply for Funding Opportunities	23
Step 7: Make Internal Changes Needed for Data Exchange	26
Step 8: Exchange Data in 2024	28
Appendices	
Definitions	29
Resource List	33
DxF Policies & Procedures	34
Further Information on Data Exchange	51
DSA Signatory Grants	53
Acknowledgments	56

How to Use This Toolkit

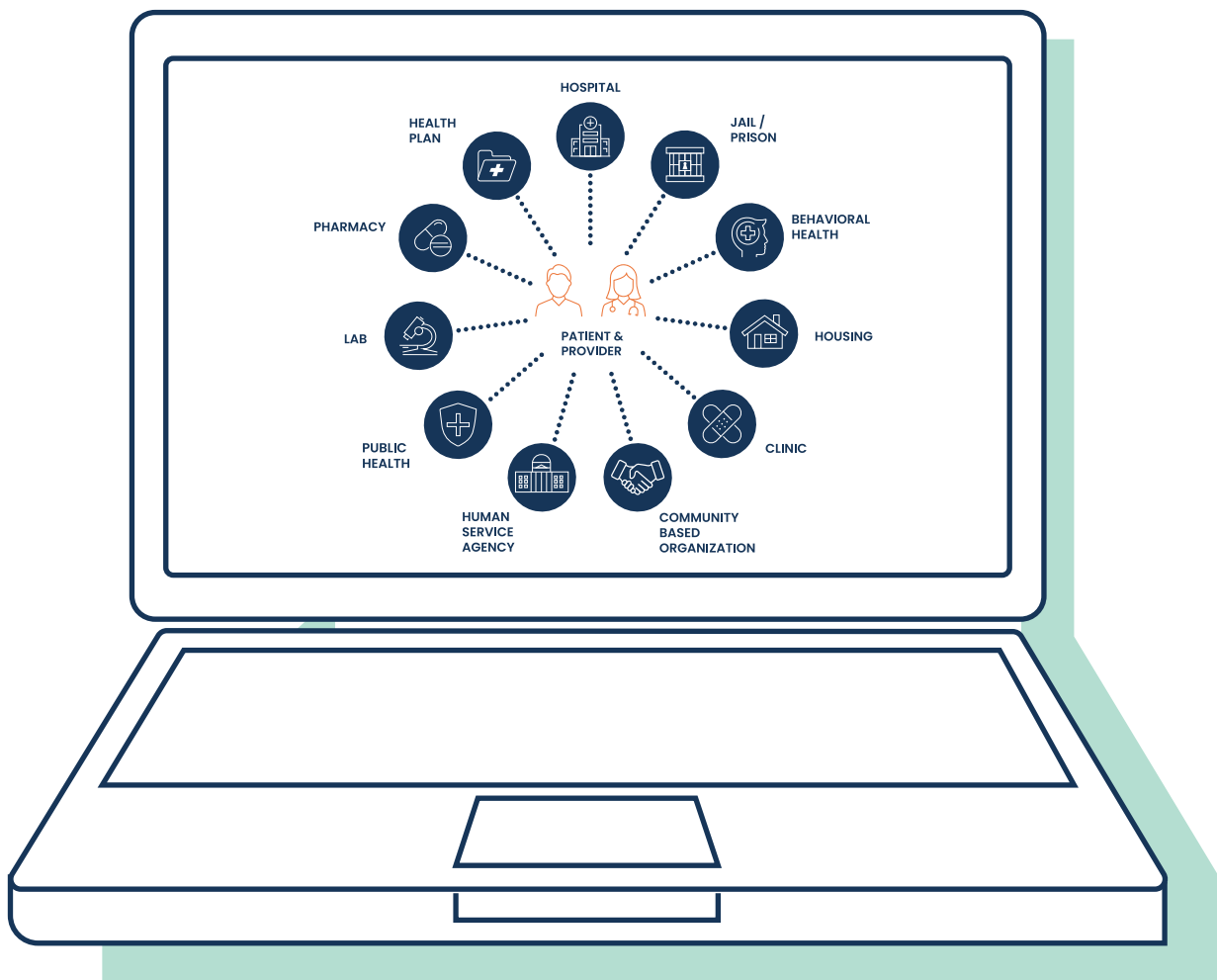
Steps 1-4 of this toolkit are designed to walk an organization step by step through the process for understanding and signing the Data Exchange Framework (DxF) Data Sharing Agreement (DSA). Signing the DSA is the first step of the DxF implementation process. Once an organization has signed the DSA, they'll need to work on implementing data sharing practices under the DxF. Steps 5-8 of the toolkit walk through key implementation steps, including altering organizational policies and procedures to align with the DxF and modifying technical systems to securely share appropriate data across entities.

Each section of the toolkit provides activities your organization will need to undertake; questions to pose to those in your organization responsible for data sharing, from a legal, operational, and technical perspective; and exercises designed to assess your readiness for DxF implementation, examine the DxF's impact on internal operations and technical exchange requirements, and explore available technology and mechanisms to securely and appropriately exchange information under the DxF.



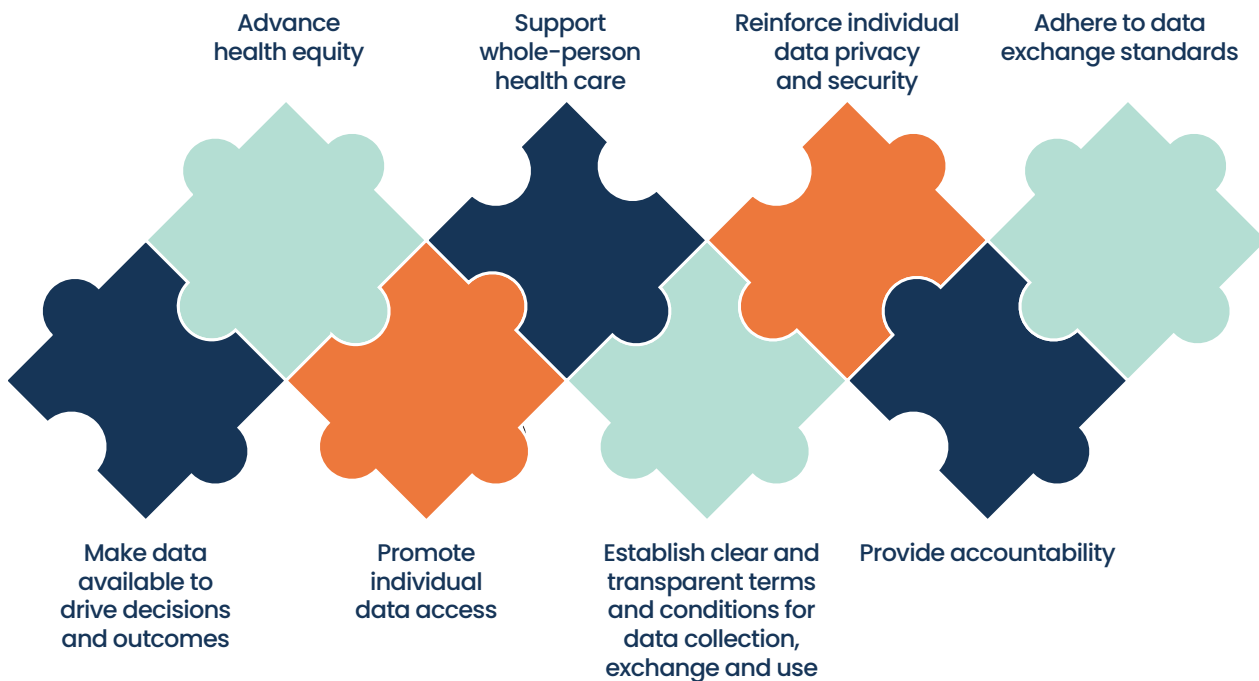
Overview

California's Data Exchange Framework is the first-ever statewide data-sharing agreement. It is intended to facilitate the secure and appropriate exchange of health and social service information (HSSI), giving providers a clear understanding of a patient's full health history, and the information needed to provide safe, effective whole-person care.



