INTRODUCING CALIFORNIA'S DATA EXCHANGE FRAMEWORK & UPCOMING STATEWIDE DATA SHARING OBLIGATIONS FOR HEALTH CARE ENTITIES

by **Andrea Frey**
Hooper, Lundy & Bookman, LLP

Andrea Frey is an associate in the Business Department of Hooper Lundy & Bookman, P.C, where she assists health care providers, including hospitals, public health care districts, physician groups, individual physicians, and health services companies with a broad range of business, general corporate and regulatory matters. Andrea graduated from Tufts University with degrees in Economics, International Relations, and Spanish in 2009 and received her J.D. degree with honors from the University of Washington while simultaneously earning her M.P.H. in 2016.

by **Paul Smith**
Hooper, Lundy & Bookman, LLP

Paul Smith is a shareholder of the firm of Hooper, Lundy & Bookman who advises clients in health care and other industries on health information privacy and security, corporate formation and governance, joint ventures, financing, reimbursement and regulatory compliance. He also represents technology companies in transactional, financing and licensing matters, and data privacy and security.

"The exchange of information is essential to a well-functioning health and human service ecosystem and lays the foundation for the coordinated delivery of care and services to support health and well-being for individuals and communities."

CalHHS, *Health Information Exchange in California, Gaps and Opportunities*

In July 2021, Governor Newsom signed Assembly Bill 133 into law, enacting California Health and Safety Code Section 130290 and putting the state on the path to building a statewide Data Exchange Framework (DxF), including a single data sharing agreement (DSA) and common set of policies and procedures (P&Ps) that govern and mandate "real-time" access to, or exchange of health information.

AB 133 charged the California Health and Human Services Agency (CalHHS) with developing and implementing the DxF, DSA, and an initial set of policies and procedures, with input from a stakeholder advisory group. After a year of development, on July 1, 2022, CalHHS adopted the DxF, and released the final versions of the DSA and P&Ps.

The DxF is not a statewide health information exchange; rather it is "technology agnostic" – meaning participants need only share health information with other participants through an existing exchange network, health information organization, or other technology as long as it adheres to specified standards and policies. However, it does represent the first time California has focused efforts on implementing a statewide data sharing network and making participation mandatory.

Below follows a summary of the development process and motivation behind the DxF, who must participate and what obligations participants have, as well as a brief overview of what's next and outstanding issues.

DXF BACKGROUND AND DEVELOPMENT PROCESS

The COVID-19 pandemic brought many long-standing issues with our health care system to the fore. In California, one of the problems spotlighted by the pandemic was the siloed and fragmented nature of how data is stored by payors, providers, hospitals, and public health systems, and the lack of seamless data exchange among such entities. The decentralized health information ecosystem created significant challenges for the state's public health system to effectively address the ongoing public health crisis, particularly the inability to examine social and economic factors in the context of medical care and health outcomes.

Mobilized by the data sharing gaps that stymied contact tracing and testing efforts early in the pandemic, the California legislature passed, and Governor Gavin Newsom signed, AB 133 as a budget trailer bill in July 2021. California's DxF aims, in part, to break down the barriers created by siloed data repositories to enable better patient access to and sharing of health information to improve the coordinated delivery of care and services for

individuals and communities.

The DSA is built upon state and national data exchange agreements that are in broad use, including the California Data Use and Reciprocal Support Agreement (CalDURSA), the federal Data Use and Reciprocal Support Agreement (DURSA), as well as previous guidance from the State and State Health Information Guidance (SHIG), and most recently, the federal Trusted Exchange Framework and Common Agreement (TEFCA), which the federal Office of National Coordinator for Health Information Technology (ONC) released in January 2022, with the goal of establishing a universal floor of interoperability through a common set of non-binding, foundational principles to facilitate information exchange and use.

Prior to this initiative, California had sponsored several privately-operated health information exchange pilot projects, focused on patient consent to health information sharing. CDPH also participates in the California Trusted Exchange Network (CTEN), an initiative of the California Association of Health Information Exchanges designed to provide a framework for information sharing among health information exchanges, and modeled on the national eHealth Exchange.

Following the passage of AB133, CalHHS convened the DxF Stakeholder Advisory Group beginning August 2021, which comprised a diverse set of representatives from 14 state departments and 27 stakeholder organizations (including health care service plans, insurers, physicians, hospitals, clinics, consumers, organized labor, privacy and security professionals, health information technology professionals, community health information organizations, county health, county social services, county public health, and community-based organizations). Over the course of the last year, the stakeholder group met with CalHHS monthly, providing information and advice on data elements, gaps in data collection, privacy and security, and assisting with the development of the DSA and P&Ps, of which there were various iterations released for review and comment from the public more broadly. Final versions of the DSA and the initial set of Policies and Procedures were released on CalHHS's website on July 5, 2022.

