URGENT!
Please populate & return the Excel checklist asap!
1 YOU ASKED, WE LISTENED

Since its inception as a U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC) initiative, the eHealth Exchange has evolved from a pioneer network connecting federal agencies, private sector providers, and state/regional health information networks, to become the largest, broadest, nationwide network with over 200 health systems, four federal agencies, 59 state and regional Health Information Networks, and other health care organizations using a wide variety of vendor platforms. We exchange an estimated 200,000 million clinical documents annually in all 50 states.

Due to dramatic growth over the past ten years, eHealth Exchange Participants (such as your organization) requested the eHealth Exchange introduce a new solution to:

- Reduce the complexity and expense associated with exchanging patient data
- Further expand the network’s nationwide reach
- Lay the foundation to provide compelling new capabilities

In response, the eHealth Exchange Coordinating Committee prioritized the development of a strategic roadmap to maximize value and support sustainable growth. The process included identification of market needs, evaluation of market forces, consideration of potential new use cases, and a thorough assessment of the current federated architecture’s ability to support future growth.

A summary illustration of the innovative strategic roadmap is illustrated below:
As a result of the roadmap exercise and evaluation of the federated architecture, the Coordinating Committee approved as a first priority, enhancing the current eHealth Exchange architecture by implementing a centralized platform solution to be known as the “Hub”. To accelerate adoption, the Veterans Health Administration (VHA) will be one of the Hub early adopters.

The Veterans Health Administration (VHA) plans to be a Hub early adopter
1.1 What’s Changing?

The eHealth Exchange is deploying an innovative new national data exchange technology platform, an integration of the eHealth Exchange FHIR Healthcare Directory with Intersystems’ HealthShare-as-a-Service (HaaS), where a single connection from your organization to the eHealth Exchange Hub will provide your organization a:

- Simpler, less expensive way to exchange within our nationwide eHealth Exchange network
- Simple, inexpensive solution to exchange patient information with healthcare organizations who are not part of the eHealth Exchange network, but who exchange within other networks such as Carequality-enabled networks
- Connection with the Patient Unified Lookup System for Emergencies (PULSE) platform to facilitate patient care during disasters
- Platform to facilitate future potential capabilities

Instead of each eHealth Exchange Participant creating and maintaining a separate connection with eHealth Exchange Participants, your organization is now asked to create a single connection to the eHealth Exchange Hub so the Hub can connect Participants to one another.

The Hub can also connect your organization to Carequality-enabled networks beyond the eHealth Exchange if your organization does not already have this access.
1.2 Why Are We Doing This?

Today’s “federated” architecture (see illustration above) has served us well over the past ten years connecting the United States. As interoperability expands and matures, we all need a simpler, less expensive way to connect to more healthcare organizations to support an expanding list of use cases and to broaden Participants’ reach to new exchange partners.

Your organization will have a single point of entry to connect nationwide

1.2.1 Scalability within eHealth Exchange Network

Asking each eHealth Exchange Participant to create and maintain separate connections with other eHealth Exchange Participants is expensive and duplicative. In contrast, with the Hub, once your organization creates a single connection to the eHealth Exchange Hub, the Hub will connect your organization to other eHealth Exchange Participants. As a result, your organization’s interoperability cost and effort will decrease.

One Connection to eHealth Exchange Participants
1.2.2 Scalability with Additional Networks
The Hub can connect your organization to additional networks beyond the eHealth Exchange such as Carequality-enabled networks. If you do not already have Carequality access, with your single connection to the eHealth Exchange Hub, your organization could be connected to Carequality-enabled networks such as CommonWell, AthenaNet, eClinicalWorks, NextGen, Epic Care Everywhere, and many others.

One Connection to Carequality Participants

1.2.3 PULSE Disaster Response
To improve patient care, the Hub will be integrated with the Patient Unified Lookup System for Emergencies (PULSE) platform. PULSE was initially developed by the Office of the National Coordinator (ONC) for Health IT to provide secure health data exchange during emergencies for use by credentialed volunteer clinicians in disaster response settings such as school gyms, church cafeterias, and even tents. As PULSE is integrated with the eHealth Exchange hub, it will be rolled out nationally.

1.2.4 Technology Platform for New Capabilities
See section 5.
1.3 What are the Benefits?

The eHealth Exchange Hub provides a number of benefits including operational efficiencies, lower cost, data transparency, and improved patient care. The Hub will also allow the network to expand its reach and will serve as the building block for future enhanced services. Utilizing the centralized Hub will require fewer connections to implement and maintain, a lower support effort, and will enable more meaningful exchange. Additional details are highlighted below:

- **Expand Reach While Lowering Cost:** eHealth Exchange Participants need access to broader network connections, including acute care, ambulatory, payer networks, and behavioral health. Utilizing the centralized Hub will require fewer connections to implement and maintain, a lower support effort, and will enable more meaningful exchange. The Hub is designed to provide single connection to up to 250 Participants & 12+ diverse Carequality networks.