The DxF is technology agnostic. It does not require providers to use a certain technology, but rather, provides the rules of the road for bringing existing standalone health systems, providers and social services together to seamlessly provide better care and outcomes for all Californians. The DxF was developed with the following principles in mind:

DxF Principles:



Step 1:

Understand the DxF



Activity:

Understand the DxF and educate others in your organization about it. This can be achieved in a variety of ways, including meeting with key decision makers.

Actions to Take:

- Learn About the DxF

What is the DxF?

The DxF is the first-ever, required statewide data sharing agreement of its kind in California and key to achieving the state's plans for transforming healthcare. It 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.

Key Terms Defined

Data Sharing Agreement (DSA):

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

Policies & Procedures (P&Ps):

The rules and guidance to support on-the-ground implementation. P&Ps contain detailed implementation requirements. They will evolve and be refined over time through a stakeholder process.

Where possible, the DSA and P&Ps were developed to align with and build upon existing state and federal data exchange laws, regulations and initiatives, such as HIPAA, TEFCOA, and CalDURSA. (See Definitions for more about these laws.)



What kind of data is shared under the DxF and DSA?

The DxF mandates that participants share Health and Social Services information (HSSI). This includes:

- Information related to the provision of health care services, including but not limited to Protected Health Information (PHI)
- Information related to the provision of social services.

Health and Social Services information may include PHI, Personally Identifiable Information (PII), and digital identities.

Amidst ongoing legal developments related to reproductive health care and gender-affirming care, increased attention to ensuring the privacy of sensitive health information is critical. Organizations should note that laws, rules, and regulatory guidance are subject to change.

What are the DxF Policies & Procedures (P&Ps)?

CDII has released 13 P&Ps to date. Many of them will require organizations to review and align their own internal P&Ps to the DxF P&Ps. In later sections of the toolkit, we review the P&Ps in more detail. To review all 13 P&Ps, see the CDII website.

Determine if your organization is a HIPAA Covered Entity or a Business Associate of a Covered Entity

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

You will need to look at your organizational P&Ps and ensure they align with the DxF P&Ps. If you aren't sure if your organization is a HIPAA Covered Entity or Business Associate, use the Office of Civil Rights (OCR) Covered Entity Decision Tool or OCR Business Associate Guidance.

Step 2:

Check if You're a Required Signatory



Activity:

First, understand the difference between required and voluntary signatories and their DxF compliance dates, then determine your organization's signatory type.

Actions to Take:

□ Understand the Differences between Required vs. Voluntary Signatories

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 or more)
- **Skilled nursing facilities that currently maintain electronic records or electronic health information**
- **Health care service plans and disability insurers**
- **Clinical laboratories regulated by California Department of Public Health**

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 less than 25 physicians)
- **Some types of small hospitals** (For more information, visit DxF FAQ resource here)
- **Nonprofit clinics** with less than 10 providers

Not required to sign, but if they do, are **required to begin exchanging information** or provide access by January 31, 2026

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



Is your Organization a Voluntary Signatory?

If you are part of a governmental or social services organization, such as a county public health department or CBO, you are not currently required to sign the DSA, but may choose to do so. If you do decide to sign the DSA, then you need to take steps to implement data sharing practices and be ready to start exchanging data by January 31, 2026.

Have you already signed the DSA?

- If you aren't sure whether your organization has signed the DSA, CDII keeps a list that is frequently updated. Check here to see if you've already signed. If so, you can skip Steps 3 and 4 and move on to Step 5: Plan for Implementation.

Step 3:

Talk to Leadership



Activity:

Convene key people in your organization who will be involved in determining whether your organization needs to sign the DSA and the date by which you are required to sign. Educate and share information about why signing and sharing data is important, and how it impacts your organization.

Actions to Take:

- Determine who needs to get involved.** Depending on the size of your organization, some or all of the following may need to be involved:
 - Chief Executive Officer
 - Chief Information Officer
 - Chief Operating Officer
 - Attorney
 - Privacy Officer
 - IT Manager
 - Compliance Officer
 - Operational staff who manage internal P&Ps

- Determine how signing the DSA impacts data sharing agreements and contracts.**

Answer the following questions:

- **Do you have a parent entity?** If so, the parent entity will need to sign the DSA.
- **Do you have subordinate entities?** If you are the parent entity, you will need to sign the DSA on behalf of subordinate entities.
- **Who can legally bind the organization?** Only the person who can legally bind the organization contractually can sign the DSA.

Step 4:

Sign the DSA



Activity:

Gather needed materials and important pieces of information and sign the DSA.

Actions to Take:

- Know the type of Signatory you are (Required vs. Voluntary) and your compliance date.** If you are an entity that's required to exchange data by 2024, make sure you have signed the DSA by then. If you don't need to exchange data until 2026, you have more time. But implementing DxP data sharing practices will take time, so don't wait too long! Read the next steps in the toolkit to see what it takes to implement.
- Review the DSA.** Your attorney, compliance officer, and others should read the DSA to know to what you are committing your organization. You can read the full legal contract [here](#).
- Decide who in the organization is authorized to sign the DSA.** Who is authorized in the organization to sign contracts? This is the person who should sign the DSA.
- Decide if you are a single organization.** All locations or entities must be under a single EIN or California License from CDPH, DMHC, DHCS, or CDI.
- Decide what facilities or subordinate entities are to be included.** A Signatory may sign on behalf of multiple facilities or subordinate entities if authorized. 'Subordinate' means under the Signatory's umbrella, and this does not necessarily signify a hierarchical relationship.
- Gather Information about the organization & entities.** California state license number (or EIN for physician organizations and medical groups) will need to be listed on the DSA prior to signing.



Actions to Take (Cont.) :

- Log into the CalHHS DxP Data Sharing Agreement Signing Portal, create an account, and register your organization.**
- Send the DSA to the Signatory for signature through the portal.** If you need to later amend the DSA or need to add an additional subordinate organization, you can make changes and resend to the signatory for signature.
- Receive funding assistance to aid in making changes required for implementation.** This could be a DSA Signatory Grant or another funding opportunity (see Step 6 for more information).
- Begin exchanging data** (see Steps 5 through 8 of the toolkit).

Step 5:

Plan for Implementation



Activity:

Figure out what changes are needed internally for your organization to meet DSA requirements and exchange data, including changes to policies & procedures, technology, and workflows. We'll break these down into three parts below.

Actions to Take:



Part 1: Plan for Organizational Policies & Procedure Changes. Analyze your current data sharing policies and procedures (P&Ps), as well as data use agreements, for any needed updates to ensure they align with the DSA.

Many payors require providers to have policies & procedures in place that govern breach protocols, permitted, required and prohibited uses of the data, and privacy and security. If you're a HIPAA Covered Entity or Business Associate, you should have P&Ps on these topics already established.

- In particular, you'll want to review the following DxF P&Ps against your organization's internal P&Ps to ensure alignment:
 - **Permitted, Required and Prohibited Purposes** – sets forth the purposes for which Participants may, or are required to, exchange health and social services information (HSSI) and certain restrictions on the use of HSSI obtained through the DxF.
 - **Breach Notification** – describes the procedure that Participants must follow in the event of a breach of information.
 - **Privacy and Security Safeguards** – requires Participants to use appropriate safeguards to protect the privacy of protected health information (PHI) or personally identifiable information (PII).
 - **California Information Blocking Prohibitions** – aligns the DxF with applicable law that facilitates the timely access, exchange, and use of HSSI.

