



Fact Sheet: California Data Sharing Agreement and Policies and Procedures

On July 5, 2022, the California Health and Human Services Agency (CalHHS) Center for Data Insights and Innovation (CDII) released the final Data Exchange Framework (DxF) and associated Data Sharing Agreement (DSA) and Policies and Procedures (P&Ps), as required under [A.B. 133 \(2022\)](#). (For more information on A.B. 133, please see our [fact sheet](#).) CalHHS developed these policies with input from a Stakeholder Advisory Group and Data Sharing Agreement Subcommittee. All policies will go into effect on January 31, 2024.

In collaboration with its Stakeholder Advisory Group, CalHHS CDII developed several [guiding principles](#) as part of the Data Exchange Framework to guide design and implementation, support deliberations, and build trust among data exchange partners. These principles include:

- Advance health equity
- Make data available to drive decisions and outcomes
- Support whole person care
- Promote individual data access
- Reinforce individual data privacy and security
- Establish clear and transparent terms and conditions for data collection, exchange, and use
- Adhere to data exchange standards; and
- Ensure accountability.

Key Provisions of the Data Sharing Agreement and Policies and Procedures

A.B. 133 requires certain entities to “exchange health information or provide access to health information to and from” other specified entities in “real-time” by January 31, 2024, including but not limited to general acute care and psychiatric hospitals, physician organizations and medical groups, SNFs, clinical labs, and health care service plans and Medi-Cal Managed Care Plans. Other entities, like physician practices with fewer than 25 physicians, will not need to comply with the mandate until January 31, 2026.

Such entities must agree to participate in a single data sharing agreement and common policies and procedures that govern the exchange of health information among all of the participating entities and that are intended to “leverage and advance national standards for information exchange and data content.” Other entities can sign the DSA to become a participant but are not required to under state law.



Below are several topics and associated provisions addressed by both the final DSA and Policies and Procedures released by CDII on July 5th:

<p>Requirement to Exchange Health and Social Services Information¹</p> <p>(P&P OPP-5)</p>	<p>Participants that sign the DSA have an obligation to share certain data with all other participants, unless they do not have the data requested or cannot share it under law.</p> <p>“All Participants shall respond to requests for Health and Social Services Information made by other Participants and shall share Health and Social Services Information when required under the Required, Permitted and Prohibited Purposes Policy. A Participant shall fulfill its duty to respond by either (i) providing the requested Health and Social Services Information in accordance with the Data Sharing Agreement (the “DSA”) and Applicable Law, or (ii) providing a clear written response that states the Health and Social Services Information is not available, cannot be exchanged under Applicable Law, or is not required to be shared under the DSA.”</p>
<p>Data Elements to be Exchanged</p> <p>(P&P OPP-8)</p>	<p>Participants that are health care providers are required to share clinical data, while those that are health plans are required to share claims, encounter and clinical data.</p> <p>Providers: “Health Care Providers...shall provide access to or exchange at a minimum: a. Until October 6, 2022, data elements in the United States Core Data for Interoperability (USCDI) Version 1 if maintained by the entity. b. After October 6, 2022, all Electronic Health Information (EHI) as defined under federal regulation in Section 171.102 of Title 45 of the Code of Federal Regulations, including data elements in the United States Core Data for Interoperability (USCDI) Version 2, if maintained by the entity.”</p> <p>Plans: “Health Plans, including but not limited to health care service plans and disability insurers that provide hospital, medical, or surgical coverage that are regulated by the Department of Managed Health Care or the Department of Insurance, Medi-Cal managed care plans, shall provide access to or exchange, at a minimum, the data required to be shared under the Centers for Medicare and Medicaid Services Interoperability and Patient Access regulations for public programs as contained in United States Department of Health and Human Services</p>

¹ The DSA defines “**Health and Social Services Information**” as “any and all information received, stored, processed, generated, used, transferred, disclosed, made accessible, or shared pursuant to this Agreement, 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, deidentified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), anonymized data, pseudonymized data, metadata, digital identities, and schema.”

