DRAFT – FOR DISCUSSION

California Data Exchange Framework
Qualified Health Information Organization (QHIO) Application 2023

Introduction. The QHIO Application 2023 has been designed to gather information to assist California's Center for Data Insights and Innovation (CDII) in determining if an organization has the structure and capabilities to function as a Qualified Health Information Organization (QHIO) in California's Data Exchange Framework (DxF). QHIOs will be identified for Data Sharing Agreement (DSA) signatories who are seeking assistance to meet their DSA obligations. Organizations interested in serving as QHIOs are encouraged to complete this application for consideration.

General Instructions. Please respond to the questions in each of the following sections:

A. Organization Information
B. Privacy and Security
C. Functional Capabilities
D. Operations

Please keep your responses brief and responsive to the question, following specific instructions with respect to the format of the response. If the response requests an attachment, please submit the attachment as a PDF file unless otherwise specified. Label the attachment with your organization name/nickname and the section/number of the question. For example, the attachment describing the corporate history of fictional applicant HealthyExchange might be labeled HealthyXChg A3. For more information, please refer to the *QHIO Application Guide 2023*.

Please note:

- All information collected by CDII as part of the QHIO Application is considered public information under the California's Public Records Act.
- Failure to respond to a question or to misrepresent the organization's capabilities will be cause for failure to receive (or subsequent removal of) Qualified status.

2023 Timeline. 2023 QHIO applications are due on or before 4:30pm PST on March 31, 2023**.** Applications received after that date and time will not be considered for review in this first cycle of the 2023 program. The next application cycle will be announced at a future date.

CDII will review the 2023 applications in April 2023, reaching out to applicants as needed for questions and clarification. Qualified HIOs will be announced on or about May 1, 2023.

A. Organization Information

1. Please complete the chart below with details regarding the organization:

Question	Response
Organization name	
Alternative names/nicknames	
Address of principal place of business	
Primary telephone number	
Primary website URL	
State/jurisdiction where incorporated	
Date of incorporation	

2. QHIOs must be registered corporations in United States. Please submit a brief letter, certificate or other form of documentation from the state where the organization is incorporated that reflects its current status (e.g., good standing). For example, organizations incorporated in California should submit a letter of good standing from the California Secretary of State.

3. QHIOs must have current business with health and/or social services organizations in California. Please submit a brief description (not to exceed 500 words) of the corporation's history, current products and services, clients, regions served, etc. Please attach a list of current clients delivering health and/or social services in California.

4. QHIOs must demonstrate the organizational infrastructure to responsibly serve DSA signatories, including a representative and participatory governance function. Please submit relevant documentation and a description (not to exceed 1,000 words) of this governance function including:
    a. Corporate documentation that provides authority to the governing body
    b. Details on eligibility to serve on the governing body and how representatives are selected
    c. Details describing how often the governing body convenes
    d. Description of the scope of decisions that the governing body is charged with
    e. Details describing how the governing body's actions are communicated to DSA signatories

5. As Participants in the DxF, QHIOs must sign the Data Sharing Agreement and attest that the agreements with current clients do not conflict with the terms of the DSA and its Policies and Procedures. Please submit an attestation indicating that the organization has signed the DSA and does not have client agreements in place that conflict with the terms of the DSA or its Policies and Procedures.

6. QHIOs who leverage the services of third parties to transmit and/or manage health and social services information must have agreements in place with these vendors that are consistent with and do not conflict with the DSA including its Policies and Procedures. If the organization leverages the services of third parties to transmit and/or manage health and social services information, please submit an attestation to indicate a valid and enforceable written agreement with that party exists that is consistent with the DSA and its Policies and Procedures. Please attach to this attestation, a list (not to exceed one page) of these third parties including their corporate name, location and the nature of the services they provide to the organization.

7. QHIOs must be financially viable companies, capable of serving DSA signatories for several years. Please provide documentation that reflects the financial health of the organization. This may include one or more of the following documents:
    a. Internal Revenue Service Form 990 for the most recent year
    b. Audited financial statements financial statements for the most recent year
    c. An auditor's attestation that indicates the organization is financially stable with fiscal resources to support operating as a QHIO without placing financial strain on the rest of the organization and available cash (or cash equivalents) equal to at least six months of operating expense

8. QHIOs must be insured up to $2M per incident and $5M per annum to address general liability, errors and omissions, and cyber risks. Please submit documentation of insurance coverage.

9. Please complete the chart below with the name, title, phone and email of the organization's contacts. In the first column, please flag the primary contact for communication regarding this application.

*	Contact	Response
	Executive *(name, title, phone, email)*	
	Technical *(name, title, phone, email)*	
	Operations *(name, title, phone, email)*	

B. Privacy and Security

QHIOs will play an important role in establishing and maintaining trust in the DxF. Thus, each QHIO must have robust structures and processes in place to protect the privacy and security of health and social services information. Please submit the following documentation on the organization's privacy and security practices:

1. A brief summary (not to exceed 500 words) of the organization's information security program.

2. An organizational chart that reflects the structure of the information security team, including the Chief Information Security Officer (CISO) and his/her reporting relationships. Please indicate if the CISO is a full-time or part-time role.

3. A one-page list of the information security policies and procedures maintained by the organization, including the date each policy was last reviewed or updated.

4. A list of nationally recognized security certifications received by the organization. (If your technical infrastructure is managed by a third party, please include that party's security certifications. This may include one of the following certifications:

    - HITRUST Risk-based, 2-year (r2) Validated Assessment
    - EHNAC accreditation

    If certification has not been achieved at the time of application, please submit a brief description (not to exceed 500 words) of the efforts underway to achieve recognition with a nationally recognized programs and the expected completion date.

5. An attestation that indicates no Protected Health Information (PHI) or Personally Identifiable Information (PII) managed by the organization, or its subcontractors, is transmitted or stored outside of the United States.

6. A one-page summary of any HIPAA-reportable breaches over the past three years including the nature of the breach, the number of individuals affected by the breach, the remediation measures taken, and the amount of any fines or penalties.

7. A one-page summary of the organization's approach to security risk assessments including the frequency with which third-party security risk assessments are conducted. Please also attach documentation (e.g., an invoice, a dated assessment cover page) of the most recent such assessment and a brief summary (not to exceed 500 words) describing actions taken to address any vulnerabilities identified.

8. A one-page summary of the organization's approach to penetration testing including the frequency with which third-party penetration testing is conducted. Please also attach documentation (e.g., an invoice, a dated assessment cover page) of the most recent such test and a brief summary (not to exceed 500 words) describing actions taken to address any vulnerabilities identified.

9. The organization's current privacy policy including the most recent date it was reviewed and updated.

10. A brief summary (not to exceed 500 words) of the organization's business continuity and disaster recovery plans. Please attach the table of contents, revision history and management approvals for each plan.