CHCF DATA EXCHANGE EXPLAINER SERIES

MAY 2022

by Karen Ostrowski, MBA, and Rachel Goldberg, MPH

Designing an Effective Statewide Data Sharing Agreement

The opportunity. Assembly Bill 133 (AB 133) requires the California Health and Human Services Agency (CalHHS) to develop a data exchange framework that includes a single statewide data sharing agreement and common set of policies and procedures to govern the exchange of health information among health care entities and government agencies beginning in June 2024. This framework will enable and require real-time access to and exchange of health information among providers and payers directly between each other and through qualified data exchange networks. The framework will be aligned with other state and federal data exchange standards and requirements.

Currently, data exchange in California takes place under a patchwork of voluntary data sharing agreements established by state and national networks, as well as under a multitude of community and program-specific agreements. Many data exchange arrangements are missing key stakeholders — such as rural providers, health plans, community-based organizations, and behavioral health and state and county-based entities — and missing important types of data; for example, social determinants of health information. The opaque maze of federal and state health privacy laws and regulations persistently inhibits many kinds of information sharing including, for example, the sharing of mental health and substance use disorder information, as well as exchange by smaller and traditionally disconnected health and human service organizations and county health departments.

AB 133 calls for the establishment of a single agreement that addresses these challenges, is inclusive and responsive to the needs of all participants, and scales robust data exchange across California.

Considerations for successful design and implementation of a statewide data sharing agreement. CalHHS is charged with building a statewide contract — with feedback from an advisory group of state policymakers and stakeholders — that defines the basic requirements and expectations amongst signatories and meets California's unique needs. The statewide data sharing agreement (DSA) is intended to serve as the legal agreement executed by a broad spectrum of health care organizations and data exchange intermediaries, while the policies and procedures will outline the detailed rules and guidance to support implementation of the framework. The agreement should address the following:

- Clinical and nonclinical data sharing, including behavioral health and social service data
- Participation by a range of service providers, including community, state, and county-based providers
- Direct and network-mediated exchange, including how consent and accountability are managed for each
- Alignment with existing national and local data exchange frameworks
- Accordance with federal and state law and regulatory requirements across data and participant types
- Adaptability of the data sharing agreement to changes in the external environment over time

The following three tables are intended to support the effort by state policymakers and their advisors to design a data sharing agreement that meets these needs and is executable by all applicable entities. Table 1 summarizes the key elements of any data sharing agreement. Table 2 on page 3 considers these elements in the context of AB 133. Table 3 on page 4 describes how these elements are at play in other data sharing agreements that are relevant, though designed for other purposes.

Table 1. Common Data Sharing Agreement Provisions

PURPOSE AND SCOPE	PERMITTED USES AND DISCLOSURES	GOVERNANCE AND AUTHORITY	PARTICIPANTS AND RESPONSIBILITIES	PRIVACY AND SECURITY SAFEGUARDS
Describes, in general terms, the purpose of the data sharing arrangement, the organizations involved and their relationship to one another, and the data to be exchanged.	Lists the ways that data may be used and shared, in accordance with applicable (and specified) federal and state laws, regulations, and policies. Examples include treatment, payment, health care operations, and public health.	Specifies the entity responsible for maintaining the agreement, as well as enforcement of the data sharing terms and conditions.	Specifies signatories of the agreement and their rights and responsibilities, such as user management, training, and individual consent.	Describes at a high level the administrative, technical, and physical protections that all participants must adopt to ensure users and systems meet minimum standards for protecting the privacy, confidentiality, and security of the data.