	<p>final rule CMS-9115-F, 85 FR 25510 including, but not limited to, adjudicated claims, encounter data and clinical data as defined in the USCDI if maintained by the entity.”</p>
<p>Methods to Exchange Data (P&P OPP-5)</p>	<p>Participants may use various technology solutions to support the exchange of Health and Social Services Information, including Qualified Health Information Organizations (HIOs)</p> <p>“The Data Exchange Framework is intended to be technology agnostic, meaning that no particular technology or method to exchange data is preferred. Participants may use various technology solutions, applications, interfaces, software, platforms, clearinghouses and other information technology resources.”</p>
<p>Permitted, Required, and Prohibited Uses (P&P OPP-4)</p>	<p>Participants are required to share data related to Treatment, Payment and some Health Care Operations activities (as such terms are defined under HIPAA) that do not require patient authorization and are permitted to share data where allowed by law and subject to patient authorization. Participants cannot access information through the DSA with the intention of selling that data, and participants cannot charge fees to other participants for any exchange under the DSA.</p> <p>Required purposes: “...Participants are required to exchange Health and Social Services Information and/or provide access to Health and Social Services Information pursuant to the Data Exchange Framework for Treatment, Payment, Health Care Operations and Public Health Activities as those terms are defined herein.”</p> <p>Permitted purposes: “Participants are permitted to exchange or provide access to Health and Social Services Information, including information subject to 42 C.F.R. Part 2, for any purpose not set forth in Section 3 below, provided appropriate Authorizations are made, if necessary, and the disclosure or use of Health and Social Services Information is permissible under Applicable Law. Such purposes include but are not limited to Social Services Activities and Research activities.”</p> <p>Prohibited purposes: “Unless otherwise permitted by Applicable Law or a legally valid agreement, Participants shall not access Health and Social Services Information through the DSA in order to sell such information.”</p> <p>Fees: “Participants are prohibited from charging fees to other Participants for any exchange of Health and Social Services Information under the DSA; provided that the foregoing shall not prohibit a Qualified HIO from charging fees to Participants who engage in data-sharing activities through the Qualified HIO.”</p>

<p>Breach Notification²</p> <p>(P&P OPP-3)</p>	<p>Participants must notify the Governance Entity (once it is established) and any affected participants of any breach, in addition to complying with all other applicable breach notification laws.</p> <p>“As soon as reasonably practicable after discovering a Breach has occurred, and within any timeframes required by Applicable Law, a Participant shall notify the Governance Entity and all Participants impacted by the Breach.”</p>
<p>Individual Access Services</p> <p>(P&P OPP-7)</p>	<p>Individuals have the right of access to inspect and copy their data maintained by any Participant, except where the Participant has sufficient grounds to deny such right of access under applicable law.</p> <p>“To the extent permitted by Applicable Law, an Individual User or an Individual User’s Personal Representative has a right of access to inspect and obtain a copy of PHI or PII about the Individual User, for as long as the PHI or PII is maintained by a Participant. Notwithstanding the foregoing, if permitted under Applicable Law, a Participant shall have the authority to deny right of access to inspect or obtain a copy of PHI or PII.”</p>

Remaining Policy Issues

CDII has stated that additional P&Ps will be developed through the forthcoming DxF governance process and stakeholder input, including:

- Qualification process for health information organizations:** Stakeholders have identified the need for a qualification process for Qualified Health Information Organizations, as defined in the DSA, in California that can serve as data sharing intermediaries, like the qualification process developed for the California HIE Onboarding Program.
- Definition of “real-time” data exchange:** A.B. 133 calls for “real-time” data sharing among organizations in the state, which is currently not addressed in the initial set of P&Ps.
- Statutory authority for governance and enforcement:** The DSA and P&Ps reference a governance entity that will oversee the DxF and develop of subsequent policies related to data exchange and enforcement of the DSA. CalHHS and its governance entity need statutory authority to enforce the DSA and P&Ps.

² It should be noted that the DSA and P&P definition of “breach” is broader than both the HIPAA and CMIA definitions. In example, a breach notification is not required under HIPAA or the Cal. Health and Safety Code is a risk analysis concludes that there is a low probability that data has been compromised.

Other needs include:

- **Funding for onboarding and infrastructure:** Many health information organizations, providers, and plans will require funding for infrastructure, workflow development and technology adoption to support their data sharing obligations under the DSA.
- **Development of policies pertaining to social services organizations:** Social services organizations capture and share a wide variety of data related to demographics, care plans and social needs, for example, that are not usually captured using the same standards as health care organizations outlined in the DSA P&Ps.
- **Refinement of the DSA and P&Ps to ensure consistency with existing legal obligations under state and federal law.** The DSA and P&Ps will need to be updated to ensure they align with other laws. For example, the current definition of “minimum necessary” under the DSA and P&Ps allows an exception where compliance is “not feasible,” which diverges from the exceptions under HIPAA and requires further guidance on what constitutes feasibility.

What’s next?

Health plans and most health care providers must execute the DSA on or before January 31, 2023, while health and social services organizations will be encouraged to execute the DSA by then. Health plans and most health care providers must then begin sharing data with other participants on or before January 31, 2024.

In the meantime, CalHHS CDII plans to establish an interim Implementation Advisory Committee and DSA P&P Subcommittee in July 2022, along with a legislative proposal to establish a permanent Health and Human Services (HHS) Data Exchange Board.³ By 2023, CalHHS plans to establish the HHS Data Exchange Board to oversee implementation of the DxF and divide the governance functions between the agency and the HHS Data Exchange Board.⁴ CalHHS will also produce several additional P&Ps over the coming months.⁵ Stakeholders will have the opportunity to provide public comment on these proposals under the modification and amendment provisions of the P&Ps.