- **Disaster Response:** The Patient Unified Lookup System (PULSE) is a system that pulls patient histories for credentialed volunteer clinicians working in alternative care facilities (tents, shelters, churches) during and after disasters. The eHealth Exchange Hub will likely be leveraged by the PULSE disaster response system to query for patient records.

- **New Capabilities:** Currently, Participants are able to query for data when they already know where care has been delivered elsewhere and the volume of information that is returned can prove to be difficult to search through. With the Hub, Participants will have access to a Record Locator Service (RLS) via Carequality for additional fees and in the future, the ability to push CDAs & discrete data along with support for FHIR.

- **Reduces Cybersecurity Risk:** The Hub is expected to reduce the “attack surface area” from multiple direct connections to a single connection which is much easier to defend and manage than 250+ individual connections. The Hub can also mitigate the risk from...
Hub Information & To Do List

a Participant that can be misconfigured in terms of FIPS, cipher suites allowed, NIST guidelines, IT best practices, firewall rules, digital signature validation, digital (private) key management, etc.

1.4 Who Selected the Hub?

To select a vendor to provide the necessary technology that would integrate with the eHealth Exchange FHIR Healthcare Directory, a formal Request for Proposal (RFP) process was managed by eHealth Exchange staff with significant input from a formal Participant Workgroup. The Workgroup included Non-Federal Participant representatives from community health systems, academic health systems, pediatric providers, payers, HIEs, pharmacies, and dialysis providers. Federal Participants included the VHA, Social Security Administration (SSA), and Department of Defense (DoD). The Workgroup evaluated and score the responses using objective criteria, unanimously recommending Intersystems’ HealthShare-as-a-Service (HaaS).

1.5 What will the Hub do?

Beyond connecting your organization’s gateway to the eHealth Exchange Hub and utilizing the Hub to exchange data with other Participant gateways, the initial implementation of the Hub will include current core operational services such as PKI certificate testing and operational monitoring activities. The Hub’s support staff will assess Participant system availability and performance. The Hub will provide significant enhancements to the existing transport testing and operational monitoring services that are currently implemented within a federated architecture since eHealth Exchange support staff will be able to perform these activities with direct access to each Participant’s endpoint. Enhanced services include:

- **Production-level transport and surveillance**: eHealth Exchange support staff will conduct periodic testing that validates that a configured production instance of a system operates in production with Participants. This will include a testing service that enables bidirectional testing of transport and security in the eHealth Exchange production environment and verifies that systems used for production-level exchange comply with eHealth Exchange specifications related to transport and security.

- **Operational Monitoring**: eHealth Exchange support staff will develop mutually defined Service Level Agreement (SLA) and provide enhanced capabilities such as a real-time
performance dashboard that will allow Participants to know immediately, whether trading partner gateways are up and responsive according to the SLA. Staff will remediate performance issues through the appropriate channels with eHealth Exchange Participants, informal issue resolution and, if escalated, via the eHealth Exchange dispute resolution process.

1.6 How Will Data Flow?

The Hub will not store data in a longitudinal central data repository, but will store audit logs as required for information security and regulatory compliance. Messages will simply pass through the Hub as the Hub directs your requests to the desired trusted location.

How does the Hub work?

1.7 How Does Hub Security Work?

The eHealth Exchange has applied its secure by design architecture, Federal Bridge Certification Authority (FBCA) operational policies and procedures, a leading edge PKI production assessment process, an associated validation program, and Sequoia Project innovations. Details are provided in Appendix A.
2 WHAT IS THE LIKELY TIMELINE?

While a few early adopters such as the Veterans Health Administration (VHA) have slightly more accelerated timelines, most Participants will connect to the Hub as follows:

**May 30, 2019**
Sign amended Participation agreement

**April 30, 2019**
Return checklist

**Early July 2019**
Expect the Hub’s test harness to initiate a query to Participants’ gateways for the test patient coordinated for use

Most Participants can be live responding to queries originated via the Hub

**August 2019**
Each Participant initiates a test query to the Sequoia Interoperability Platform (ITP)’s home community ID (HCID) with the Hub’s Responding Gateway (RG) endpoint to make their connection bi-directional.

Most Participants can be live initiating queries to the Hub instead of using point to point

**September 2019**
The Hub’s implementation team helps remediate any issues

**October 2019**
Help prioritize new capabilities for the eHealth Exchange
3 Carequality Timing

Once the 9/30/2014 version of the Data Use and Reciprocal Support Agreement (DURSA) is amended by Participants such as your organization to allow the Coordinating Committee to enter into agreements to broaden connectivity across platforms and networks, the eHealth Exchange plans to become a Carequality Implementer. We hope this is accomplished by mid-2019.

This milestone will **not** impact Participants who already have access to Carequality such as health systems running Epic. This also will **not** impact Participants who choose to opt-out of connecting to Carequality via the eHealth Exchange after the DURSA is amended to allow the Coordinating Committee to sign the Carequality Connected Agreement.

