UNIVERSITY OF CALIFORNIA HEALTH

University of California Health
1111 Franklin Street
Oakland, CA 94607

universityofcalifornia.health



September 18, 2023

John Ohanian
Director, Center for Data Insights and Innovation Office
California Health and Human Services Agency
1215 O Street
Sacramento, CA 95814

Submitted electronically to CDII@chhs.ca.gov

**Re: Amended Policies and Procedures for Data Sharing Agreement**

Dear Mr. Ohanian:

I write on behalf of University of California Health (UCH) regarding the Data Exchange Framework Data Sharing Agreement (DSA).

UCH comprises six academic health centers, twenty health professional schools, four children's hospital campuses and a Global Health Institute. UCH hospitals are ranked among the best in California and serve over 1.8 million unique patients annually across the state.

UCH recognizes the significant work that the California Health and Human Service Agency (CalHHS) and the Data Exchange Framework Committee and Subcommittees have done to promote greater health information exchange for all Californians. Indeed, UCH supports the goals of improving health information exchange in the state and public health reporting while at the same time prioritizing the privacy and security of sensitive patient data.

UCH appreciates the revisions to the current Data Exchange Framework Policies and Procedures to address the concerns UCH has raised in its correspondence to CalHHS, comments to the Policies and Procedures, and meetings with CalHHS personnel. While meaningful progress has been made, UCH remains concerned that the current versions of the DSA and the Policies and Procedures do not optimally serve its public service mission, and that protections for the privacy and security of sensitive patient data are still needed. These concerns are highlighted below and are also set forth in the comments submitted today. We look forward to continuing to work with CalHHS to resolve these important issues.

**1. Concerns with how the data will be protected by Participants located outside of California and other actors that may not be subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or other laws protecting sensitive patient data.**

The current version of the Data Exchange Framework's draft policy on privacy and security (Privacy P&P) requires that each Participant access, use, maintain and disclose health and social services information (HSSI) "consistent with Applicable Law." This draft policy does not address the situation of a Participant that is not subject to any of the enumerated laws or is only subject to certain of them. For example, UCH in most respects is not subject to the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA). More important, UCH is subject to AB 2091 and SB 107, laws that prohibit the disclosure of sensitive medical information in response to certain subpoenas and requests. Would a Participant be limited to compliance with laws that only apply directly to it? If a Participant is subject to a law that permits or requires it to disclose records of individuals receiving an abortion, would they be able to comply even if CA law would prohibit this disclosure?

Moreover, there is no language in the policies and procedures regarding enforcement of Participants' compliance with "Applicable Law." UC Health remains concerned with respect to the lack of clarity around "Applicable Law," and requests that the Privacy P&P be modified to require that any access, use, maintenance, and disclosure of HSSI is used only as required or permitted by HIPAA, the Confidentiality of Medical Information Act (CMIA), Part 2 or other law, ***as applicable to the data itself and the originating discloser of the data***.

2. **Align Permissive Participants with the 21st Century Cures Act and HIPAA and California Law-Compliant Entities and Organizations.**

UCH continues to be concerned with the scope of Participants that may participate in the Framework and requests that CalHHS limit permissive participation to health care providers, health information exchanges, health information networks, and health IT developers of certified health IT (as all are defined under 45 C.F.R. § 171.102). All these actors are subject to the prohibition to engage in information blocking, and as acknowledged by the U.S. Office of the National Coordinator for Health Information Technology on its official website, "nearly all [information blocking] actors are HIPAA-covered entities or business associates." See Information Blocking: Eight Regulatory Reminders for October 6th (available at healthit.gov). Limiting the scope of Permissive Participants to such entities would promote consistency with federal interoperability standards.

UCH also reiterates its request that Permissive Participants be further limited to those entities who are directly subject to California law, which would largely address UCH's concerns with respect to ensuring that the Framework meets the intent of California laws, including, but not limited to AB 2091. UCH questions why additional entities and individuals would be allowed to participate in the Framework and requests information about the use cases contemplated by CalHHS. Any additional requests for an individual's HSSI by entities who are not subject to the 21st Century Cures Act can and should continue to be subject to already-established mechanisms for obtaining health information – via a patient request (and authorization) to share information with the individual or entity.

UCH recognizes that the Permitted, Required and Prohibited Policy and Procedure ("Permitted/Required/Prohibited P&P") mitigates some of UCH's concerns, in that the Policy allows UCH to refuse to provide data subject to a Permitted Request. However, this Policy puts the significant burden of vetting the legality and appropriateness of requests on the entities providing data. Moreover, technical limitations result in the inability to consistently segment sensitive data from a patient record (to respect the patient's privacy) when complying with a request from a Participant. Currently, an entire record could be flagged for review by the relevant office, but then a Participant could potentially be subject to liability for noncompliance by failing to respond to a Required request. To comply with the Permitted/Required/Prohibited P&P, signatories to the DSA would need several years to develop and modify their systems and policies, and to train users on these new systems and policies, to implement the policy. A more effective and appropriate approach would be to focus on the core goals of the Data Framework Exchange by limiting Permissive Participants as set forth above.

At minimum, we request delay (to January 31, 2026) of mandatory exchange of health data with Permissive Participants.

### 3. Lack of Clarity around "secure environment" and liability for cybersecurity breach

The current draft Privacy P&P requires that Participants use "a secure environment" that supports HSSI exchange. However, this policy does not specify what a "secure environment" entails nor what safeguards are appropriate. Organizations need to be assured that data is exchanged only between and among Participants with physical, technical, and operational security safeguards such that they can trust that the environment is secure. Accordingly, UCH requests that the Policy be revised to require a third-party review of security posture as a prerequisite of being a DSA Participant.

The draft Privacy P&P also does not provide sufficient standards for enforcement and liability with respect to breaches of HSSI. For example, if UCH shares patient data with another Participant that does not have a secure environment and there is a breach of the HSSI that would subject one Participant to breach reporting requirements and penalties, who would be liable under that instance?

UCH agrees with, and supports, the goal of the Data Exchange Framework to promote health equity within the State of California. UCH's comments and requests for clarity and revisions are rooted in a deep belief that while today's health information should be used to improve clinical outcomes for all in the future, protecting the confidentiality and security of data is critical to honor the privacy rights of the patient. UCH looks forward continued engagement with CalHHS on these important issues so that it can move forward with signing the DSA.

Sincerely,

Tam Ma
Associate Vice President
Health Policy and Regulatory Affairs