See the Appendix on DxF Policies & Procedures for information about each of these P&Ps.



Actions to Take (Cont.) :

- As you are reviewing your organization's P&Ps against the DxF P&Ps, answer the questions below. You may want to tear out the Appendix on DxF P&Ps, so you can review them as you answer these questions.
- Once you've reviewed the P&Ps and identified changes that need to be made, you'll want to make those changes. You may also want to consult legal counsel.

Questions to Ask on Breach Notification P&P:

1. Does your organization have a breach notification P&P?
 - Yes
 - No
2. Is your organization subject to HIPAA? (If you aren't sure if your organization is a HIPAA Covered Entity or Business Associate use the OCR Covered Entity Decision Tool or OCR Business Associate Guidance.)
 - 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



Questions to Ask on Privacy and Security P&P:

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



Questions to Ask on Information Blocking P&P:

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



Part 2: Technology & Workflow Changes. Assess your data infrastructure needs and current workflows to identify technology changes needed for your organization to meet DxF requirements. You'll need to consider your entire data infrastructure, including electronic health record (EHR), referral management systems, and whether you'll need to connect to Qualified Health Information Organization (QHIO) management systems, and whether and how to connect to a QHIO.

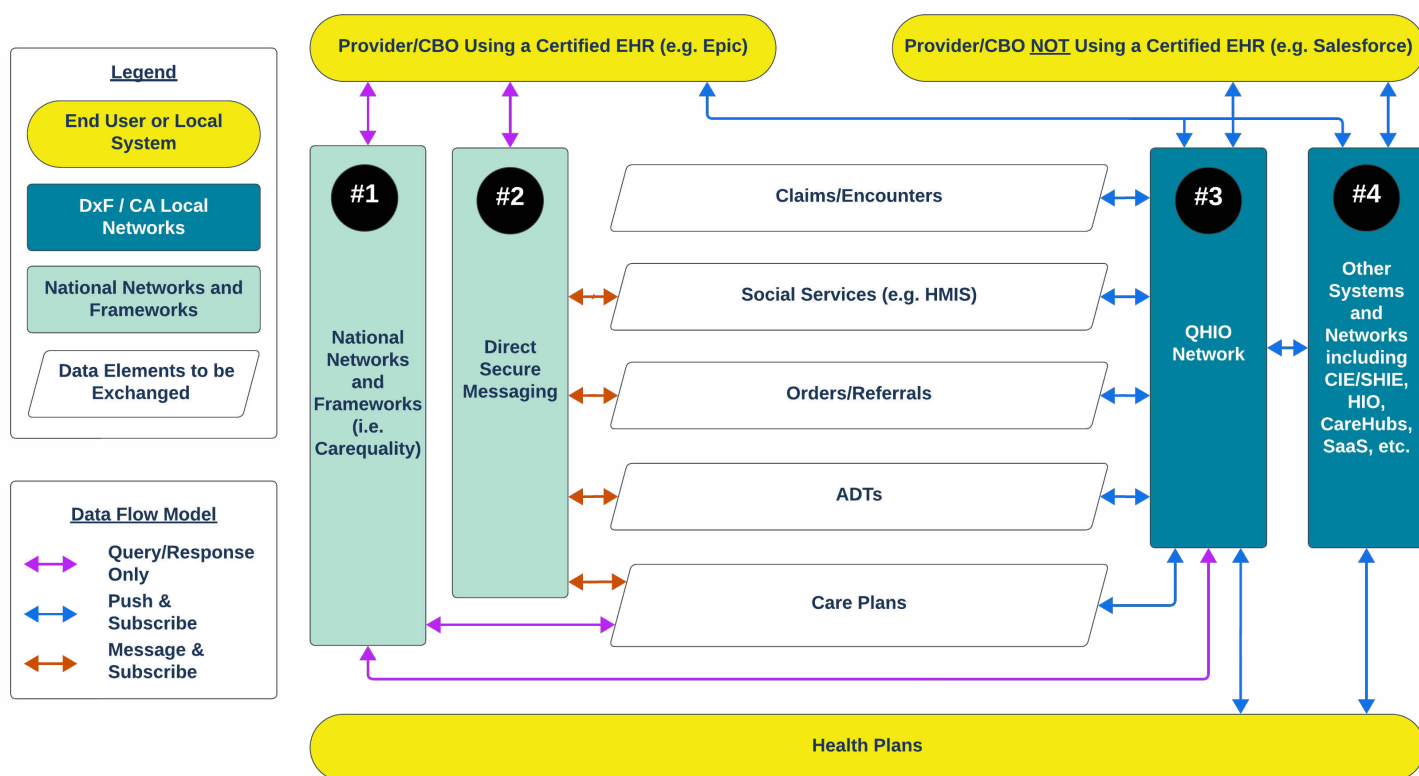
- Types of Data to Be Exchanged:** The DxF requires specific types of data to be exchanged. There are several P&Ps related to technical exchange requirements that your organization should review, including:
 - **Requirements to exchange HSSI** – sets forth Participants' responsibilities to respond to requests for health and social services information, and to exchange these data.
 - **Data elements to be exchanged** – describes the information that Participants must make available or exchange, including all electronic health information defined in the federal information blocking rules.



- **Technical requirements for exchange** – describes data exchange under the DxF and the exchange of data that participants must support, including requests for information, information delivery, ADT event notifications, and person matching.
- **Individual access services** – requires DxF Participants to provide individuals with access to their personal health information and personally identifiable information.

See the Appendix on DxF Policies and Procedures (P&Ps) for more information about each of these.

- **How to Share Data Under the DxF.** In general, there are four ways to achieve interoperability or data exchange, depending on whether you are using a certified EHR as your record keeping system. See the table “Ways to Exchange Data” (page 17) for more about the different options for sharing data, as well as the Further Information on Data Exchange Appendix for more on data sharing methods.





- Depending on organization type, data elements maintained, and EHR/record-keeping platform, entities can engage in data exchange through one or multiple options. These include:
 1. National Networks and Frameworks
 2. Direct Secure Messaging
 3. Qualified Health Information Organizations (QHIO)
 4. Other Systems, including Community Information Exchange (CIE), Health Information Organization (HIO), Software as a Service (SaaS), CareHub, etc.
- If you are an entity with a certified EHR, you can achieve interoperability and exchange data through mechanisms 1 through 4.
- If you are an entity NOT using a certified EHR, your route to interoperability is mechanisms 3 or 4, through QHIOs or other state/regional exchanges.

Consideration on How to Share Data Under the DxF:

Many DxF participants will need to employ multiple methods listed here to securely exchange data.



Ways to Exchange Data

Network / System	Capabilities	Examples	Limitations
National Networks and Frameworks	<ul style="list-style-type: none"> • Access to clinical records in external systems • Centered on certified EHRs 	<ul style="list-style-type: none"> • Carequality • CommonWell Health Alliance • eHealth Exchange • TEFCA (not yet live) 	<ul style="list-style-type: none"> • Limited to CCDAs at this time; no ADT, claims, social services data • Largely limited to treatment purposes
Direct Secure Messaging	<ul style="list-style-type: none"> • Enables a push mechanism (sender-initiated) for exchanging encrypted health information among clinicians, patients, and organizations via the Internet 	<ul style="list-style-type: none"> • DirectTrust 	<ul style="list-style-type: none"> • Data integrity issues • Lack of standardization or message handling • May increase clinician burden with more manual processes
QHIOs	<ul style="list-style-type: none"> • Aggregation of health and social services information across participants • Centered on all DSA Signatories 	<ul style="list-style-type: none"> • Cozeva • Health Gorilla, Inc. • LANES • Long Health, Inc. • Manifest Medex • Orange County Partners in Health HIE • Sac Valley MedShare • San Diego Health Connect • Serving Communities HIO 	<ul style="list-style-type: none"> • DSA P&Ps largely focused on health care organizations; additional guidance needed
Other HIOs and CIE/SHIEs	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Alameda SHIE • Epic Care Everywhere • 2-1-1 San Diego CIE 	<ul style="list-style-type: none"> • Often limited to use of vendor solution/specific community • Only CIEs typically contain social service data
Certified EHR	<ul style="list-style-type: none"> • An electronic system that meets certain criteria, with ability to build and maintain a longitudinal patient record 	<ul style="list-style-type: none"> • EPIC • Cerner • NextGen • Allscripts • Other C-EHRs 	<ul style="list-style-type: none"> • Variability of national network standards used



What is a QHIO and Do You Need One?

