January 31, 2023

John Ohanian, Chief Data Officer and Director, Center for Data Insights and Innovation
California Health and Human Services Agency
1660 Ninth Street, Room 460
Sacramento, CA 95814

Re: Feedback on QHIO Application

Dear Director Ohanian:

Connecting for Better Health is a coalition of industry stakeholders dedicated to advancing data sharing policies in California. We appreciate the opportunity to provide input on the draft QHIO Application released in January 2023. QHIOs will be critical partners that enable many Data Sharing Agreement (DSA) signatories meet their data sharing obligations under AB 133. This letter outlines our coalition's feedback on the following topics related to the draft QHIO Application: (1) QHIOs' ability to serve all DSA signatories and required purposes, (2) cybersecurity insurance coverage, (3) security certification, and (4) data quality.

1. **QHIOs' ability to serve all DSA signatories and required purposes**

In Section C of the draft QHIO Application, CDII proposes detailing QHIOs' functional capabilities in a future draft. In anticipation of these forthcoming functional requirements, we recommend CDII ensure that QHIOs be required to serve—or demonstrate their plan to be able to serve—all likely signatories of the Data Sharing Agreement. QHIOs should be able to help any signatory comply with the current requirement to exchange health and social services information and any future modifications to CDII's policies and procedures with respect to additional signatory types.

While we recognize that serving the data sharing needs of all signatories is a large undertaking, we note that CDII has noted previously that the QHIO "…program should prioritize investments in under-resourced health and human service providers, particularly those serving high-need, low-income, and historically disadvantaged populations, seeking connection to "qualified" data

exchange intermediaries."[1] DSA Policy OPP-04 published last July also reiterates that "Participants are required to exchange…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.[2] Existing data sharing frameworks and networks primarily serve provider and hospital data sharing needs related to Treatment Purposes, leaving out the additional needs of stakeholders such as counties, social services providers, health plans including Medi-Cal Managed Care Plans, jails, behavioral health providers, public health agencies, and other entities that serve the whole person, as outlined in CDII's vision. CDII should consider adopting an amended version of the California Health Information Exchange Onboarding Program (Cal-HOP) criterion that required qualified HIOs to be "open to participation by any healthcare enterprises that serve Medi-Cal patients regardless of their business affiliations or health IT vendors,"[3] removing the reference to Medi-Cal patients and expanding the participating enterprises to include social services organizations. CDII should also strongly consider qualifying the entities previously qualified in Cal-HOP, given the significant investments the state has made in HIE onboarding to date. Ensuring that all signatories can join a QHIO will also reinforce the Data Exchange Framework and QHIO Application's focus on equity.

The development of such comprehensive capabilities complies with the requirement in AB 133 that the Data Exchange Framework remain technology neutral. Signatories will still be able to utilize non-QHIO technology tools to meet their data sharing needs, and, per the draft grant program, be able to utilize Technical Assistance Grants at the same funding level as those organizations that choose to onboard with a QHIO.

2. Cybersecurity insurance coverage

CDII has proposed that QHIOs be "insured up to $2M per incident and $5M per annum to address general liability, errors and omissions, and cyber risks" in section A of the draft QHIO Application. We recommend CDII remove the insurance requirement completely. The average cost of health

[1] CDII, Health Information Exchange in California: Gaps and Opportunities (July 5, 2022), https://www.chhs.ca.gov/wp-content/uploads/2022/07/6_CalHHS_DxF_Gaps-and-Opportunities_Final_v1_07-01-2022.pdf.
[2] CDII, CalHHS Data Exchange Framework Policy and Procedure OPP-4 (July 5, 2022), https://www.chhs.ca.gov/wp-content/uploads/2022/07/6.-CHHS_DSA-Permitted-Required-and-Prohibited-Purposes-PP_Final_v1_7.1.22.pdf.
[3] Dep't Health Care Servs., California Health Information Exchange Onboarding Program (Cal-HOP): Policies and Procedures (last updated June 30, 2021), https://www.dhcs.ca.gov/provgovpart/Documents/OHIT/Cal-HOP-Policies-and-Procedures.pdf.

