DIBBs Query Connector

Query Connector IT Guide

Created Date: January 14, 2025

Last Updated: June 4, 2026

Prepared by:

U.S. Department of Health and Human Services

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR DISEASE CONTROL AND PREVENTION

This document has been developed by Skylight under a contract with the U.S. Centers for Disease Control and Prevention – Department of Health and Human Services.

Version History

Version	Author	Reviewed By	Revision Date	Revision Notes
1.0	Matthew Goldberg	Maya Mascarenhas	04/17/2026	
1.1	Matthew Goldberg	Maya Mascarenhas	06/04/2026	

This document has been developed by Skylight under a contract with the
U.S. Centers for Disease Control and Prevention – Department of Health and Human Services.

Table of Contents

This document has been developed by Skylight under a contract with the
U.S. Centers for Disease Control and Prevention – Department of Health and Human Services.

To contact the Query Connector team, email dibbs@cdc.gov

1 Objective

This guide provides the information IT teams need to evaluate, approve, and deploy Query Connector within their jurisdiction.

2 Product overview

Query Connector is a free, open-source application offered by CDC that lets public health jurisdictions securely query Fast Healthcare Interoperability Resources® (FHIR®)[1] APIs at healthcare organizations (HCOs) and health information exchanges (HIEs) to efficiently retrieve patient data.

3 Use case

By streamlining data exchange between public health jurisdictions and healthcare systems, Query Connector:

1. **Reduces manual burden.** Improves workflows for public health case investigators by replacing the process of collecting patient data by individual searches via portal, phone, email, or fax
2. **Increases speed of data queries.** Gives public health staff immediate access to patient data relevant to their specific use case
3. **Protects patient privacy.** Only requests the minimal data necessary and implements role-based permissions to manage who can request and access the data

Collectively, the reduced manual burden and increased query speed helps public health staff more effectively do case investigations and manage public health responses.

4 Core components

Query Connector consists of four main parts:

1. The app itself, a Next.js application bundled as a Docker container

[1] [1] *Disclaimer: HL7®, and FHIR® are the registered trademarks of Health Level Seven International and the use of these trademarks does not constitute an endorsement by HL7.*

This document has been developed by Skylight under a contract with the U.S. Centers for Disease Control and Prevention – Department of Health and Human Services.

2. A PostgreSQL database that stores basic information and configuration for the app
3. An Identity Provider (IdP) that manages user authentication; while the app typically integrates with an organization's existing IdP, one must be available to ensure secure access
4. A FHIR server that will respond to queries

As the person or team deploying Query Connector, you're responsible for managing the core application, the database, and the integration with an identity provider (either your organization's existing IdP or by establishing one). Regarding data access, your Query Connector instance must be registered as a client. This can be done directly with a specific data provider or through an HIE (such as eHealth Exchange) to enable broader access across multiple providers.

5 Deployment model and data ownership

Each public health jurisdiction deploys and operates its own instance of Query Connector on infrastructure it controls, either on-premises or in its cloud environment.

Query Connector integrates with a jurisdiction's existing identity provider via OAuth, allowing staff to authenticate using existing credentials (such as Microsoft Entra or Keycloak), with no separate Query Connector–specific accounts required.

As a result:

- Public health jurisdictions own all data associated with their instance
- CDC does not have access to jurisdictional data
- Data residency requirements are easily met by deploying in U.S. cloud regions or on-premises

6 Deploying the app

Query Connector is a relatively lightweight application with two deployment options:

- **Docker container**, which lives in GitHub Container Registry here
- **Virtual machine**, with a VM image you can deploy on your hypervisor of choice

Both options are straightforward, and once you have identified the right technical leads, your team can independently manage the installation and integration process at your own pace.

For more detailed information on deployment, see Query Connector Deployment Guide.

This document has been developed by Skylight under a contract with the
U.S. Centers for Disease Control and Prevention – Department of Health and Human Services.

7 Database

Query Connector requires a PostgreSQL database to store configuration data, value sets, user management, and audit logs. For test or QA environments, the database may run alongside the app in the same VM, but for production we recommend a managed PostgreSQL service.

8 Identity integration:

Query Connector uses your existing identity provider, so there's no need to create or manage new user accounts. We currently support:

- **Microsoft Entra** (formerly Azure Active Directory)
- **Keycloak**
- **PingFederate**

Support for additional OAuth-compatible providers may be possible depending on our team's current capacity. Please reach out if you have specific requirements.

9 Security

Query Connector is designed to minimize data exposure. The application does not retain source patient health data or downstream query results (e.g., Protected Health Information (PHI)).

The application database contains only query templates, configuration data, and audit logs used for oversight. Audit logs may contain Personally Identifiable Information (PII), depending on what users include in their queries.

Recommended security controls include:

- **Network security:** Deploy behind a reverse proxy or load balancer, enforce SSL/TLS, use network segmentation, and enable WAF protection
- **Access controls:** Use Query Connector's built-in role-based access controls and regularly audit user permissions
- **Compliance:** Ensure deployments meet applicable regulatory requirements (such as HIPAA where relevant), use Query Connector's built-in audit logging for keeping a log of all patient data access, and implement appropriate data retention policies

This document has been developed by Skylight under a contract with the
U.S. Centers for Disease Control and Prevention – Department of Health and Human Services.

10 Support and ownership

Your jurisdiction retains full operational control of its Query Connector deployment. The CDC DIBBs team provides implementation guidance, documentation, and support for setup and troubleshooting. For questions or assistance, contact dibbs@cdc.gov.

This document has been developed by Skylight under a contract with the U.S. Centers for Disease Control and Prevention – Department of Health and Human Services.