- A QHIO is a DxF designated intermediary that facilitates the secure exchange of health and social services information, helping DxF Participants meet the data sharing requirements of the DSA.
- To participate in the DxF, Signatories must be able to send and receive HSSI, locate a patient record based on person attributes, format HSSI to conform with DxF standards, meet privacy and security requirements, and more.
- For many Participants, these are not current capabilities, and they may choose to seek the services of an Intermediary to help manage the exchange. QHIOs are Intermediaries that CDII has determined meet certain requirements that may ease the selection of an Intermediary for some Participants.
- Participants are not required to use a QHIO — however, a QHIO is a vetted source that can assist a Participant to meet the requirements of the DSA.
- If you are not sure how to exchange health and social services information with other DxF Participants, you may benefit from the services of a QHIO. Reach out to CDII, California Association of Health Information Exchanges (CAHIE) or Connecting for Better Health.
- QHIOs may also have additional workflows and information that you may want to access – consider talking to your QHIOs to learn what additional locale functionality may be available to you.



Questions to Ask on Technology and Workflow Changes :

1. What system(s) are you using to collect HSSI?
2. What data is collected?
3. How are you Exchanging (sending and receiving) different types of HSSI?
 - Claims :
 - Encounters :
 - CCD :
 - Other :
4. Do you have a Certified EHR (C-EHR)? This will determine what path you can take for sharing data. Use the following link to find out if you have a C-EHR:
<https://chpl.healthit.gov/#/search>
 - Yes
 - No
5. If you are connected to a national network or framework, is there additional HSSI required to exchange under the DxF? Do you need to consider another solution, such as a QHIO?
6. Do you plan to link to and exchange data through a QHIO? if so , which one?
 - Cozeva
 - Health Gorilla, Inc.
 - Long Health, Inc.
 - Los Angeles Network for Enhanced Services (LANES)
 - Manifest MedEx
 - Orange County Partners in Health HIE
 - SacValley Medshare
 - San Diego Health Connect
 - Serving Communities HIO



Part 3: Understanding Your Environment and Partners. Connect with your trading partners that you work with regularly to understand if they've signed the DSA, how your organizations share data with each other, and to identify how data sharing works in your local community. A trading partner is a health or social services-related entity with which my organization shares or receives data from management systems, and whether and how to connect to a QHIO.

- **Map out your trading partners and what each one is using to exchange data or how they will exchange data under the DxF.** If you have many trading partners, we recommend starting out by mapping out your top three partners. Find out if they plan to use a specific QHIO: will it impact a shared workflow, and will you need to make changes as a result?
 - Complete the exercise on page 22 to map out your trading partners.
- **Identify knowledge gaps.** Are you unable to answer these questions about certain partners?
- **Talk to your partners where these knowledge gaps exist.** Reach out to them directly or through a local collaborative.



Questions to Ask on Understanding Your Environment and Partners:

1. With whom do you share data?
 - Health plan :
 - Hospital :
 - Other provider :
 - CBO :
 - Other :

2. What data would you like to be receiving, and from whom?

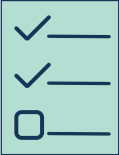
3. What data would you like to be sending, and to whom?

4. What mechanisms are available to receive or send such data?

5. 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:

6. Will you take advantage of or participate in these resources? What specific issues related to these resources do you need more information on to make an informed decision?
 - Onboarding process
 - Workflow
 - Data governance
 - Cost
 - Availability
 - Other

7. What other resources not mentioned here are required for your community to meet your DSA needs?

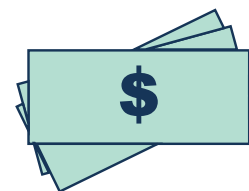


Exercise: Map Your Trading Partners

Partner Name	Are they exchanging data electronically? If yes, how?	Type of Data Exchange	Are they part of a QHIO? Which one?	Are you in a shared workflow that will be impacted?	What changes are needed? Technology, P&P, training
Example: Hospital XYZ	Commonwell/ Carequality	Discharge Data- CCD	LANES		

Step 6:

Apply for Funding Opportunities



Activity:

There may be funding opportunities available to support data sharing and DxF implementation.

Actions to Take:

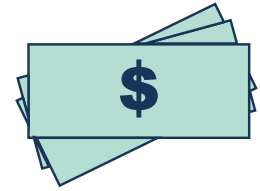
The DxF provides the rules of the road to bring existing standalone health systems, providers, and social services together to seamlessly provide better care and outcomes for all Californians.

- **Check What Funding Opportunities are Available to You Now.** There are a number of time-limited funding options available to you to support your ability to implement the DxF. You may also consider whether funding opportunities may be combined or braided together. Funding may include:
 - DSA Signatory Grants
 - Providing Access and Transforming Health (PATH)
 - Incentive Payment Program (IPP)
 - Equity & Practice Transformation (EPT) Payments Program
 - CalAIM Behavioral Health Quality Improvement Program (BH-QIP)

More Information on Possible Funding Opportunities

1. DSA Signatory Grants

- These grants provide direct support to entities that have signed the DSA to subsidize their implementation efforts and implement a range of activities to achieve real-time data exchange according to the DxF. For more information about the 2023 DSA Signatory Grants, see our Appendix on DSA Signatory Grants (pages 53 -55)
- **Timeline:** Grants are available in 2023 through three funding rounds. Whether funding will be available in 2024 is unknown at the date of this publication.
- **DSA Signatory Grant Resources:** CDII webpage



2. Providing Access and Transforming Health (PATH)

- **PATH** is a five-year, \$1.85 billion initiative to build up the capacity and infrastructure of on-the-ground partners to successfully participate in Enhanced Care Management (ECM), Community Supports, and the Justice-Involved Initiative. Two of the PATH funding streams could offer funding to support DxF implementation if entities are also implementing ECM and Community Supports. These are:
 - **Funding Opportunity 1: Capacity and Infrastructure Transition, Expansion and Development (CITED) Grants**
 - CITED grant funding enables the transition, expansion, and development of Enhanced Care Management and Community Supports capacity and infrastructure.
 - Allowable uses could include modifying, purchasing and/or developing the necessary clinical, referral, billing, data reporting or other infrastructure and IT systems, to support integration into CalAIM, including IT/data systems, hardware and equipment software, implementation support, or planning.
 - **Timeline:** Grants are available 2023–2026. Round 3 should open in early 2024.
 - **Resources:** PATH CITED webpage
 - **Funding Opportunity 2: Technical Assistance (TA) Marketplace Grants**
 - Provides no-cost TA resources to providers, counties, hospitals, CBOs and others.
 - **Timeline:** Technical assistance available 2023–2026.
 - **Resources:** PATH TA Marketplace webpage

3. Incentive Payment Program

- Medi-Cal Managed Care Plans (MCPs) receive state funding to pass on to providers to support the implementation and expansion of Enhanced Care Management and Community Supports.
- **Timeline:** 2022–2024
- **Resources:** DHCS IPP webpage; reach out to your county MCPs for additional information, including how to apply for time-limited funding.



