FHIR at Scale Taskforce (*FAST*)

Proposed Solutions Working Document: Directory (V3)

December 17, 2020

Table of Contents

[Revision History 2](#_Toc59181839)

[Introduction & Background 4](#_Toc59181840)

[Current State Overview *(see Assumptions to provide context)* 4](#_Toc59181841)

[Examples of Endpoints Providing Access To 5](#_Toc59181842)

[Content of Future State Directory 6](#_Toc59181843)

[Technical Barriers *(from prior presentations)* 7](#_Toc59181844)

[Problems to be Solved, In addition to the Technical Barriers 7](#_Toc59181845)

[Recommended Future State & Intermediate Steps 8](#_Toc59181846)

[Proposed Directory Solution Overview 9](#_Toc59181848)

[Supporting Diagrams & Flows 10](#_Toc59181850)

[In Scope 12](#_Toc59181851)

[Out of Scope 13](#_Toc59181852)

[Assumptions 14](#_Toc59181853)

[Pre-Conditions 14](#_Toc59181854)

[Post Conditions 14](#_Toc59181855)

[Solution Component Analysis 15](#_Toc59181856)

[Key Impacts to Timeline & Cost 15](#_Toc59181857)

[Appendix 16](#_Toc59181858)

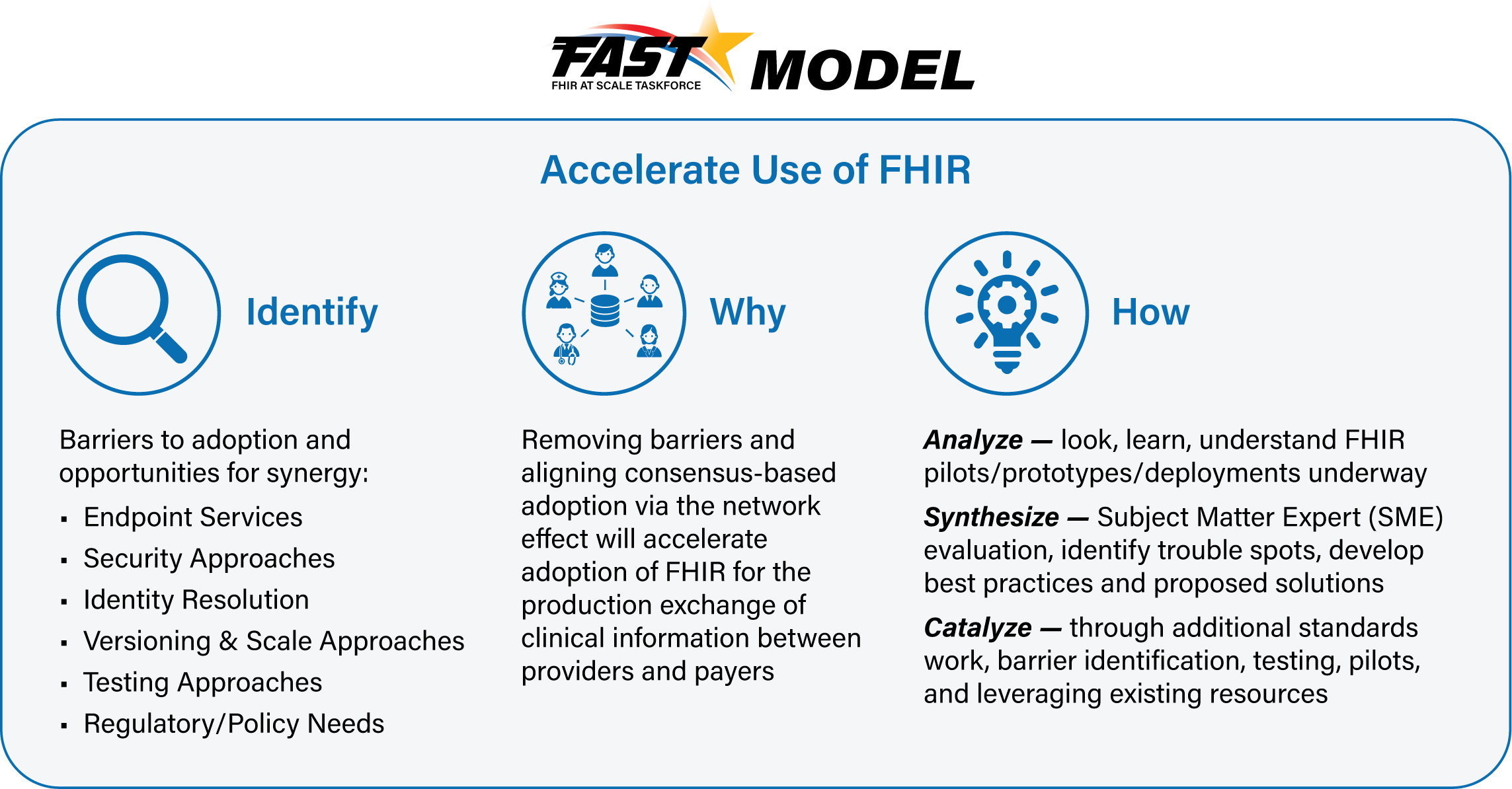
# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description of Change |
| 0.5 | 7/9/19 | Robert Dieterle | Initial draft |
| 1.0 | 8/29/19 | Robert Dieterle | Updated initial draft from tiger team review |
| 1.2 |  | Dan Chaput | Updated draft for TLC |
| 2.0 | 2/27/2020 | Robert Dieterle | Incorporation of all new content from TLC preparation and TLC curated feedback |
| 2.1 | 2/27/2020 | Robert Dieterle | Updated based on DVS TT review |
| 2.1 AG | 3/2/2020 | Alix Goss | Document Review |
| 2.2 | 3/11/2020 | Robert Dieterle | Draft Final |
| 2.3 | 3/18/2020 | Robert Dieterle | Updated with Alix Goss Comments |
| 2.4 | 4/16/2020 | Robert Dieterle | Review on TT call for additional SME Review Content |
| 2.5 | 4/23/2020 | Robert Dieterle | Updated version with changes from 4/16/2020 review |
| 2.6 | 5/12/2020 | Robert Dieterle | Update with Friday review recommendations |
| 2.7 | 5/19/2020 | Robert Dieterle | Final updates for SME Session |
| 2.8 | 12/5/2020 | Robert Dieterle | Updates from SME Sessions and FAST Workshop |
| 3.0 | 12/17/2020 | Robert Dieterle | Include Tiger Team Feedback on V3 Update |