Participants connecting to Carequality-enabled networks via the eHealth Exchange will be able to exchange with an additional 12 networks such as AthenaNet, CommonWell, eClinicalWorks, NextGen, Epic CareEverywhere, etc. Instead of these organizations building and maintaining the required 350+ connections via 350+ point-to-point connections, your **single** connection to the Hub will provide this connectivity.

4 What Do I Need to Do?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Return populated Excel Checklist</td>
<td>So the Hub implementation team understands:</td>
<td>Return via email to <a href="mailto:administrator@ehealthexchange.com">administrator@ehealthexchange.com</a></td>
<td>By April 30, 2019</td>
</tr>
<tr>
<td></td>
<td>• Which test patients &amp; environments your organization uses</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• firewall considerations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Current contacts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.2 Return signed agreement (see Appendix B for)</td>
<td>So your organization can be setup to initiate messages via the Hub instead of</td>
<td>Return via email to <a href="mailto:administrator@ehealthexchange.com">administrator@ehealthexchange.com</a></td>
<td>By May 30, 2019</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>contract change highlights)</td>
<td>maintaining multiple, expensive point to point connections.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>So your organization has access to powerful information regarding</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>how it exchanges information with other healthcare organizations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.3 Attend Hub information</td>
<td>To learn the basics regarding this new connectivity approach.</td>
<td>Register at <a href="https://ehealthexchange.org/events">https://ehealthexchange.org/events</a></td>
<td>Typically:</td>
</tr>
<tr>
<td>meetings</td>
<td>To ask questions.</td>
<td></td>
<td>• Tuesdays at 1ET &amp;</td>
</tr>
<tr>
<td></td>
<td>To collaborate with the eHealth Exchange community.</td>
<td></td>
<td>• Thursdays at 4ET</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Beginning 4/11/2019</td>
</tr>
<tr>
<td>4.4 Expect a Message to Your</td>
<td>To confirm your system is ready to respond to queries originated by</td>
<td>The Hub implementation team will contact your organization to notify</td>
<td>Early July</td>
</tr>
<tr>
<td>Gateway from the Hub’s Test</td>
<td>other eHealth Exchange Participants that are routed via the Hub.</td>
<td>you it plans to initiate a test message using the test patient agreed</td>
<td></td>
</tr>
<tr>
<td>Harness</td>
<td></td>
<td>upon.</td>
<td></td>
</tr>
<tr>
<td>4.5 Connect to the Hub as an</td>
<td>To confirm your organization can send patient searches to other</td>
<td>1. <strong>Configure</strong> your system to use the new Hub-Aware directory</td>
<td>August</td>
</tr>
<tr>
<td>Initiating Gateway</td>
<td>Participants via the Hub and receive</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>requested clinical documents.</td>
<td></td>
<td>2. <strong>Initiate</strong> a test query to the Sequoia Interoperability Testing Platform (ITP)’s Home Community ID (HCID) with the Hub’s endpoints</td>
<td></td>
</tr>
</tbody>
</table>

**4.1 Return the Excel Checklist ASAP**

Please return a populated Hub Connectivity Excel Checklist to administrator@ehealthexchange.com no later than April 30, 2019. The checklist should be quick and easy to populate.

**4.2 Sign the Amended Participation Agreement**

Please return a signed amended Participation agreement before May 30, 2019 to administrator@ehealthexchange.com so:

- Your organization can be setup to initiate messages via the Hub instead of maintaining multiple, expensive point to point connections.
- Your organization has access to powerful information regarding how it exchanges information with other healthcare organizations.

**4.3 Attend Hub Information Meetings**

Attend Hub information web meetings to learn the basics regarding this new connectivity approach, to ask questions, and to collaborate with the eHealth Exchange community.

- Typically Tuesdays at 1pm ET & Thursdays at 4pm ET for an hour
- Register at https://ehealthexchange.org/events
4.4 Expect a Message to Your Gateway from the Hub’s Test Harness to Connect Your Organization as a Responding Gateway

In late June, the Hub implementation team will contact your organization to notify you we plan to initiate a test message using the test patient we agree upon via the Excel checklist you return. If your system successfully matches the test patient and returns a clinical document, we’ll know your system is ready to respond to queries originated by other eHealth Exchange Participants that are routed via the Hub. Unless your organization maintains firewall whitelisting as described in the Excel checklist, you shouldn’t have to do anything to respond to queries routed via the Hub. If your organization maintains a Firewall “whitelist” limiting inbound messages to a specific list of trusted IP addresses, then please configure your firewall asap to trust messages originating from the Hub’s IP addresses:

1. LIVE/PROD IP Address: 164.52.129.167
2. UAT/VAL IP Address: 164.52.129.166
3. LIVE/PROD Failover IP Address: 74.209.254.145
4. UAT/VAL Failover IP Address: 74.209.254.144