4. Equity and Practice Transformation (EPT) Payments Program

- Payments to primary care providers to transform their practices to advance health equity and reduce disparities by investing in upstream care models and partnerships to address health and fund practice transformation. Three components:
 - **Initial Planning Incentive Payments to small and medium sized independent practices:** \$25 million over one year. Practices chosen by Medi-Cal Managed Care Plans.
 - **Provider Directed Payment Program:** \$650 million over five years to primary care practices of any size or setting. Applications due Fall 2023 and first cohort will begin in January 2024.
 - **Statewide Learning Collaborative:** \$25 million to run collaborative for practices participating in the Provider Directed Payment Program.
- **Timeline:** 2023-2028
- **Resources:** EPT Payments Program webpage

5. CalAIM Behavioral Health Quality Improvement Program (BH-QIP)

- Incentive payment program to support Mental Health Plans, Drug Medi-Cal State Plans and Drug Medi-Cal Organized Delivery Systems (also known as County Behavioral Health Plans) as they prepare for CalAIM. Each County Behavioral Health Plan can earn incentive payments in the CalAIM BH-QIP by completing deliverables tied to program milestones. Funds may be used for staffing, technology and infrastructure, contracting, training, and/or technical assistance.
- **Timeline:** 2021-2024
- **Resources:** DHCS BH-QIP webpage

Step 7:

Make Internal Changes Needed to Exchange Data

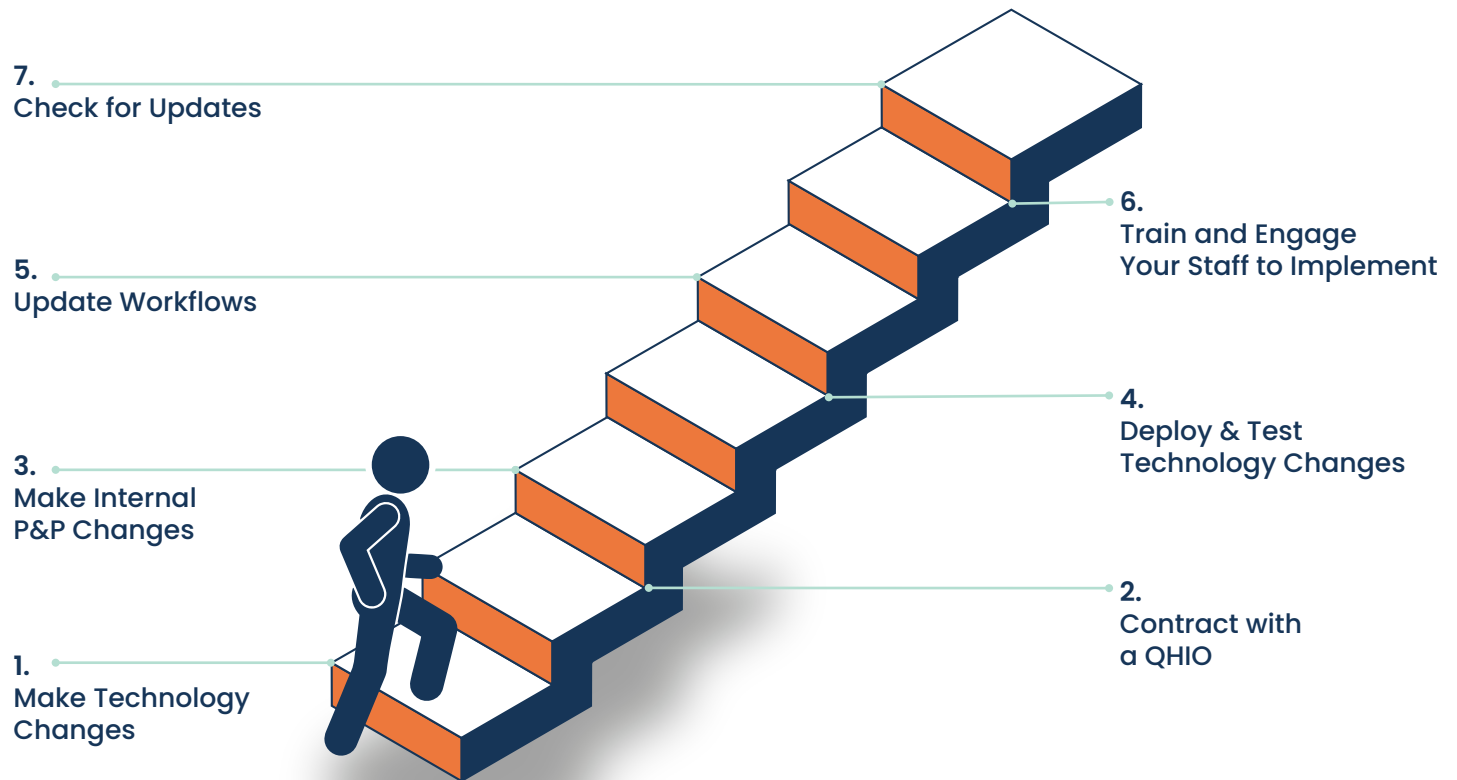


Activity:

Based on the information gathered and analyzed in Step 5, all the internal organizational changes needed to implement the DxF should have been identified. You may need to hire or contract with vendors and with a QHIO to start exchanging data in 2024. You will also need to deploy and test any technological changes, update workflows, and train your staff on changes affecting operations or workflow.

Actions to Take:

- 1: Make Technology Changes.** Make the technology changes your organization identified in Step 5.
- 2: Contract with a QHIO if Needed.** There may be funding identified in Step 6 to assist with the associated costs.
- 3: Make Internal P&P Changes.** Make changes to your organizational policies and procedures identified in Step 5 in order to align with the DxF.
- 4: Deploy & Test Technology Changes.**
- 5: Update Workflows.** Make updates to your workflows based on the changes you need to make or the changes your partners are making.
- 6: Train and Engage Your Staff.** Make sure your staff is knowledgeable and up to date on the changes.
- 7: Check for Updates.** CDII is updating the DxF P&Ps on an ongoing basis. As new P&Ps are established and implemented, or existing P&Ps are updated, your organization will also need to review these documents and continue to update your P&Ps on an ongoing basis. To support these types of activities, consider joining a coalition such as Connecting for Better Health or a regional CalAIM PATH Collaborative that will provide updates when new P&Ps go into effect or changes are made.