|  |
| --- |
| Reference Documentation |
| [*FAST*-Directory SME Session Summary Report](https://oncprojectracking.healthit.gov/wiki/download/attachments/149848177/FAST-Directory%20SME%20Session%20Summary%20Report.pdf?version=1&modificationDate=1608068187000&api=v2)  [ONC FHIR at Scale Taskforce (*FAST*) Workshop: An Architectural Framework for Ecosystem Infrastructure](https://oncprojectracking.healthit.gov/wiki/display/TechLabSC/2020+ONC+FAST+Workshop)  [*FAST*-Technical Barriers](https://oncprojectracking.healthit.gov/wiki/display/TechLabSC/FAST+Technical+Barriers)  [*FAST*-Regulatory Barriers](https://oncprojectracking.healthit.gov/wiki/display/TechLabSC/FAST+Policy+and+Regulatory+Barriers)  [*FAST*-UC-Endpoint\_Discovery-Core\_Capability-CC1](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Endpoint_Discovery-Core_Capability-CC1.docx?version=5&modificationDate=1573053958000&api=v2)  [*FAST*-UC-Authentication\_and\_Authorization-Core\_Capability-CC2](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Authentication_and_Authorization-Core_Capability-CC2.docx?version=2&modificationDate=1566917471000&api=v2)  [*FAST*-UC-Version\_Identification-Core\_Capability-CC3](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Version_Identification-Core_Capability-CC3.docx?version=2&modificationDate=1566917581000&api=v2)  [*FAST*-UC-Patient\_and\_Provider\_Identity\_Management-Core\_Capability-CC4](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Patient_and_Provider_Identity_Management-Core_Capability-CC4.docx?version=2&modificationDate=1566917581000&api=v2)  [*FAST*-UC-Patient\_Information\_Request\_Plan\_to\_Provider](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Patient_Information_Request_Plan_to_Provider.docx?version=2&modificationDate=1566919693000&api=v2)  [*FAST*-UC-Patient\_Information\_Request\_Provider\_to\_Plan](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Patient_Information_Request_Provider_to_Plan.docx?version=2&modificationDate=1566919694000&api=v2)  [*FAST*-UC-Documentation\_Templates\_and\_Rules\_Processing](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Documentation_Templates_and_Rules_Processing.docx?version=3&modificationDate=1573054516000&api=v2)  [*FAST*-UC-Event\_Based\_Alerts](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Event_Based_Alerts.docx?version=2&modificationDate=1566918841000&api=v2)  [*FAST*-UC-Quality\_Reporting](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Quality_Reporting.docx?version=2&modificationDate=1566920580000&api=v2)  [*FAST*-UC-Push\_Patient\_Information](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Push_Patient_Information.docx?version=2&modificationDate=1566920050000&api=v2)  [*FAST*-UC-Shared\_Care\_Planning](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Shared_Care_Planning.docx?version=2&modificationDate=1566921988000&api=v2)  [*FAST*-UC-Consults\_and\_Referrals](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Consults_and_Referrals.docx?version=3&modificationDate=1573054370000&api=v2)  [*FAST*-UC-Care\_Team\_Coordination](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Care_Team_Coordination.docx?version=3&modificationDate=1566922154000&api=v2)  [*FAST*-UC-Scheduling](https://oncprojectracking.healthit.gov/wiki/download/attachments/118849809/FAST-UC-Scheduling.docx?version=2&modificationDate=1566921653000&api=v2) |

# Introduction & Background

The purpose of the FHIR at Scale Taskforce (*FAST*) is to augment and support recent HL7® Fast Healthcare Interoperability Resources (FHIR®) efforts focused on ecosystem issues that, if mitigated, can accelerate adoption. A number of regulatory and technical barriers, as well as required core capabilities, have been identified related to Directory, Versioning and Scale. This document will outline proposed solutions to address these issues and capabilities.



# Current State Overview *(see* [*Assumptions*](#_Assumptions) *to provide context)*

1. Multiple places to find endpoints (Sequoia, Commonwell, HIEs, DirectTrust, NPPES, etc.) – may require tribal knowledge to determine where endpoint is defined.
2. In many cases there is no resource to find an endpoint for a specific organization or service.
3. Lack of an authoritative source of provider (individual and organizational) information that includes information defined in “Content of Future State Directory” as a “place” to anchor the FHIR endpoints. Builds upon work done and documented at the following:

* <https://oncprojectracking.healthit.gov/wiki/display/TechLabSC/Healthcare+Directory>
* <http://build.fhir.org/ig/HL7/VhDir/> and <http://hl7.org/fhir/us/davinci-pdex-plan-net/STU1/>

1. Amount of information at an endpoint varies greatly depending on source
2. Each source has its own implied trust framework
3. Degree of audit and currency of the information varies tremendously
4. Method of access to the directory varies tremendously
5. Operational endpoint capability discovery unavailable
6. Endpoint discovery focused on organizational level resource necessitating provider/organizational linkage
7. No initial or recurring validation of endpoints for compliance to FHIR specification
8. Limited to current ability to utilize an intermediary for routing to specific endpoints (with further complexities regarding patient vs. organizational queries)