<table>
<thead>
<tr>
<th>eHealth Exchange’s Preferred Approach</th>
<th>Setup Approaches as Responding Gateway (RG)</th>
<th>Environment</th>
<th>Patient</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Choice</td>
<td>The Hub’s Test Harness initiates a query to your gateway for the test patient you have active in your Production environment.</td>
<td>Production or Validation</td>
<td>Test Patient</td>
</tr>
<tr>
<td>2nd Choice</td>
<td>Another eHealth Exchange Participant initiates a query to your gateway for a real common patient you have active in your Production environment, as appropriate.</td>
<td>Production</td>
<td>Real Common Patient</td>
</tr>
</tbody>
</table>
4.5 Connect to the Hub as an Initiating Gateway

Finally, after your organization is successfully setup as a Responding Gateway (RG), we’ll leverage the Sequoia Interoperability Testing Platform (ITP) to serve as a test Responding Gateway (RG).

The Sequoia Interoperability Testing Platform (ITP) will simulate a responding Participant connected to the Hub by matching to your patient and responding to your organization’s query with a clinical document. Your organization will be asked to initiate a test query destined for the ITP, routed via the Hub, with the goal of retrieving a clinical document from ITP gateway using a test patient.

The Hub Implementation team will instruct you:

- To initiate a query to the Sequoia Interoperability Testing Platform (ITP)’s Home Community ID (HCID) with the Hub’s endpoints. The ITP will then hopefully match to your patient and respond to your organization’s query with a clinical document.

- To configure your system use the new Hub aware directory with the Hub’s Responding Gateway (RG) endpoints, so the ITP can hopefully match to your patient and return a clinical document.

4.5.1 How would I configure my gateway to initiate queries to route via the Hub?
4.5.2 Sequoia ITP’s Home Community ID (HCID)

Sequoia ITP’s Validation Home Community ID (HCID)

After your organization has been setup to respond to queries other Participants route via the Hub, the Hub implementation team will provide you a Sequoia Interoperability Platform (ITP) Validation environment Home Community ID (HCID) unique to your organization. You'll then be asked to initiate a query to the Sequoia Interoperability Platform (ITP) Home Community ID (HCID) using the Hub's endpoints to confirm your organization can send patient searches to other Participants via the Hub and receive a requested clinical document.

4.5.3 Directory

If your organization initiates requests to the Hub to retrieve patient information from other Participants, even if some of the responding Participants are not yet connected to the Hub, configure your system to use the new Hub-aware directory.

1.1 The eHealth Exchange recommends that your system utilize one directory at any given time. Although it may be possible to consume both eHealth Exchange directories with additional application client logic, there is no known reason to do this.

1.2 If your organization initiates requests to the Hub to retrieve patient information from other Participants, even if some of the responding Participants are not yet connected to the Hub, use the new Hub-aware directory.

- The hub-aware directory provides Home Community IDs (HCIDs) and Hub endpoints for Participants connected to the Hub, while also providing HCIDs and traditional point to point endpoints for Participants not yet connected to the Hub, so that communication can be routed directly to the Participants.

Technical note: To initiate requests through the Hub, the directory publishes HCIDs and Hub endpoints for Participants connected to the Hub. Once a request is received by the Hub, it is routed to the appropriate Participant by looking up the traditional point to point endpoints by the Participant’s HCID. For that reason, it is important that the traditional eHealth Exchange directory is maintained and updated with your organization’s point to point endpoints.
• The Hub-aware directory is recommended to initiate requests to Participants since the Hub is trusted by the corporate firewalls some participants use to filter network traffic. In addition, requests sent through the Hub will be monitored and added to a dashboard for your review.

1.3 If none of the Participants you query have yet onboarded to the Hub as a Responding Gateway, then you have the option to continue to use the Legacy UDDI Directory and continue your point to point connections. But if any of the Participants you query has onboarded to the Hub as a Responding Gateway, please use the Hub-aware Directory.

If your organization does not initiate requests via the Hub with 1 Participant, assuming your organization and that Participant have mutually agreed to continue using point to point connections, continue using the traditional eHealth Exchange directory.

1.4 To configure your system from using the traditional eHealth Exchange directory to the new Hub-enabled directory, consult your vendor if you are unsure how to accomplish this.

• Switching directories typically involves simply entering the new Hub-enabled directory’s Production and Validation URLs.

• Both the legacy and Hub-aware directories have two available interfaces using either SOAP or FHIR APIs.

• Currently, both the SOAP and FHIR APIs have access to the same directory information, but in the near future, FHIR capabilities may be expanded beyond those of SOAP. For example, once Carequality Implementers connect to the Hub, the SOAP directory API will only show one connection for a majority of the Carequality Implementers. However, the FHIR directory API will show a top-level connection for the Carequality Implementer and additional information for each Carequality Connection.