Table 2. Considerations for AB 133 Data Sharing Agreement

PURPOSE AND SCOPE	PERMITTED USES AND DISCLOSURES	GOVERNANCE AND AUTHORITY	PARTICIPANTS AND RESPONSIBILITIES	PRIVACY AND SECURITY SAFEGUARDS
AB 133 requires a broad spectrum of health care organizations to execute the DSA and to exchange, or provide access to, health information with other mandated organizations. The DSA must align with federal and state data requirements and privacy laws, be technology agnostic, and support additional data types and providers over time.	AB 133 requires the data exchange framework DSA to address the exchange of information for treatment, payment, and operations purposes, and strongly encourages that it fulfill public health and social services purposes.	AB 133 designates CalHHS as the entity responsible for the development of the data exchange framework DSA. A stakeholder advisory group is responsible for guiding decision-making and advancing recommendations on the initial design of specific elements of the DSA and forwarding recommendations about governance and enforcement.	AB 133 requires entities including hospitals and health care providers, health plans, and clinical laboratories to execute the data exchange framework DSA and exchange data in accordance with federal and state health privacy laws and regulations. **January 31, 2023.** Execution of data exchange framework DSA by health and human service organizations.* **January 31, 2024.** Most providers implement data exchange framework.* **January 31, 2026.** Remaining providers implement data exchange framework.†	AB 133 stipulates that the stakeholder advisory group will advance recommendations on privacy, security, and equity risks of data sharing, but it does not include specific safeguards for participants or consumers.

* General acute care hospitals, physician organizations and medical groups, skilled nursing facilities, health service plans and disability insurers, Medi-Cal managed care plans, clinical laboratories, and acute psychiatric hospitals. County health, public health, and social services providers are encouraged to connect to the data exchange framework.

† Physician practices of <25 physicians, rehabilitation hospitals, long-term acute care hospitals, acute psychiatric hospitals, critical access hospitals, and rural general acute care hospitals with <100 acute care beds, state-run acute psychiatric hospitals, and nonprofit clinics with <10 providers.

Table 3. Potential Models for California's Statewide Data Sharing Agreement

PURPOSE AND SCOPE	PERMITTED USES AND DISCLOSURES	GOVERNANCE AND AUTHORITY	PARTICIPANTS AND RESPONSIBILITIES	PRIVACY AND SECURITY SAFEGUARDS	LIMITATIONS AS A MODEL FOR DATA EXCHANGE FRAMEWORK DSA
Trusted Exchange Framework and Common Agreement (TEFCA)					
Trust framework and data sharing agreement to enable the exchange of basic clinical information under a common set of principles, terms, and conditions.	Treatment, payment, and health care operations; public health activities; government benefits determination; and individual access services.	Federal Office of the National Coordinator (ONC) has ultimate authority and approves all agreements and frameworkdocuments. Governance and enforcement authority is delegated to the Recognized Coordinating Entity (RCE), an independent nonprofit operating under an agreement with ONC after a competitive bid process.	Approved Qualified Health Information Networks (QHINs) that serve providers, HIOs, health plans, government agencies, and other entities. Participation is voluntary, though participants must adhere to exchange standards.	Establishes HIPAA (Health Insurance Portability and Accountability Act) as the standard and specifies the safeguards that must be in place for protecting data as they are exchanged. Describes security incident notification and reporting. Requires written privacy policies related to individual access to information.	Designed to support data exchange between networks (e.g., HIOs), not peer-to-peer (e.g., between individual data sources). Participation is limited to a small number of designated QHINs able to meet requirements specified by the RCE. Aligns with national standards for exchange, but purposes are limited and exclude nonclinical data types and participants. Data standards do not currently include SDOH.
Carequality Connected Agreement					
Nationwide interoperability framework to enable clinical data exchange between health information networks (e.g., Commonwell, eHealth Exchange), electronic health record vendors (e.g., Epic, Cerner, SureScripts), and other technology platforms and service providers.	Treatment, payment, and health care operations as defined by HIPAA.	Carequality is an independent 501(c)(3) organization. Governance and enforcement authority is delegated to a steering committee appointed by the board of directors and is comprised of representatives from founding organizations, ONC, federal agencies, and other stakeholders.	Electronic health record (EHR) vendors and specialized commercial exchange networks, as well as a limited number of community or statewide HIOs. Participation is voluntary, though participants must adhere to exchange standards. Other responsibilities include requirement to respond and to apply network obligations to participants and their end users.	Establishes HIPAA as the standard and specifies the safeguards that must be in place for protecting data as they are exchanged. Describes adverse security event notification and reporting.	Designed for exchange between EHRs and networks (e.g., HIOs), not peer-to-peer (e.g., between individual data sources). Aligns with national standards for exchange, but purposes are limited to treatment, payment, and health care operations, and exclude nonclinical data types and participants.