Step 8:

Exchange Data in 2024

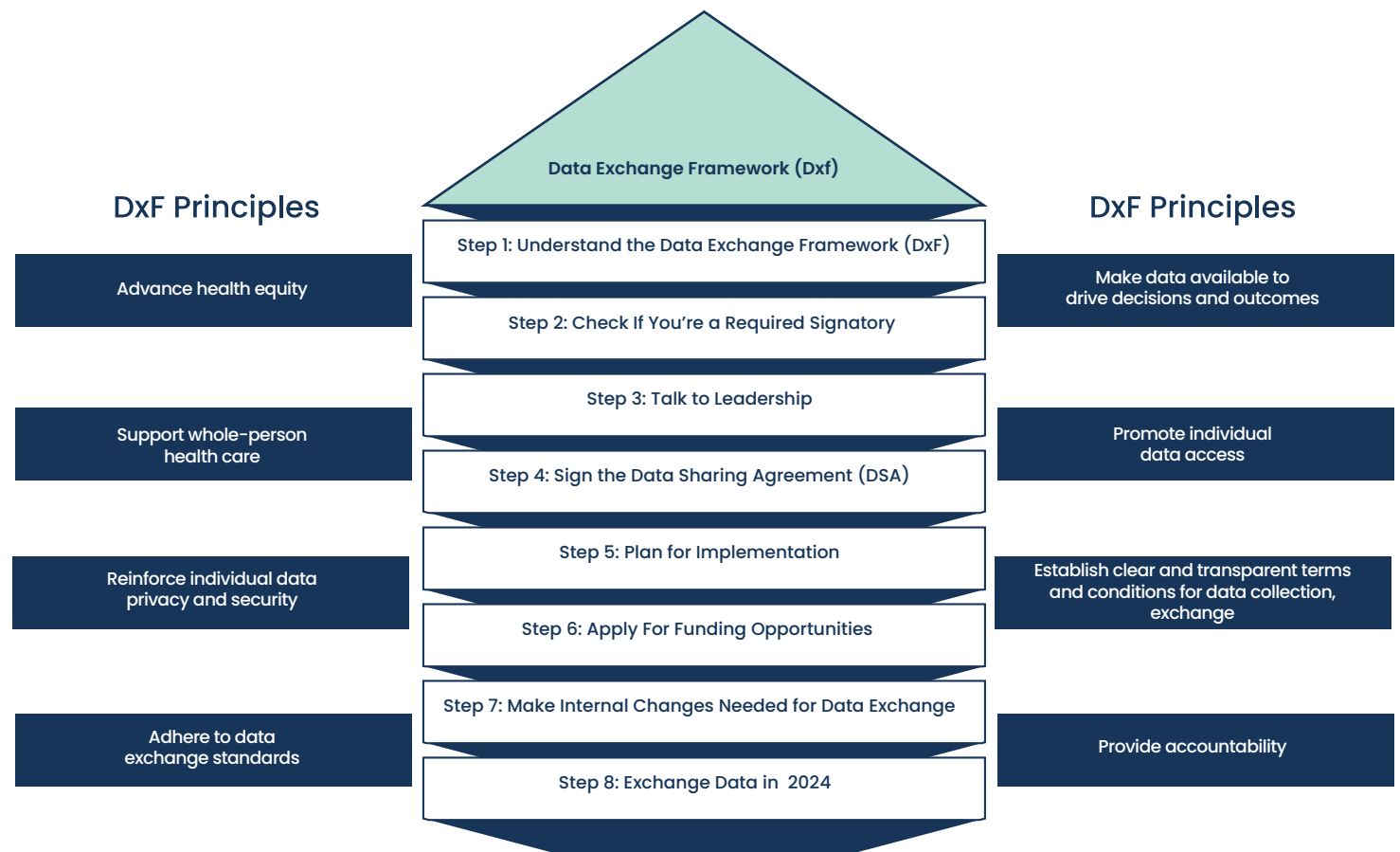


Activity:

Successfully exchange data beginning in 2024.

Reminder:

While most health care entities will need to start exchanging data by January 31, 2024, some entities, such as physician practices of fewer than 25 physicians, or voluntary signatories, including social service organizations and counties, will have until January 31, 2026 to begin exchanging data. For the full list of required and voluntary Signatories, see Step 2 on page 6.



DxF Implementation and Achieving Successful Data Exchange

Definitions

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

Application Programming Interfaces (APIs): APIs are messengers or translators that work behind the scenes to help software programs communicate with one another.

(Certified) Electronic Health Record (EHR): EHRs are electronic versions of a patient's medical history that are maintained over time. These records may include demographics, progress notes, past medical history, immunizations, etc.

Care Management Platforms: Care Management Platforms are documentation and record-keeping platforms used by social service agencies.

CaIDURSA: The California Data Use and Reciprocal Support Agreement (CaIDURSA) is a multi-party data sharing agreement that establishes common policies, procedures, and operational practices necessary for trusted statewide health information sharing in California. It is the basis for the California Trusted Exchange Network (CTEN).

Community Information Exchange (CIE): A network of collaborative partners using a multidirectional technology platform to connect people to the services and supports they need. Partners may include human and social service, healthcare, and other organizations.

Data Aggregation: Data aggregation is the process of combining information from multiple systems to produce interconnective, shareable information.

Data Exchange Framework (DxF): A set of rules and policies that govern the secure and appropriate exchange of HSSI data in California and make this exchange mandatory between certain signatories. It is not a singular technology system, nor is it a singular repository for data.

Data Sharing Agreement (DSA): The DSA is a legal agreement that a broad spectrum of health organizations will be required to execute by January 31, 2023, with required data sharing beginning January 31, 2024, or January 31, 2026, depending on participant type. This sets forth a common set of terms, conditions, and obligations to support secure, real-time access to, or exchange of, health and social services information between and among participants.

DSA Policies and Procedures (P&Ps): The terms and conditions of the DSA that operationalize the DxF.

DSA Signatory Grants: Grants available to support capacity and infrastructure building needed to support successful data sharing in California. These include Qualified Health Information Organization (QHIO) Onboarding Grants and Technical Assistance (TA) Grants.

Extract, Transform, and Load (ETL) systems: A process that extracts, transforms, and loads data from multiple sources to a data warehouse or other unified data repository.

FHIR: Fast Healthcare Interoperability Resources (FHIR): A standard that defines how healthcare information can be exchanged between different computer systems regardless of how it is stored in those systems.

Health Information Exchange (HIE): A system that allows the mobilization and exchange of health care data electronically across organizations within a region, community, or delivery system. HIEs provide the capability to move clinical information among different health care information systems electronically. HIEs are both a function and an entity type that provides this service. HIE organizations may also be called an HIO, HIN, QHIN.

Health Information Organization (HIO): An organization that offers services and functions to support the exchange of health and social services information. HIOs serve as an intermediary to support health and human service organizations as they send information or initiate/receive/reply to requests for information.

Health and Social Services Information (HSSI): Any and all individually identifiable information received, stored, processed, generated, used, transferred, disclosed, made accessible, or shared under 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.

HIPAA: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge.

Interoperability: The ability of different entities to communicate and exchange information. Currently, separate organizations utilize separate systems, and data is not easily shared across these systems.

Information Blocking: Business, technical, and organizational practices that prevent or materially discourage the access, exchange or use of electronic health information (EHI) when these practices are likely to interfere with access, exchange, or use of EHI. If conducted by a health care provider, there must also be knowledge that such practice is unreasonable and likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

Message-Subscribe: A data exchange method; 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.

Nationwide Network or Framework: Any vendor-agnostic health information network or health information exchange framework with nationwide scope, including coverage in California, available to some or all Participants for the exchange of Health and Social Services Information that may or may not have signed the DSA. Some examples include eHealth Exchange, CommonWell Health Alliance, Carequality, DirectTrust, or Trusted Exchange Framework.

Participant(s): An organization that is a Signatory to the Data Sharing Agreement, including any identified subordinate entities of that Signatory.

Personal Health Information (PHI): Any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

Population Health Management (PHM): Under the umbrella of CalAIM, PHM is designed to proactively assess and address the care needs of beneficiaries with tailored interventions that ensure access to a whole-system, person-centered program. Plans are expected to be responsible for more than 90% of Medi-Cal beneficiaries by this year (2023).

Push-Subscribe: A data exchange method; communication or information exchange that occurs proactively for a provider's patients based on an established roster of information to be shared when a patient event occurs.

Qualified Health Information Organization (QHIO): A state-designated data exchange Intermediary that facilitates the exchange of Health and Social Services Information between Participants.

Query-Response: A data exchange method; 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.

Referral management systems: A tool that allows providers to transmit a patient's data across their care team simultaneously. They typically include clinical and community resource referrals and aim to track, act on referrals, and facilitate closed-loop communication, to the extent possible, between all provider types (e.g., MCPs, physicians, case managers, social workers, nurses, caregivers, and community-based providers).

