June 1, 2022

To: John Ohanian
Chief Data Officer and Director Center for Data Insights and Innovation
California Health and Human Services Agency

From: Michelle Cabrera, Executive Director, CBHDA

Subject: CBHDA Comments – Draft Data Exchange Framework

The County Behavioral Health Directors Association (CBHDA) represents the county behavioral health executives who administer Medi-Cal and safety net services for serious mental health (MH) conditions and substance use disorders (SUDs) in all 58 counties in California. County behavioral health (BH) plans are currently implementing significant policy changes and delivery system improvements required under DHCS' CalAIM initiative. Delivery system goals include expanding and improving data exchange capabilities.

On behalf of our members, we recognize and support the need for a broadly accepted framework to facilitate the sharing of information, including information related to behavioral health. The California Health and Human Services Agency (CHHSA) Data Exchange Framework (DxF) is an important step forward. However, the Data Sharing Agreement and accompanying Policies and Procedures do not address recognized challenges specific to exchanging behavioral health data, nor does the statute or analysis of gaps and opportunities explicitly recognize the need to exchange data related to Medi-Cal specialty mental health and substance use disorder services covered by county BH plans. If California hopes to advance meaningful data exchange, particularly for Medi-Cal beneficiaries with complex health and social service needs, county behavioral health agencies need to be acknowledged and supported in state policy guidance and budget initiatives that fund data exchange.

I. Data Sharing Agreement (DSA)

AB 133[1] does not obligate county behavioral health plans to join the agreement within the established time frames. However, it does require the state to work with other trade associations representing counties to "encourage the inclusion of county health, public health, and social services, to the extent possible, as part of the California Health and Human Services Data Exchange Framework in order to assist both public and private

[1] Health & Safety Code § 130290

entities to connect through uniform standards and policies."[2] While county behavioral health services are not explicitly called out, this list recognizes the state's desire to limit the required participation of a broad range of county-led services. Behavioral health plans are also omitted from the statute's requirements for Medi-Cal managed care plans and health care service plans, as it only specifies inclusion of Medi-Cal plans *with a risk contract*.[3] Because county behavioral health Medi-Cal plans are not risk-based, AB 133 does not require county behavioral health Medi-Cal plans to participate.

Nonetheless, we do expect that county BH plans will sign the Data Sharing Agreement (DSA) and participate in the DxF in order to collaborate with important Medi-Cal partners (providers and managed care plans) and pursue other data sharing initiatives underway at the Department of Health Care Services (DHCS). If BH plans sign on, the Data Exchange Framework would significantly alter and expand the scope of responsibilities for county behavioral health plans. For example, county behavioral health plans are not currently subject to federal "information blocking" requirements intended to promote robust information sharing.[4] It is not yet known to us how execution of the DSA may subject BH plans to additional expectations related to information blocking. County BH plans will need to address any such ambiguities and consider attendant risks before moving forward with the agreement.

Another expansion of existing obligations for many entities that will execute the DSA is the DSA's inclusion of "PII, de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), pseudonymized data, metadata, digital identities, and schema." Sharing de-identified data may be beyond the scope of data sharing that entities are currently doing or expected to do. It is our understanding that the DSA subcommittee and DxF Workgroup discussed the use of de-identified data as something that could be useful for research and informing policy, but did not engage in an in-depth analysis surrounding specific use cases and permitted uses of these data. CBHDA recommends that de-identified data be excluded from the DSA unless further guidance is developed to clarify when a Participant would be required to provide de-identified data to another Participant, and how such information would be used. This could be discussed and further developed in a future Policy and Procedure. At a minimum, there should be a clarification that Participants are never required to share de-identified data under the terms of the DSA (but may do so if both parties agree).

While we have concerns about areas like the two examples above, we appreciate that the DSA permits a Governmental Participant to terminate the Agreement immediately if it determines "after reasonable diligence, that any action or inaction relative to an obligation, including conformance to changes in the Specifications or Policies and Procedures, will cause it to violate Applicable Law." We also appreciate that the Requirement to Exchange Health and Social Services Information Policy allows Governmental Participants to access Health and Social Services Information starting

[2] Health & Safety Code § 130290(e).
[3] Health & Safety Code § 130290(f)(4)
[4] 45 C.F.R. § 171.101(a) (federal rules apply to health care providers, health IT developers of certified health IT, health information exchanges, and health information networks)

January 31, 2024, but does not require them to disclose information until they are "technologically ready and able."