4.5.4 Hub Endpoint URL Naming Convention

The Hub endpoint URLs are based on the following naming convention (bold = static value, <label> = required variable value, [,_eHxHubTimeout=<integer seconds>]=optional parameter):

hub<environment><incrementor>.ehealthexchange.org/<Sequoia initiative>/<hub version>/<IHE ITI transaction id>/<transaction version>/?_eHxHubRouteTo=<OID in dotted decimal format>[&_eHxHubTimeout=<integer seconds>]

If your organization does not initiate requests via the Hub with 1 Participant, assuming your organization and that Participant have mutually agreed to continue using point to point connections, continue using the traditional eHealth Exchange directory.
### Hub Information & To Do List

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;incrementor&gt;</code></td>
<td>001</td>
<td>For future use. Initial value will be “001”.</td>
</tr>
<tr>
<td><code>&lt;environment&gt;</code></td>
<td>“val” or “prod”</td>
<td>Specifies the environment.</td>
</tr>
<tr>
<td><code>&lt;Sequoia initiative&gt;</code></td>
<td>&quot;ehx&quot; or &quot;cq&quot;</td>
<td>Different endpoints for eHealth Exchange and Carequality participants to use: eHealth Exchange Participants should direct their requests to &quot;ehx&quot; Carequality Implementers should direct their requests to &quot;cq&quot;</td>
</tr>
<tr>
<td><code>&lt;hub version&gt;</code></td>
<td>1.0.0</td>
<td>Version of the Hub. Can be used to differentiate (potential) parallel implementations of multiple Hub versions.</td>
</tr>
<tr>
<td><code>&lt;IHE ITI transaction id&gt;</code></td>
<td>iti##</td>
<td>Initial values limited to (iti55, iti56, iti38, iti39)</td>
</tr>
<tr>
<td><code>&lt;transaction version&gt;</code></td>
<td>2.0, 3.0</td>
<td></td>
</tr>
<tr>
<td><code>?_eHxHubRouteTo=&lt;OID in dotted decimal format&gt;</code></td>
<td>HCID OID</td>
<td>The value matches the home community ID of the participant. The Hub will use the parameter value to route the request to the appropriate responding gateway. This value will be populated by the directory administrator and should not be modified by participants.</td>
</tr>
<tr>
<td><code>&amp;_eHxHubTimeout=&lt;integer seconds&gt;</code></td>
<td>5 to 600</td>
<td>This optional querystring parameter can be added to the endpoint in order to override the Hub default timeout. The timeout value should be represented in seconds and be in the range of 5 to 600. With default Hub timeouts, when your system initiates queries, the Hub allows your system to wait: up to 120 seconds for Patient Discovery messages up to 120 seconds for Query for Documents messages up to 300 seconds for Retrieve Documents messages</td>
</tr>
</tbody>
</table>

#### 4.5.5 Hub Endpoint URLs

The following endpoints are for use by eHealth Exchange Participants only. Gateways that are part of Carequality, but are not part of the eHealth Exchange (e.g. CommonWell and AthenaNet) are provided a different set of endpoints.

**Cross Gateway Patient Discovery**

hub001val.ehealthexchange.org/ehx/1.0.0/iti55/2.0?_eHxHubRouteTo=<HCID OID>

hub001prod.ehealthexchange.org/ehx/1.0.0/iti55/2.0?_eHxHubRouteTo=<HCID OID>

**Cross Gateway Patient Discovery (deferred/asynchronous)**

hub001val.ehealthexchange.org/ehx/1.0.0/iti55async/2.0?_eHxHubRouteTo=<HCID OID>

hub001prod.ehealthexchange.org/ehx/1.0.0/iti55async/2.0?_eHxHubRouteTo=<HCID OID>

**Cross Gateway Query**

hub001val.ehealthexchange.org/ehx/1.0.0/iti38/3.0?_eHxHubRouteTo=<HCID OID>

hub001prod.ehealthexchange.org/ehx/1.0.0/iti38/3.0?_eHxHubRouteTo=<HCID OID>
Cross Gateway Retrieve

hub001val.ehealthexchange.org/ehx/1.0.0/iti39/3.0?_eHxHubRouteTo=<HCID OID>
hub001prod.ehealthexchange.org/ehx/1.0.0/iti39/3.0?_eHxHubRouteTo=<HCID OID>

NOTE: An optional "_eHxHubTimeout " query string parameter is supported to allow an Initiating Gateway to override the Hub default timeout values. If provided, this parameter value should be represented in seconds and be in the range of 5 to 500. Further guidance is provided in the “Hub Endpoint URL Naming Convention” section above.

4.5.6 Hub Ports

The Hub supports ports 443 (designated as the "primary port"), port 4437 (designated as the "secondary port"), and port 14430 (designated as the "tertiary port"). Port 443 is recommended since 443 is generally accepted by security teams as a standard SSL/TLS port.

5 MUST MY ORGANIZATION CONNECT TO THE HUB?

If your organization exchanges via the eHealth Exchange with any other eHealth Exchange Participant for Treatment purposes, your organization has a Duty to Respond to all other eHealth Exchange Participants exchanging for Treatment, even if their queries arrive infrequently from distant regions, and even if information cannot be provided.