Registries: Organized systems that use observational study methods to collect uniform data (clinical and other) to evaluate specified outcomes for a population defined by a particular disease, condition, or exposure and serve a predetermined scientific, clinical, or policy purpose(s).

Signatories: Also referred to as DSA Participants or Entities, 'Signatories' are entities or participants that sign the DSA.

Trusted Exchange Framework and Common Agreement (TEFCA): Establishes a universal floor of interoperability, connecting providers, public health entities and individuals across the U.S. healthcare system.

Resource List

California State Government DxF Guidance & Legal Resources

CalHHS DxF Guiding Principles (CDII)
Data Exchange Framework FAQ (CDII)
DxF Single Data Sharing Agreement (CHHS)
Policies and Procedures of DSA (CDII)
DxF Glossary

General Resources on DxF or Data Sharing

CA DxF 101 Fact Sheet (ITUP)
DxF Education: Data Exchange Framework Information Hub (Connecting for Better Health) HIE Fact Sheet (ITUP)

DxF Grants/Funding Resources

DxF Grant Program Overview Document (CDII)
DSA Signatory Grants 101 (CDII)
DSA Signatory Grant Guidance Document (CDII)
DSA Signatory Application Template (CDII)
Webinar: DxF Grant Program Overview & DSA Signature Portal Demonstration
Webinar: Applying for DxF Grants & DxF Program Updates (CDII)
Webinar: DSA Signatory Grants Town Hall (CDII)
Factsheet: Understanding the Funding Opportunities to Support DSA Signatories (Connecting for Better Health)

Signing the DSA

DSA Signing Portal and User Instructions to Sign DSA (CDII)
Webinar: What is a QHIO? How do I sign the DSA? (CDII)
Webinar: DxF DSA Signing Portal Townhall (CDII)

Policies & Procedures

Webinar: The DxF DSA and Policies and Procedures: An Overview (CDII)
Factsheet on Data Sharing Agreement & Policies & Procedures (Connecting for Better Health)
Video Explainer on Breach Notification P&P (DxF Multi-Association Ed. Initiative) Video Explainer on Permitted, Required and Prohibited Purposes P&P (DxF Multi-Association Education Initiative)
Video Explainer on Privacy and Security Safeguards P&P (DxF Multi-Association Ed. Initiative)
Video Explainer on Individual Access Services (DxF Multi-Association Ed. Initiative) Explainer on Technical Requirements for Exchange (DxF Multi-Association Ed. Initiative) Video Explainer on California Information Blocking Prohibitions (DxF Multi-Association Ed. Initiative)

DxF Policies and Procedures

How to use this section:

As you assess your own internal P&Ps against the DxF P&Ps, use the “Notes” section to take notes on what changes your organization needs to make to align with the DxF.

Please note: CDII is continuing to release revisions to DxF P&Ps, as well as new P&Ps. This content is up to date as of December 1, 2023. For updated information on DxF P&Ps, please refer to CDII’s website. Terms used in the P&Ps are defined in CDII’s DxF Glossary

P&P: Permitted, Required, and Prohibited Purposes		
PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>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.</p>	<p>Required Purposes:</p> <ul style="list-style-type: none"> DxF Participants <u>must</u> exchange and provide access to HSSI for Treatment, Payment, Health Care Operations and Public Health Activities. <p>Permitted and Prohibited Purposes:</p> <ul style="list-style-type: none"> 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 lawful purpose. Participants are prohibited from using HSSI to sell or to take adverse action against an individual (e.g., limit access to medical services or discriminate). <p>Fees:</p> <ul style="list-style-type: none"> Participants are 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 through the QHIO. 	<p>Required Purposes:</p> <ul style="list-style-type: none"> 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.

P&P: Permitted, Required, and Prohibited Purposes (cont.)

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>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.</p>	<p>Required Purposes:</p> <ul style="list-style-type: none"> DxF Participants <u>must</u> exchange and provide access to HSSI for Treatment, Payment, Health Care Operations and Public Health Activities. <p>Permitted and Prohibited Purposes:</p> <ul style="list-style-type: none"> 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 lawful purpose. Participants are prohibited from using HSSI to sell or to take adverse action against an individual (e.g., limit access to medical services or discriminate). <p>Fees:</p> <ul style="list-style-type: none"> Participants are 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 through the QHIO. 	<p>Permitted and Prohibited Purposes:</p> <ul style="list-style-type: none"> 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. <p>Fees:</p> <ul style="list-style-type: none"> 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.

NOTES:

P&P: Privacy and Security Safeguards

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>Describes privacy standards and security safeguards Participants must comply with in connection with the exchange of HSSI under the DSA.</p>	<ul style="list-style-type: none"> • 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): <ol style="list-style-type: none"> I. Non-Covered Entities' and Business Associates' privacy and security obligations; II. Standards for De-Identification under the DSA; III. Record retention requirements related to privacy and security trainings; and IV. Defined terms, including "Securely Destroy," "Loss," "Disruption," and "Destruction." 	<ul style="list-style-type: none"> • Reminds Participants of more stringent privacy laws beyond HIPAA and CMIA, including <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ▪ 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) • Privacy Requirements: • HIPAA Covered Entities, Business Associates and hybrid entities: <ul style="list-style-type: none"> ▪ Must comply with HIPAA as applicable, and all other Applicable Laws ▪ Need to review/update BAAs if conflict with DxP P&Ps

NOTES:

P&P: Privacy and Security Safeguards (cont.)

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>Describes privacy standards and security safeguards Participants must comply with in connection with the exchange of HSSI under the DSA.</p>		<ul style="list-style-type: none"> • Non-Covered Entities/Business Associates: <ul style="list-style-type: none"> ▪ With respect to PHI: <ul style="list-style-type: none"> ◦ 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)). ▪ With respect to PII: <ul style="list-style-type: none"> ◦ 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

NOTES:

P&P: Privacy and Security Safeguards (cont.)

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>Describes privacy standards and security safeguards Participants must comply with in connection with the exchange of HSSI under the DSA.</p>		<ul style="list-style-type: none"> ◦ Comply with HIPAA’s verification requirements (45 CFR section 165.514(h)) <p>Security Requirements:</p> <ul style="list-style-type: none"> ▪ HIPAA Covered Entities, Business Associates and hybrid entities: <ul style="list-style-type: none"> ◦ Must comply with HIPAA Security Rule, and all other Applicable Laws ◦ Need to review/update BAAs if conflict with DxP P&Ps ▪ Non-Covered Entities/Business Associates: <ul style="list-style-type: none"> ◦ 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>Secure Destruction:</p> <ul style="list-style-type: none"> ▪ 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).

NOTES:

P&P: Privacy and Security Safeguards (cont.)

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>Describes privacy standards and security safeguards Participants must comply with in connection with the exchange of HSSI under the DSA.</p>		<p>P&Ps; Trainings:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> ▪ Participants must properly train staff, contractors, agents, employees, and other workforce members before granting access to HSSI. <ul style="list-style-type: none"> ◦ Refresher trainings “no less than annually” ▪ Store records of trainings for at least 6 years.

NOTES:

P&P: California Information Blocking Prohibitions

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>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.</p>	<ul style="list-style-type: none"> • 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. • This policy has no impact on a Participant's obligation, if any, to comply with the Federal Information Blocking Regulations. • 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. <ul style="list-style-type: none"> ▪ Participants are deemed in compliance with the P&P if they comply with the Federal Information Blocking Regulations. <ul style="list-style-type: none"> ◦ 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. 	<ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> ▪ 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.