WHO MUST PARTICIPATE IN THE DXF?

AB 133 requires most health plans, hospitals, physician organizations, and clinical laboratories in California to execute the DSA by January 1, 2023[1], and begin sharing what is called "Health and Social Services Information" for treatment, payment and health care operations over the DxF by January 1, 2024. Health and Social Services Information means "any and all information received, stored, processed, generated, used, transferred, disclosed, made accessible, or shared pursuant to [the DSA], including but not limited to: (a) Data Elements as set forth in the applicable Policy and Procedure; (b) information related to the provision of health care services, including but not limited to PHI; and (c) information related to the provision of social services." The required data elements are described below.

While the duty to *respond* is effective for all participants on January 31, 2024, some participants are not required to *exchange* data until January 31, 2026. These are governmental participants, social services organizations, physician practices of fewer than 25 physicians, rehabilitation hospitals, long term acute care hospitals, acute psychiatric hospitals, critical access hospitals, rural general acute care hospitals with fewer than 100 acute care beds, state-run acute psychiatric hospitals, and nonprofit clinics with fewer than 10 health care providers.

A participant that is not technologically capable of exchanging Health and Social Services Information by the relevant due date must use best efforts to contract with another entity that provides data exchange services.

DXF PARTICIPANTS' DATA SHARING OBLIGATIONS: OVERVIEW & CONSIDERATIONS

AB 133 and the newly enacted Health and Safety Code § 130290 directed CalHHS to develop the exchange framework in addition to a common data sharing agreement and set of policies outlining the standards for and governance of compulsory information exchange among participants.

CalHHS also developed an initial set of policies and procedures implementing the DSA, though these are likely to be amended once CalHHS develops a form of governance process to oversee the DxF along with the promulgation of additional policies and procedures.

The initial P&Ps contain the bulk of

guidance, technical specifications, and processes to support the DSA and address the purposes and requirements for the exchange of information, breach notification, privacy and security safeguards, data elements to be exchanged, and the individual's right to access. CalHSS has said that future policies and procedures will address other topics, including information blocking, monitoring and auditing, enforcement, and technical requirements for exchange.

Below follows a high-level summary of participants' obligations under the DxF as detailed in each P&P:

Requirement to Exchange Health and Social Services Information

The central policy of the DxF requires all participants to exchange "Health and Social Services Information", by responding to a request for information from another participant by providing the requested information in accordance with the DSA, or stating that the requested information is not available, cannot be exchanged under applicable law, or is not required to be shared under the DSA. The policy is expressly "technology agnostic," meaning that it does not prescribe the method of exchange.

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

Permitted, Required and Prohibited Purposes

Participants will be *required* to exchange Health and Social Services Information for treatment, payment, health care operations and public health activities, as those terms are defined in the policies. However, a participant may disclose information to another participant for health care operations only if each entity has or had a relationship with the individual who is the subject of the information being requested and the information pertains to the relationship. This is consistent with the HIPAA rule (45 CFR 164.506(c)(4)).

The definitions of treatment, payment, health care operations and public health activities are also consistent with the HIPAA definitions, although the scope of "health care operations" encompasses only a subset of the activities that fall within the HIPAA definition of the term. These are:

1. Quality assessment and improvement activities as described in subsection (1) of the HIPAA definition.

2. Population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination and contacting of health care providers and patients with information about treatment alternatives, as set forth in the HIPAA definition.

Breach Notification Requirements

The enabling statute, Health and Safety Code section 130290, does not expressly impose a new data breach reporting obligation on participants in the DxF. However, beginning January 31, 2024, DxF policies will require participants to notify other "impacted" participants and the DxF Governance Entity of "Breaches."