Creating 1 connection to the Hub is much more practical than creating and maintaining connections with over 250 other gateways who exchange for Treatment.

Your organization can fulfill this DURSA obligation to exchange for Treatment by either:

- Creating 1 connection to the eHealth Exchange Hub to connect with other Participants exchanging for Treatment, or

- Mutually-agreeing with other Participants exchanging for Treatment to maintain direct point-to-point connections. Importantly, your organization may not require another Participant who has implemented the HUB to spend resources to establish or maintain direct point-to-point connections with it.
Not only will the Hub simplify Query & Retrieve exchange, it will provide the building blocks for future potential capabilities such as:

- PDMP exchange
- FHIR queries for discrete data resources such as Problems, Allergies, Medications, Immunizations, or Lab Results
- Pushing data
- Image Exchange
- In-line content quality assurance
- Population-level exchange

### Potential Future Hub Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FHIR</td>
<td>Participants connecting to Carequality via the eHealth Exchange could leverage this optional service.</td>
</tr>
<tr>
<td>RLS</td>
<td>Optional service randomly running Partner CDAs through the Content Validation test scripts.</td>
</tr>
<tr>
<td>Quality Scans</td>
<td>Optional service that combines multiple CDAs for a given patient.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Optional service automatically pushing unsolicited CDAs via IHE XDR (or perhaps via XDS.b).</td>
</tr>
<tr>
<td>Push</td>
<td>Patient Matching Optional service</td>
</tr>
<tr>
<td>Patient Matching</td>
<td>ADT Notifications Optional service</td>
</tr>
<tr>
<td>ADT Notifications</td>
<td>tbd</td>
</tr>
<tr>
<td>tbd</td>
<td>Above and beyond reliance upon the existing Sequoia Project FHIR directory, we hope to begin offering additional FHIR capabilities for meds problems, allergies, vitals, &amp; lab results.</td>
</tr>
</tbody>
</table>
7 **How Much Will the Hub Cost My Organization?**

To minimize adoption impediments, align with the proposed Information Blocking rule, align with the drafted Trusted Exchange Framework, position state & regional Health Information Networks for success, and support Federal Partners’ goals:

- There will be no charge for any Participant to respond to queries other Participants have routed to the Hub
- 95% of eHealth Exchange Participants will not be asked to pay any new fees to initiate queries with other Participants routed to the Hub

Instead, to cover a portion of the eHealth Exchange’s vendor fees, an annual Hub technology fee will be charged to the Participants exchanging the most since they receive the most benefit by no longer having to maintain so many point to point connections.

---

**No charge for Participants to Respond to queries routed through the Hub**

<table>
<thead>
<tr>
<th>Participant Type</th>
<th>Fee to Respond to Queries Routed Through the Hub</th>
<th>Fee to Initiate Queries Routed Through the Hub</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Systems, HIOs, &amp; Other Providers Operating in &lt; 5 States</td>
<td>$0*</td>
<td>$0*</td>
</tr>
<tr>
<td>Health Systems, HIOs, &amp; Other Providers Operating in 5 or More States with Annual Revenue or Expenses Under $500M</td>
<td>$0*</td>
<td>$0*</td>
</tr>
<tr>
<td>Health Systems, HIOs, &amp; Other Providers Operating in 5 or More States with Annual Revenue or Expenses Between $500M - $3B</td>
<td>$0*</td>
<td>$60,000 Annually (In addition to Annual Network Participation Fee)</td>
</tr>
<tr>
<td>Health Systems, HIOs, &amp; Other Providers Operating in 5 or More States with Annual Revenue or Expenses Over $3B</td>
<td>$0*</td>
<td>$110,000 Annually (In addition to Annual Network Participation Fee)</td>
</tr>
<tr>
<td>Payers and Vendors Retrieving &lt; 500K Documents Annually</td>
<td>$0*</td>
<td>$150,000 Annually (In addition to Annual Network Participation Fee)</td>
</tr>
</tbody>
</table>
### Hub Technology Fees to Exchange Within eHealth Exchange Network

<table>
<thead>
<tr>
<th>Participant Type</th>
<th>Fee to Respond to Queries Routed Through the Hub</th>
<th>Fee to Initiate Queries Routed Through the Hub</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payers and Vendors Retrieving 500K to 999K Documents Annually</strong></td>
<td>$0*</td>
<td>$250,000 Annually (In addition to Annual Network Participation Fee)</td>
</tr>
<tr>
<td><strong>Payers and Vendors Retrieving &gt; 1M Documents Annually</strong></td>
<td>$0*</td>
<td>$400,000 Annually (In addition to Annual Network Participation Fee)</td>
</tr>
</tbody>
</table>