NOTES:

P&P: Breach Notifications

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>Set forth the procedure Participants must follow in the event of a "Breach."</p>	<ul style="list-style-type: none"> • Requires Participants to notify and provide written reports to "impacted" participants and the DxF Governance Entity of "Breaches." <ul style="list-style-type: none"> ▪ 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.). 	<ul style="list-style-type: none"> • Extends Participants' data breach reporting obligations beyond current requirements (e.g., HIPAA, Cal. Health & Safety Code, Section 1280.15, etc.). <ul style="list-style-type: none"> ▪ 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,...

NOTES:

P&P: Breach Notifications (cont.)

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>Set forth the procedure Participants must follow in the event of a “Breach”</p>	<ul style="list-style-type: none"> • Requires Participants to notify and provide written reports to “impacted” participants and the DxF Governance Entity of “Breaches.” <ul style="list-style-type: none"> ▪ 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.). 	<ul style="list-style-type: none"> ◦ ... 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.

NOTES:

P&P: Breach Notifications (cont.)

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
Set forth the procedure Participants must follow in the event of a "Breach"		<ul style="list-style-type: none">• 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.

NOTES:

P&P: Requirement to Exchange Health & Social Services Information (HSSI)

PURPOSE	OVERVIEW	
<p>Set forth Participants' responsibilities to respond to requests for HSSI, and to exchange HSSI.</p>	<ul style="list-style-type: none"> • All Participants must respond to requests for HSSI made by other Participants: <ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> • Imposes new requirement that all Participants respond to requests. <ul style="list-style-type: none"> ▪ 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.

NOTES:

P&P: Data Elements to Be Exchanged

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>Set forth the information that Participants must either make available or exchange.</p>	<ul style="list-style-type: none"> • 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— <ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> • Providers are 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. <ul style="list-style-type: none"> ▪ These requirements may differ from existing contributions made by these entities to HIEs today (e.g., CCDA, ADT and claims/encounter feeds).

NOTES:

P&P: Technical Requirements

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>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.</p>	<ul style="list-style-type: none"> • Key Terms: <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> ▪ 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 • Information Delivery: <ul style="list-style-type: none"> ▪ Governs the delivery of HSSI regarding a specific Individual to a specific Participant in conjunction with an Order or Referral. 	<ul style="list-style-type: none"> • Creates new legal obligation to adhere to technical requirements that otherwise don't exist in statute or regulation (exception for ADTs, see below). <ul style="list-style-type: none"> ▪ 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.

NOTES:

P&P: Technical Requirements (Cont.)

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>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.</p>	<ul style="list-style-type: none"> • Notification of Admit, Discharge, Transfer (ADT) Events: <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> ▪ 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. 	

NOTES:

P&P: Technical Requirements (cont.)

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>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.</p>	<ul style="list-style-type: none">• Person Matching:<ul style="list-style-type: none">▪ Sets out the process by which a Participant ensures that exchanged Health and Social Services Information is appropriately linked to the correct real person.	

NOTES:

Empty box for notes.

P&P: Individual Access Services

PURPOSE	OVERVIEW	IMPACT ON PARTICIPANTS
<p>To require Participants to provide individuals with access to their PHI or PII.</p>	<ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> ▪ 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 PII 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. 	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ▪ 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.

NOTES:

Further Information on Data Exchange

Methods	Definitions	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.	<p>Provider X requires a summary of care for 'new' Patient 1 to establish an understanding of their health history.</p> <p>Real-time access to data as needed and comprehensive access to information.</p>
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.	<p>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.</p> <p>Request and receive data as needed with known delay.</p>
Push - Subscribe	Communication or information exchange that occurs proactively for a provider's patients based on an established roster of information to be shared when a patient event occurs .	<p>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.</p> <p>Data access via push when patients have a healthcare event that requires provider awareness and/or follow-up.</p>

Specific types of Data

Claims/Encounters: Encounter data are detailed data about individual services provided by a capitated managed care entity. Claims data are generated whenever healthcare providers submit a request for payment to a health plan, providing information about the interactions between patients, healthcare providers, and insurers.

Orders/Referrals: Orders or referrals are generated when a provider refers a patient to an external party or puts in an order for a patient to receive a service from an external entity or provider.

Admission, Discharge, Transfer Notifications (ADTs): ADT notifications are alerts that are sent when a patient is admitted to a facility (commonly a hospital), transferred to another facility, or discharged from a hospital.

CCD: An electronic document summarizing a patient's health record that is shared when their care is transferred from one healthcare provider to another.

Social Services: Data encompassing non-health care, social services information for a patient, such as housing data from the Homeless Management Information System (HMIS).

DSA Signatory Grants

DSA Signatory Grant Timeline:

- Grants are available in 2023 through three funding rounds. Whether funding will be available in 2024 is unknown at the date of this publication.

DSA Signatory Grant Resources:

- CDII DSA Signatory Grants 101
- Multi-Association Education Initiative Webinar on Applying for a DSA Signatory Grant
- CDII DSA Signatory Grants Guidance

Actions to Take:

- Determine if a DSA Signatory Grant Round is open.**
- Determine if your organization is eligible for a grant.** For either type of DSA Signatory Grants, eligible organizations are those who:
 - **Have signed the DSA**
 - **Have a health information technology (HIT) need to conduct data exchange.** In their grant application, Signatories must demonstrate that they require technical support and additional capabilities to assist in conducting data exchange in accordance with the DSA and its Policies & Procedures.
- Determine which grant you will apply for:**
 - **QHIO Onboarding Grant:** QHIO Onboarding grants are for organizations that are already connected to an EHR and want to connect to an all-in-one solution that will establish all the infrastructure they need to conduct data exchange in accordance with the DxF. Applicants for this grant receive support with submitting applications and managing grants.
 - **Technical Assistance (TA) Grants:** TA grants are for organizations that either still need to connect to an EHR (or a relevant electronic record system for social service organizations), or who want to establish their own HIE solution in order to conduct data exchange in accordance with the DxF. Applicants for this grant submit applications and manage grants independently.

Actions to Take (Cont.):

- **Determine if you will apply on your own or with others as part of an “umbrella” application.**
 - Eligible Signatories may choose to apply on their own, or as part of an “umbrella” application with other Signatories
 - 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 through an umbrella application. All DSA Signatories included in an application must co-sign the application. Examples include a corporate parent, an Independent Practice Association, or others. Each grant needs to tie back to one shared technology approach. **An umbrella application is eligible for up to \$500,000.**

Signatory Type		Funding Maximum
General Acute Care Hospitals, Acute Psychiatric Hospitals, and Skilled Nursing Facilities	Serving Underserved Communities/Geographies <u>and</u> Did Not Receive Cal-HOP Funding	\$100,000
	Other	\$50,000
Physician Organizations and Medical Groups	Serving Underserved Communities/Geographies <u>and</u> 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 <u>and</u> Did Not Receive Cal-HOP Funding	\$50,000
	Other	\$25,000

Acknowledgments

This toolkit was prepared through a DSA Education Initiative Grant from the Center for Data Insights and Innovation at the California Health and Human Services Agency.

BluePath Health and Transform Health staff contributed to the development of this Toolkit, including Heather Bates, Olivia Bundschuh, Lisa Chan-Sawin, Robby Franceschini, Maia Kosek, Timi Leslie, Stephanie Thornton, John Weir, and Sarabeth Zemel. We thank the Center for Data Insights and Innovation and Rally for their review and contributions to this Toolkit. We also thank the Multi-Association DxF Education Initiative partner associations for their contributions to this project. The views expressed in this toolkit are the authors' own, and do not necessarily reflect those of the partner associations.

To support DxF education and participation, the following partner organizations and consulting partners have come together to form the Multi-Association DxF Education Initiative:



Consulting Partners