³ CalHHS, Data Exchange Framework Stakeholder Advisory Group Meeting #9, June 23, 2022, https://www.chhs.ca.gov/wp-content/uploads/2022/06/CalHHS_DxF-Stakeholder-Advisory-Group_Meeting-9_June-23-2022_Deck_Final_v1.pdf.

⁴ Id.

⁵ Topics for additional P&Ps include Qualified HIO Designation Process; Real-time Data Exchange; Monitoring and Auditing; Enforcement; Information Blocking; Technical Requirements for Exchange. Id.

Standards and regulations referenced within the DSA and P&Ps

<p>United States Core Data for Interoperability (USCDI) versions 1 and 2</p>	<p>The USCDI version 1 created a set of 16 standardized data classes to facilitate the aggregation of data elements, easing interoperability for providers across the country (The Office of the National Coordinator for Health Information Technology, 2020). Version 2 was released in 2021, expanded the data classes from 16 to 19, and included more detailed data elements within each class. (Note that version 3, not mentioned in the DSA or P&Ps, was released in July 2022.)</p>
<p>HIPAA Regulations under Title 45 of the Code of Federal Regulations (C.F.R.)</p>	<p>Title 45 of the Code of Federal Regulations encompasses the federal rules and regulations that apply to public welfare. A few of the more frequently referenced within the DSA are summarized here.</p> <p>45 C.F.R. § 164.501 contains the definitions for correctional institution, data aggregation, designated record set, direct treatment regulation, health care operations, health oversight agency, indirect treatment relationship, inmate, marketing, payment, psychotherapy notes, public health authority, research, and treatment, as they relate to health information privacy and security.</p> <p>45 C.F.R. § 164.502 includes the general rules for uses and disclosures of protected health information.</p> <p>45 C.F.R. § 164.504 outlines the organizational requirements for uses and disclosures.</p> <p>CFR § 164.508 contains the uses and disclosures that require authorization.</p> <p>45 C.F.R. § 164.512 outlines what uses and disclosures do not require authorization.</p> <p>45 C.F.R. § 164.514 specifies other requirements related to the use and disclosure of protected health information, including standards and implementation of de-identification, minimum necessary, and verification requirements.</p> <p>45 C.F.R. § 164.524 is in reference to the right of individuals to access their protected health information.</p> <p>45 C.F.R. part 164, subpart C refers to the security standards for the protection of electronic health information.</p> <p>45 C.F.R. part 164, subpart E refers to the privacy of individually identifiable health information.</p>
<p>Confidentiality Regulations for Substance Use Disorder Records at</p>	<p>Title 42 of the Code of Federal Regulations sets out the federal rules and regulations that govern the disclosure and use of patient records related to substance use disorders. It includes relevant definitions, safeguards,</p>

<p>42 C.F.R. Part 2 and for Mental Health under the Lanterman-Petris-Short Act</p>	<p>and procedures, which are significantly more stringent than HIPAA for any subject “Part 2 Programs.”</p> <p>Lanterman-Petris-Short Act confidentiality provisions refer to California Welfare and Institutions Code §§ 5328-5328.9. It provides more stringent protections than HIPAA for information related to mental health treatment delivered in certain institutional and outpatient settings.</p>
<p>HL7 Data Formats</p>	<p>Health Level 7 is an organization that creates standards for electronic health data exchange, integration, and aggregation.</p> <p>HL7 Messaging Standard Version 2.5.1 refers to the messaging standards for electronic health data exchange, with emphasis on the inpatient acute care setting.</p> <p>HL7 Clinical Document Architecture (CDA®) Release 2 contains the standards for clinical documents between healthcare providers and patients.</p> <p>HL7 Companion Guide to Consolidated Clinical Document Architecture (C-CDA®) 2 is meant to provide additional tools, resources, and guidance to assist implementers in improving interoperability.</p> <p>HL7 Fast Health Interoperability Resources (FHIR®) Release 4.0.1 is the standard for interoperability between all players of the healthcare ecosystem and contains applicable resources and regulations.</p> <p>US Core Implementation Guide 4.0.0 STU4 contains the standards and FHIR resources necessary to create the United States Core Profiles.</p>
<p>U.S. Department of Health and Human Services Interoperability and Patient Access Final Rule</p>	<p>This final rule implements certain provisions of the 21st Century Cures Act granting the Centers for Medicare and Medicaid Services (CMS) to create a set of policies to advance interoperability and patient access to health information. This rule’s key points include the enabling of patients to electronically access their health information and ensuring providers and payers can attain access to all relevant patient health information.</p>
<p>U.S. Office of the National Coordinator for Health IT Cures Act Final Rule</p>	<p>This final rule implements certain provisions of the 21st Century Cures Act related to HIT developer certification requirements, information blocking, and patient access.</p>