*Included in Annual Network Participation Fee

---

95% of Participants pay $0 in new fees to INITIATE queries through the Hub

---

### 8 HOW CAN I OBTAIN ADDITIONAL INFORMATION?

<table>
<thead>
<tr>
<th>How</th>
<th>When</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Web Site</td>
<td>Any time (Registration for the secured Participant-only section is fast &amp; easy)</td>
<td><a href="https://ehealthexchange.org/participant-area/ehealth-exchange-operations-wiki/hub-development-updates">https://ehealthexchange.org/participant-area/ehealth-exchange-operations-wiki/hub-development-updates</a></td>
</tr>
<tr>
<td>2 Monthly Participant Web Meetings</td>
<td>Typically the 3rd Thursday of Each Month at 1 pm ET</td>
<td><a href="https://ehealthexchange.org/events">https://ehealthexchange.org/events</a></td>
</tr>
<tr>
<td>3 Hub Web Meetings</td>
<td>Typically Tuesdays at 1pm ET &amp; Thursdays at 4pm ET</td>
<td><a href="https://ehealthexchange.org/events">https://ehealthexchange.org/events</a></td>
</tr>
<tr>
<td>4 Email</td>
<td>Any time if you have a specific question and cannot attend the Hub Web meetings</td>
<td><a href="mailto:administrator@ehealthexchange.com">administrator@ehealthexchange.com</a></td>
</tr>
<tr>
<td>5 Annual eHealth Exchange Meeting</td>
<td>December 4-6, 2019</td>
<td><a href="https://ehealthexchange.org/events">https://ehealthexchange.org/events</a></td>
</tr>
<tr>
<td>How</td>
<td>When</td>
<td>Where</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gaylord National Resort &amp; Convention Center (Washington DC)</td>
</tr>
</tbody>
</table>
9 APPENDIX A – SECURITY DETAILS

9.1.1 Governance
The eHealth Exchange is self-governed by those organizations participating in the health information network. Each Participant is responsible to the other Participants under a multi-party legal agreement called the Data Use and Reciprocal Support Agreement (DURSA).

9.1.2 Policies
eHealth Exchange operational expectations, such as managing digital certificates, are specified in Operating Policies and Procedures, specifically Operating Policies and Procedures #9 “eHealth Exchange Digital Credentials”.

9.1.3 Specifications
The Hub and eHealth Exchange Participants are required to adhere to the associated eHealth Exchange technical specifications.

9.1.4 Standards
The Hub leverages the following security-focused standards:
- NIST FIPS, FISMA, CMVP, and others
- FBCA
- W3C XML Digital Signatures
- IETF TLS
- IHE XCPD
- IHE XCA
- IHE ATNA
- eHealth Exchange Messaging Platform
- eHealth Exchange Authorization Framework
- eHealth Exchange Access Consent Policies
- W3C SAML
- IETF X.509

9.1.5 Reduced Cyber Threat Attack Surface Area
One benefit of the Hub is that Participants will have a reduced attack surface area since:
- Only a single outbound and inbound connection will need to be established
- Only a single IP address will need to be communicated with for the Hub and all eHealth Exchange Participants connected to the Hub
- Only a single 2-way TLS x.509 certificate will need to be trusted
- All communications will now go through port 443 (the standard TLS port)
9.1.6 Encryption of PHI In-Transit
Communications between eHealth Exchange Participants and the Hub are only allowed if they are encrypted using 2-way TLS with mutual authentication. Both the sender and the receiver of the technical messages must confirm the authenticity of their peers.

9.1.7 Certificate Trust
eHealth Exchange certificates adopted and required the use of at least 2048 bit X.509 certificate keys many years ago, well before it was an industry standard. Certificates are NOT in the generally trusted list of consumer-grade internet access technologies such as popular web browsers. Instead, the eHealth Exchange supports best-in-class lineage by only allowing the use of trusted Federal certificates, issued under the FBCA program. This increases security by denying attackers specific knowledge and easy access to the associated trust chain reducing their ability to understand and mount a cyber-threat. eHealth Exchange certificates are only issued to known, trusted, individual human Subscribers that have completed the eHealth Exchange identity proofing requirements including an in-person process.

9.1.8 Auditing
The eHealth Exchange PKI assessment program regularly assesses the Hub and Participants’ gateways to confirm:
- Only NIST-approved ciphersuites are employed in production. Ciphersuites families such as eNULL, aNULL, DES, 3DES, MD5, EXPORT, EXPORT 40, etc. are not allowed in production.
- Gateways use FIPS mode (or its equivalent) in production operations
- Gateways appear to support certificate attribute filtering
- Gateways do not accept revoked or suspended certificates
- Gateways do not accept self-signed or expired certificates
- Gateways do not accept forged certificates
- etc

9.1.9 Staff
eHealth Exchange staff with access to PKI systems undergo extensive background checks by a third party service. These checks include criminal history, education, employment, etc. for all current and prior states of residence going back to that person’s age of majority. Staff processes and IT systems are audited periodically to verify compliance with processes and policies, including the use of encrypted drives, antivirus software, patch levels, and much more.