Recommendations (DSA): CBHDA requests that the flexibilities for Governmental Entities to terminate the DSA, access information, and exchange when they are technologically ready be reflected in the forthcoming policy and procedure on enforcement. Additionally, we strongly recommend that "de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), pseudonymized data, metadata, digital identities, and schema" be removed from the Health and Social Services Information required to be exchanged and included in a forthcoming Policy and Procedure after further workgroup deliberations. Additionally, there should be a clarification that Participants are never required to share de-identified data under the terms of the DSA.

II. Policies and Procedures

Due to a precedent in federal and state law of applying stricter confidentiality protections on behavioral health information, county behavioral health agencies regularly work with sensitive data and have heightened legal obligations under various state and federal laws to maintain the confidentiality of that data in accordance with their clients' authorizations and wishes. Behavioral health privacy and confidentiality laws routinely impose more stringent requirements than HIPAA or the Confidentiality of Medical Information Act (CMIA). We request that the DSA and related policies and procedures clearly reflect the necessity of complying with these laws, in order to create a common understanding and improve literacy and practice regarding the laws that govern behavioral health data sharing.

Notably, neither the DSA nor the policies and procedures include any reference to the confidentiality provisions under California's Lanterman-Petris-Short ("LPS") Act or state substance-use disorder laws, and there is only a passing reference to 42 C.F.R. Part 2. While we acknowledge there are numerous laws that could potentially be referenced, these state laws are broadly applicable to a variety of plans and providers that will be required to share data under the Data Exchange Framework. For example, the LPS Act places a series of limitations on information sharing which may require health care providers to obtain explicit patient consent before sharing any LPS-related information.[5] Similarly, state SUD laws[6] do not generally permit data sharing for health care operational or payment purposes without a client authorization.

Additionally, it was acknowledged during development of the DSA that technical assistance would be necessary and strongly recommended to support the sharing of specially protected information, including behavioral health data. This will be essential for entities that have not handled this data historically, which includes many health information organizations (HIOs). CBHDA strongly recommends that CHHSA provide technical assistance to support increased understanding and implementation of how

[5] Welf. & Inst. Code § 5328(a)(1)
[6] Health & Safety Code § 11845.5 and § 11812

specially protected data can be collected, used, and exchanged. We have identified this additional need in the DxF Gaps and Opportunities portion of our comments.

The following specific changes to the relevant Policies and Procedures (P&Ps) would appropriately recognize the key limitations imposed by state laws.

a. P&P - Permitted, Required, and Prohibited Purposes

Recommendation:

In the Permitted, Required, and Prohibited Purposes Policy, the carve out for disclosures inconsistent with Applicable Law should be made plain, and the references should not be limited solely to 42 C.F.R. Part 2. (additions *italicized*)

- In Section III.1, Required Purposes:

  a. Subject to the provisions of the DSA and the Policies and Procedures, 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, *unless such sharing is prohibited by Applicable Laws*.

- In Section III.3, Prohibited Purposes, paragraph b should be modified to read as follows:

  b. Participants shall not be required to exchange or provide access to information in a manner that is not permitted by Applicable Law, including 42 C.F.R. Part 2.

b. P&P - Requirement to Exchange Health and Social Services Information

Recommendation:

- In the Data Exchange Framework Policy and Procedure, Section III. A, Duty to Respond, the language should be amended to read as follows (additions *italicized*):

  … A Participant shall fulfill its duty to respond by either (i) providing the requested Health and Social Services Information, or (ii) responding with a standardized response that indicates the Health and Social Services Information is not available, cannot be exchanged, or is not required to be shared under the Data Sharing Agreement *and/or Applicable Law* (the "DSA"). All responses to requests for Health and Social Services Information shall comply with Specifications, the DSA, any other data exchange agreements and Applicable Law….

c. P&P - Breach Notification

The Breach Notification policy requires a Participant to notify the Governance Entity and all affected Participants "no later than seventy-two (72) hours after discovering a Breach has occurred." It also requires providing a written report to the Governance Entity and all affected Participants within ten calendar days. When breaches involve a governmental participant, notifications must be made even more rapidly, within 24 hours. These obligations go beyond federal requirements under HIPAA or state law obligations for reporting to the California Department of Public Health (CDPH). Notably, the policy requires notification not only to affected individuals and government regulators, but to *all affected Participants*.