Table 3. Potential Models for California's Statewide Data Sharing Agreement, *continued*

PURPOSE AND SCOPE	PERMITTED USES AND DISCLOSURES	GOVERNANCE AND AUTHORITY	PARTICIPANTS AND RESPONSIBILITIES	PRIVACY AND SECURITY SAFEGUARDS	LIMITATIONS AS A MODEL FOR DATA EXCHANGE FRAMEWORK DSA
eHealth Exchange Data Use and Reciprocal Support Agreement (DURSA)					
Nationwide legal framework and data sharing agreement that establishes responsibilities, obligations, and expectations for the exchange of clinical data between health information networks. Began as a framework for federal agencies to share data.	Treatment, payment, and health care operations as defined by HIPAA; public health activities; pursuant to an individual authorization or consent; to support value-based payment models or alternative payment arrangements; and for certain government functions.	Governed by a coordinating committee made up of elected network representatives, which implements the DURSA and related "operating policies and procedures" (OPPs). All OPPs are presented to network participants for a 30-day "notice and objection period" before becoming effective.	Participating networks include health systems, community and statewide HIOs, and federal agencies. Participants are required to adhere to exchange standards and to manage the compliance of their end users.	Establishes HIPAA as the standard and specifies the safeguards that must be in place for protecting data as they are exchanged. Describes adverse security event notification and reporting.	Participation is largely limited to health care organizations, large health systems, and federal agencies. Aligns with national standards for exchange, but purposes are limited and exclude nonclinical data types and participants.
California Trusted Exchange Network California Data Use and Reciprocal Support Agreement (CalDURSA)					
Statewide trust framework and multiparty data sharing agreement establishing mutual responsibilities, obligations, and expectations of a peer-to-peer network for the exchange of clinical data. Modeled after federal DURSA.	Treatment, payment, and health care operations as defined by HIPAA and public health activities.	Network participants select the California Interoperability Committee, which is responsible for governance and enforcement.	Community HIOs, some health systems and state agencies. Participation is voluntary, though participants must adhere to exchange standards. Other responsibilities include a requirement to respond and to apply network obligations to participants and their end users.	Establishes HIPAA as the standard and specifies the safeguards that must be in place for protecting data as they are exchanged. Specifies breach and security incident reporting in accordance with HIPAA and state breach notification regulations.	Participation is largely limited to California-based HIOs, health systems, and some state agencies. Agreement is outdated — it has not been updated since it was developed in 2014. Exchange purposes are limited and exclude nonclinical data types and participants.
Model Modular Participants Agreement (MMPA)					
Model data sharing agreement developed between an HIO and its participants, describing the services provided by the HIO and the data to be exchanged (generally clinical information among health care providers).	Treatment, payment, and health care operations as defined by HIPAA.	Participants grant limited authority to the HIO to maintain the agreement and to enforce data sharing provisions among all participants.	Health care providers, hospitals, ancillary providers, and health plans. Responsibilities of participants include user management, role-based access, and data quality or accuracy standards. Participation is voluntary, though participants must adhere to exchange standards.	Specifies the standards for privacy and security compliance and for breach and security incident reporting.	Designed as an agreement between a service provider, such as an HIO, and community participants, which are primarily covered entities or business associates, and exchange is often limited to clinical data for treatment purposes.

About the Author

Karen Ostrowski, MBA, vice president of policy innovation at Intrepid Ascent, developed this fact sheet with Rachel Goldberg, MPH. **Intrepid Ascent** supports communities in the exchange and use of data to improve health.

About the Foundation

The **California Health Care Foundation** is dedicated to advancing meaningful, measurable improvements in the way the health care delivery system provides care to the people of California, particularly those with low incomes and those whose needs are not well served by the status quo. We work to ensure that people have access to the care they need, when they need it, at a price they can afford.

CHCF informs policymakers and industry leaders, invests in ideas and innovations, and connects with changemakers to create a more responsive, patient-centered health care system.