The DSA defines a "Breach" to mean the unauthorized acquisition, access, disclosure or use of Health and Social Services Information in a manner not permitted by the DSA or applicable law (whether or not, apparently, any other participant is "impacted"). This includes data that was, or is reasonably believed to have been, acquired by an unauthorized person (including encrypted data if the encryption key was also acquired). The notification must be in writing, and made as soon as reasonably practical after the discovery of the breach, and within any timeframes required by applicable law. The report is to include, to the extent available:

1. A one- or two-sentence description of the breach;

2. A description of the roles of the people involved in the breach (e.g., employees, service providers, unauthorized persons);

3. The type of Health and Social Services Information breached;

4. The participants likely impacted by the breach;

5. The number of individuals or records impacted/estimated to be impacted by the breach;

6. Actions taken by the participant to mitigate the breach;

7. Current status of the breach (under investigation

or resolved); and

8. Corrective action taken and steps planned to be taken to prevent a similar breach.

The DSA also requires participants to provide any requested information and assistance to the Governance Entity or other participants in the investigation of breaches, subject to a participant's right to restrict or condition its cooperation or disclosure of information in the interest of preserving privileges in any foreseeable dispute or litigation or protecting its confidential information, and participants are not required to disclose PHI or PII in violation of applicable law. However, these qualifications to the obligation to cooperate do not apparently apply to the initial report.

This policy extends participants' data breach reporting obligations beyond current requirements, and raises unresolved questions. In the absence of a business associate relationship, there is currently no obligation to report data breaches to business partners. Moreover, all the breach reporting regimens to which health care providers are subject in California allow the provider to perform a risk analysis, and do not require notification if the analysis concludes that the probability that the data was compromised is low.

The confidentiality of these reports is open to question. The DSA has a definition of "Confidential Participant Information." It is not clear whether breach reports would fall within this definition. Assuming they do, the DSA requires the Governance Entity to hold Confidential Participant Information in confidence, and not to redisclose it to any person or entity except as required by applicable law. However, this is just a contractual obligation, not a legal protection, and it does not apply to other participants who receive breach notices. The prospect that the Governance Entity will become a trove of notices of every health-care related data breach in California, however minor, is cause for concern.

Privacy and Security Safeguards

The DxF policy requires participants to develop and maintain appropriate safeguards to prevent unauthorized use or disclosure of protected health information (PHI) or personally identifiable information (PII) in a manner consistent with HIPAA regulations, including implementing appropriate administrative, physical and technical safeguards that protect the confidentiality, integrity and availability of PHI or PII. Participants that use, access or disclose behavioral health information must also comply with 42 CFR Part 2 (federal regulations governing the confidentiality of substance use disorder records), and California's Lanterman-Petris-Short Act (governing confidentiality of information and records obtained in the course of providing mental health services by certain entities).

This policy effects sweeping extensions of current security regulations. The HIPAA security rule applies only to electronic PHI; this policy would extend the HIPAA security rule to PII by requiring participants to protect PII "in a manner consistent with HIPAA Regulations." It would also subject all participants to the HIPAA security rule, whether or not they are covered entities under HIPAA.

Data Elements to be Exchanged

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. For health care providers, the P&Ps require that they "shall provide access to or exchange at a minimum … data elements in the United States Core Data for Interoperability (USCDI) Version 1 if maintained by the entity" until October 6, 2022, after which they will be required to provide access to or exchange all information contained in a "designated record set," as defined in the HIPAA regulations. This is effectively the entire medical and billing records about individuals.

Health plans, on the other hand, "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 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."

NEXT STEPS AND LOOKING FORWARD

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.[2] By next year, CalHHS intends 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. CalHHS will also promulgate several additional P&Ps over the coming months on topics that include information blocking, monitoring and auditing, and enforcement mechanisms and penalties for non-compliance or failure to participate in the DxF. Stakeholders will have the opportunity to comment on the policies, so any organization mandated to participate in the DxF would be well-advised to monitor the release of these policy proposals, in conjunction with internal preparation for participation in the DxF.

ENDNOTES

1 Specifically, AB133 stipulates that the following entities must execute the Framework's "Data Sharing Agreement" on or before January 31, 2023:

- General acute care hospitals, as defined by Section 1250.
- Physician organizations and medical groups with 25 or more physicians.
- Skilled nursing facilities, as defined by Section 1250, that currently maintain electronic records.
- 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. This section shall also apply to a Medi-Cal managed care plan under a comprehensive risk contract with the State Department of Health Care Services pursuant to Chapter 7 (commencing with Section 14000) or Chapter 8 (commencing with Section 14200) of Part 3 of Division 9 of the Welfare and Institutions Code that is not regulated by the Department of Managed Health Care or the Department of Insurance.
- Clinical laboratories, as that term is used in Section 1265 of the Business and Professions Code, and that are regulated by the State Department of Public Health.
- Acute psychiatric hospitals, as defined by Section 1250.

2 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.