Typically, HIPAA would not require a covered entity to notify another covered entity except for the case of business associates, who are required to notify the covered entity for which they are providing services within 60 calendar days.[7] Moreover, the policy imposes unreasonably tight timeframes on these notifications. Even California law—which is stricter than HIPAA when it applies—requires notification of affected patients and CDPH within 15 business days after detecting the unauthorized access, use, or disclosure of medical information.[8] HIPAA requires notification to individuals no later than 60 calendar days, and only requires notification to the federal government within the same 60-day timeframe if the breach affected more than 500 individuals.[9]

Recommendation: CBHDA recommends the policy be modified so that breach notifications to affected Participants more closely mirror applicable federal and state law. The policy could reflect HIPAA notification requirements as a minimum standard, and require following other federal and state laws when they are more strict.

d. P&P - Data Elements to Be Exchanged

- As currently drafted, formatting issues create ambiguities about who is subject to requirements. For example, paragraphs b. and c. in Section II.1. of the policy appear intended to apply to Health Care Providers as a list underneath paragraph a.i., but because they are organized at a higher level in the outline, there is uncertainty about whether they instead apply to other entities. Similar formatting issues occur throughout Section II.1. when text indicates that a list of subcategories will follow, but instead there are paragraphs at a higher level in the outline.

  Recommendation: CBHDA requests revisions to the Data Elements to Be Exchanged policy to clarify what data elements must be exchanged by each category of entity.

[7] 45 C.F.R. § 164.410(b).
[8] Cal. Health & Safety Code § 1280.15(b)
[9] 45 C.F.R. §§ 164.404(b), 164.408

- CBHDA also requests clarification about what is entailed in paragraph d of Section II.1 by the term "cost information." While CBHDA supports efforts to ensure patients have access to information about how much care will cost them, consistent with requirements outlined in CMS' Final Rule on Interoperability and Patient Access,[10] we are concerned that this term without further definition has broad implications which may be misinterpreted in the future. Given other policy considerations in the DxF surrounding the expansion of current federal and state requirements to all Participants who sign the DSA, we recommend that "cost information" be clearly defined to be consistent with the federal regulations on interoperability, which we believe is the intent behind the inclusion of "cost information" as a data element.

  Recommendation: To clarify the appropriate scope of "cost information," we request the following revision to paragraph d. (additions *italicized*):

  > d. For Individual Access Services, adjudicated claims and encounter information shall include *plan* cost information, *defined as provider remittances and enrollee cost-sharing data.*

- CBHDA recommends adding in a section identifying data exchange standards. For example, in Section 3. Data Formats, HL7 Fast Health Interoperability Resources (FHIR) is referenced as a data format, however, this is an exchange standard and in these circumstances would utilize USCDI data standards to transmit through FHIR. Additionally, other Integrating Healthcare Enterprise (IHE) initiative exchange standards still heavily in use appear to be missing or excluded for some reason (i.e. XDS.b, XCA/XCPD). For example, many health information exchange networks such as eHealth Exchange (i.e., Sequoia Project), Carequality, and EHR interoperability solutions (e.g., Epic Care Everywhere, Common Well) still extensively utilize these protocols. If the state is choosing to exclude these for some reason, it would be helpful to identify that in the DxF supporting documentation and the reasons as to why.

  Recommendation: CBHDA recommends relabeling Section 3 to Data Exchange Formats *and Exchange Standards* to promote consistency with definitions and consider adding in IHE protocols as described above.

III. DxF Components – Gaps and Opportunities

a. Technical Infrastructure and Health Information Technology (HIT) Capacity – Gap #4 Intra- and Inter Sector Data Exchange Capabilities and Opportunity #4.1

In CHHSA's discussion of HIT infrastructure, the entities identified in AB 133 are referenced including "county health, public health, and social services." However, there

[10] 85 Fed. Reg. 25510 (May 1, 2020).

is no reference to county behavioral health entities or plans. CHHSA representatives have stated that county behavioral health agencies are assumed to fall under "county health." We note that county BH plans are often administered separately from the referenced county agencies. CBHDA requests that county behavioral health agencies be specifically acknowledged in this section of the "Gaps and Opportunities."

Behavioral health providers (whether operated through counties or other private or public entities) were left out of federally Certified Electronic Health Record Technology (CEHRT) incentives, such as the Health Information Technology for Economic and Clinical Health (HITECH) Act, which prioritized hospitals and physicians. This ineligibility, coupled with historically low operating margins industry-wide, renders BH providers unable to invest in the costly technology to support the EHR adoption and data exchange necessary for care coordination. This is similar to the lack of investment in other public health systems and should be formally recognized in this analysis. While the DxF California Data Exchange Landscape discusses these historic gaps, behavioral health providers are not explicitly acknowledged as entities that continue to require significant investment and were excluded from the state-level investments proposed in the Governor's May Revision.