care breaches has been estimated at $7 million in 2022, making this proposal inadequate to cover the costs of the average incident—the highest average cost of any industry that has risen over 40% since 2020.[4]

Instead, we recommend that CDII consider creating a pooled reinsurance program to cover the cybersecurity breach costs of QHIOs. This proposal mirrors solutions proposed by national organizations like the American Hospital Association[5] and the College of Health Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS)[6] in response to U.S. Senator Mark R. Warner's request for stakeholder feedback on the subject in 2022.[7] These stakeholders raise the concern that cybersecurity insurance is increasingly out of reach for health care organizations given the steep cost. As health care organizations, QHIOs will likely experience similar barriers to obtaining insurance, making a requirement to maintain such insurance impracticable for participation in the QHIO program.

3. Security certification

CDII has proposed requiring QHIO applicants provide information regarding recognized security certifications in section B of the draft QHIO Application. We recommend that CDII require that participants have an industry-recognized certification but not endorse a specific certification given that there are several standard certifications that could satisfy the security concerns of CDII. CDII should consider publishing a list of qualifying certifications that may include HITRUST, National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), Healthcare Sector Coordinating Council (HSCC) Recommended Security Practices, and Health Information Sharing and Analysis Center (H-ISAC), among others.

4. Data quality

---

[4] IBM Security, Cost of a Data Breach: Report 2022 (2022), https://www.ibm.com/downloads/cas/3R8N1DZJ.
[5] American Hospital Association, Letter to The Honorable Mark R. Warner RE: Cybersecurity Policy Options in the Health Care Sector (December 1, 2022), https://www.aha.org/lettercomment/2022-12-01-aha-letter-senator-warner-cybersecurity-policy-options-health-care-sector.
[6] College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS), Letter to The Honorable Mark Warner (December 1, 2022), https://chimecentral.org/wp-content/uploads/2022/12/CHIME-AEHIS-FINAL-LETTER-WARNER-1.pdf.
[7] Office of Senator Mark R. Warner, Cybersecurity is Patient Safety: Policy Options in the Health Care Sector (November 2022), https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/0320658680B8F1D29C9A94895044DA31.cips-report.pdf.

Regarding functional requirements, we also recommend CDII include a data quality requirement as part of QHIO functional and operational criteria to ensure that the data shared by QHIOs is actionable and usable by DSA signatories. We recommend CDII consider the standards outlined The Sequoia Project's Data Usability Workgroup Implementation Guide, version 1.[8] This guide covers specific use cases that health care organizations including QHINs in the Trusted Exchange Framework and Common Agreement (TEFCA) can adopt to support the usability of data. Although the implementation guide is primarily focused on clinical data sharing use cases, it does include provider-to-public health and health care entity-to-consumer information exchange use cases that can serve as a baseline for developing data quality standards in the DxF QHIO program. The guide shares these use cases to illustrate key topics including data provenance, the effective use of codes, and data integrity, among others. CDII may consider leveraging this guide and working with stakeholders to further develop use cases that involve other signatory groups like health plans, community-based organizations, and other entities required to sign the DSA.

Connecting for Better Health supports CDII's efforts to advance robust data sharing as required under AB 133 and appreciates CDII's consideration of these recommendations. We look forward to working with CDII to ensure a robust QHIO program that can support DSA signatories' data sharing needs in a secure and equitable manner. If you have any questions, please contact Robby Franceschini, Director of Policy at BluePath Health, at robby.franceschini@bluepathhealth.com.

Sincerely,

Timi Leslie
Director, Connecting for Better Health
President and Founder, BluePath Health

[8] The Sequoia Project, Data Usability Workgroup Implementation Guide Version 1.0 (December 14, 2022), https://sequoiaproject.org/wp-content/uploads/2022/12/2022-12-14-Sequoia-DUWG-IG-Version-1.pdf.