9.1.10 Authenticity, Integrity and Access
Authenticity is addressed via Cryptographic Signatures of the transacted messages, and via encrypted channels. Integrity is addressed via the same approaches as authenticity. Access is controlled by the disclosing party (the Responding Gateway), enforceable legal agreement, and
governing law. Each message between eHealth Exchange Participants and the Hub includes a robust security header that allows the Responding Gateway to determine the requesting entity, the requesting person or system, the role of the requester, the purpose of the request (such as for treatment), how the end-user was authenticated, and more. This information also allows for high quality audit logging which is required by both the Initiating Gateways and the Responding Gateways.

9.1.11 Encryption at Rest and In-Transit
Data is encrypted (1) between Initiating Gateways and the Hub, (2) as it passes through the Hub, and (3) between the Hub and the Responding Gateway. The associated response is also encrypted. The message is temporarily decrypted upon receipt by the Hub only while the message is in the process of being re-encrypted for internal Hub processing. The re-encrypted message then remains encrypted until it is temporarily decrypted for final re-encryption and subsequent storage and/or transmission to the ultimate receiver. Individually Identifiable Information (III) information is stored in log files as is required for information security and regulatory compliance purposes, and as is required by the Data Use and Reciprocal Support Agreement (DURSA) auditing requirements and the eHealth Exchange technical specifications. This information includes the person’s required first, last and middle name, required administrative gender, required date / time of birth, optional addresses(s), optional telephone number(s), optional social security number and optional other identifiers (such as medical record numbers, state driver’s license numbers, federal agency identifiers, etc.). The technical specifications dictating the information collected may be found in the Patient Discovery 2.0 specification

9.1.12 Cryptographic Signatures
The eHealth Exchange requires the use cryptographically signed messages. The contents of the technical messages exchanged between Participants and the Hub must be signed using a PKI X.509 certificate issued under the FBCA program. This helps assure, strongly, that the messages are authentic and intact.
10 Appendix B – Contract Change Highlights

Why is the Participation Agreement Changing?

<table>
<thead>
<tr>
<th>To Amend the Existing Agreement Structure</th>
<th>To Add a Hub Addenda</th>
<th>To Add a BAA Addenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>• To enhance the agreement structure to facilitate the use of contract addendums</td>
<td>• To establish guardrails regarding use of the Hub</td>
<td>• Participants’ attorneys (not the eHealth Exchange) will likely insist upon signing a BAA since the eHealth Exchange is not a party to the DURSA and the eHealth Exchange is providing the Hub service on behalf of Participants</td>
</tr>
<tr>
<td>• General housekeeping</td>
<td></td>
<td>• This BAA is not replacing or superseding the DURSA.</td>
</tr>
</tbody>
</table>

Please e-mail questions or concerns to administrator@ehealthexchange.com

10.1.1 Participation Agreement

• Replaced “Sequoia Project” with “eHealth Exchange”

• Enhanced agreement structure to facilitate the use of contract addendums (e.g. a Hub addenda & a BAA addenda)

• State Governmental entities are subject to their own state law

• Revises the section on Fees to reflect that eHealth Exchange will offer services and that there will be fees for those services that will be included in the fee schedule. Also, clarifies that fees associated with a contract addenda (e.g. the Hub) have the same late fees. Also, clarifies that late fees and expenses can be waived if a Participant is prohibited by law from paying those fees and expenses.

• Corrects a mistake that stated the Coordinating Committee approved the original Participation fees years ago and removes language requiring the Coordinating Committee to approve amendments.

• Says notices should be sent to the eHealth Exchange Executive Director instead of the Sequoia Project CEO

• Adds new Hub fees and future Carequality fees to the fee schedule
• States that Carequality fees won’t be charged until the eHealth Exchange onboards to Carequality

10.1.2 Business Associate Agreement (BAA) Addenda

Clarify the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and services being performed by the business associate.

Your attorneys (not the eHealth Exchange) will likely insist upon signing a BAA since the eHealth Exchange is not a Party to the DURSA and the eHealth Exchange is providing the Hub service to Participants.

10.1.3 Hub Addenda

• Participants agree to “cooperate with eHealth Exchange and with the Gateway Vendor as reasonably requested to enhance the effective and efficient operation of the Gateway”
• Participants agree to only use the Hub for eHx approved business
• Participants agree to take responsibility of its users on the Hub
• Participants agree to use and control access to the Administrative Portal appropriately
• Participants agree any fees their vendors charge are their responsibility
• Participants agree to comply “with all applicable privacy and security laws, including the HIPAA Regulations, and local and state laws rules and regulations”
• Participants agree that eHx can monitor and audit all access to and use of the Gateway and the content of any data or messages
• Participants agree to limit the eHealth Exchange’s liability to no more than fees paid for Hub specifically in past 12 months
• Participants agree that the eHealth Exchange has the right to suspend Participant’s Hub access and terminate agreement
• Participants agree that eHx is not responsible for inaccurate data, incomplete data, Participants’ use of data, or Hub downtime