Under the Behavioral Health Quality Improvement Project (BHQIP), passed in last year's budget, county behavioral health departments will have an opportunity to earn incentive payments from DHCS, if they achieve certain data exchange milestones. However, the amount available statewide for counties to implement the data exchange goals under BHQIP is limited to $21.7 million across all 56 county behavioral health agencies. Providing the upfront investments necessary to access these incentive payments is further complicated by the way county behavioral health plans are financed. Unlike other delivery systems in Medi-Cal, county behavioral health agencies have had little ability to retain reserves or earmark funding for IT investments due to a cost-based reimbursement model and categorical funding restrictions. Based on preliminary estimates by individual counties, the funding currently available to counties under BHQIP will not cover the costs of existing BHQIP data exchange targets and fails to provide sufficient resources for contracted providers. Because data exchange activities are not required, counties will have no other mechanism to finance investments in the necessary data exchange infrastructure. County BH providers will need additional resources beyond BHQIP incentives to build the capacity needed to participate in meaningful data exchange under the DxF.

Recommendation: Explicitly include county behavioral health agencies and their contracted providers in the gaps analysis and ensure any resources appropriated to further facilitate the DxF explicitly include county behavioral health agencies and providers. Given the relative lack of investment in behavioral health provider IT infrastructure at the national level, it will be critical for California to ensure that sufficient funding is dedicated to behavioral health providers.

b. Data Exchange Law, Regulations, and Policy – Opportunity #1.1 and 1.2

Existing challenges with exchanging behavioral health data are acknowledged in the draft DxF Gaps and Opportunities. It is critical that the state continue to prioritize solutions for these challenges by supporting the development of a "Universal" Release-of-Information (ROI) authorization form and a viable consent management platform. Consent management solutions are prerequisites if behavioral health data is to be exchanged in a streamlined manner. These tools must be inclusive of both mental health and substance use disorder health information, including data protected under 42 CFR Part 2.

We recognize that DHCS has begun to undertake this important work to support implementation of CalAIM. Ideally, these items would have been in place before the DxF was developed and expected to be executed. Until these elements are in place, California will continue to struggle with exchanging behavioral health data, despite execution of the DxF. As county behavioral health departments have attempted to integrate care and promote data exchange, some have been hindered by more cautious interpretations of 42 CFR Part 2. A recent study mirrors our understanding of how California providers, including county behavioral health departments, continue to grapple with the balance between care coordination, patient safety, and privacy protections.[11] Given the complexity of the regulatory environment related to Part 2 and these historical challenges, we believe the development of statewide guidance on Part 2 compliant ROI and consent management would be a highly effective way to support behavioral health data sharing.

Additionally, CBHDA strongly recommends CHHSA collaborate with relevant state departments to support the development of technical assistance for providers and entities who have not historically handled specialty protected data (e.g., 42 CFR Part 2 data). The California Office of Health Information Integrity has recently developed multiple State Health Information Guidance (SHIG) volumes addressing how sensitive data can be shared under specific circumstances. Further resources should be dedicated to support implementation, including exploration of additional barriers facing providers, particularly those located in small, community based organizations.

Recommendation: Prioritize and expedite development of Universal ROI authorization form and implementation of a statewide consent management system. These tools have long been missing pieces of the data exchange puzzle that cannot easily be solved on a small-scale, local basis. Investment in these mechanisms can help promote standardization across the state and ensure more coordinated care is actualized in California. Further, CBHDA strongly recommends that CHHSA provide technical assistance to improve the collection, use, and exchange of specially protected data, including but not limited to behavioral health data.

[11] Campbell, A., McCarty, D., Rieckmann, T., McNeely, J., Rotrosen, J., Wu, L. T., & Bart, G. (2019). Interpretation and integration of the federal substance use privacy protection rule in integrated health systems: A qualitative analysis. *Journal of substance abuse treatment*, *97*, 41–46.

CBHDA appreciates the opportunity to have contributed to the Data Exchange Framework (DxF) through the workgroup process. Please feel welcome to contact Michelle Cabrera (mcabrera@cbhda.org), or Elissa Feld (efeld@cbhda.org) if we can answer questions or provide any additional information.