# Examples of Endpoints Providing Access To:

1. Payer, provider, patient access to patient records (e.g., Patient Access API)
2. Scheduling
3. Payer, Provider Directory
4. Formulary
5. Member access to EOBs (e.g., BlueButton 2.0)
6. Member access to clinical data (e.g., USCDI)
7. Member directed exchange of USCDI between old and new payer (data portability)
8. Exchange of information between payers to support coordination of care
9. CDS Hooks (e.g., Coverage Requirements Discovery)
10. Rules exchange (e.g., Documentation Templates and Rules)
11. Provider access to member data
12. Reporting Quality Data
13. Prior Authorization
14. Public health reporting
15. Consent management

The endpoint may provide a capability statement that defines further the resources and operations provided by the specific endpoint or it may be an operation endpoint that only provides one service and does not have a capability statement or is not part of the capability statement.

# Content of Future State Directory

This section builds upon work done and documented at the following:

* <https://oncprojectracking.healthit.gov/wiki/display/TechLabSC/Healthcare+Directory>
* <http://build.fhir.org/ig/HL7/VhDir/> and <http://hl7.org/fhir/us/davinci-pdex-plan-net/STU1/>

Proposed content for endpoints includes:

1. Address (URL/URI)
2. Type (FHIR server, operation endpoint, CDS Hooks, …)
3. FHIR version(s) supported
4. Trust framework(s) supported by this endpoint[[1]](#footnote-2)
5. Trust artifacts (e.g., digital certificates)
6. IGs supported (e.g., PDex)
7. Certification and Testing information, with effective as of dates
8. Support for dynamic registration (*FAST* Security Tiger Team approach) may vary by configuration (e.g., pt-pt, pt-broker)

**Note**: some items above (3, 6 and possibly 7) may be automatically populated from the capability statement.

Proposed content for the provider directory that will be the anchor for the endpoint information includes:

1. Individual Provider Information (e.g., demographics, licenses, identifiers)
2. Healthcare Provider Organization Information (e.g., demographics, licenses, identifiers)
3. Healthcare Payer Information (demographics, identifiers)
4. Relationships between (individual providers, provider organizations and payers)
5. Public Health Entity Information
6. Clinical Research Organizations
7. Other healthcare related individuals and organizations

Other content:

1. Applications (Identifier, description, certification, Trust Framework1, etc.)

Notes:

1. Endpoints may be associated with any of the above (including in context of relationships and Trust Framework)
2. Need code systems for non-care provider entities (individual and organization) not represented in NUCC

.

# Technical Barriers *(from prior presentations)*

1. **Endpoint Identification:** No current standard or implementation provides a generally available method to find all FHIR endpoints and their associated capabilities (e.g., beyond just the capability statement).
2. **Endpoint Characteristics:** Currently no standard or implementation guide specifies and supports additional a comprehensive list of endpoint attributes across all healthcare actors (i.e., trust framework, authentication requirements, FHIR version(s), supported services, testing and certification).
3. **Currency & Accuracy of Directory Endpoint Information:** Currently there is no agreed upon source of truth nor standard process for keeping endpoint information current and validating its accuracy. This creates uncertainty and potential for inconsistent directory endpoint information.
4. **Restricting Access to Endpoint Information:** Certain endpoints may not be generally available (require specific authorization) for reasons such as privacy or safety concerns and directory services may need to restrict discoverability for those specific endpoints (e.g., the address of a women’s shelter or the members of an emergency response team). This may be necessary to minimize attacks on these endpoints by malicious third parties.

# Problems to be Solved, In addition to the Technical Barriers

1. **Use of NPPES as the Repository for Endpoints:** The National Plan and Provider Enumeration System (NPPES) directory is not designed to hold, validate, and maintain the information required to appropriately describe the endpoints for FHIR. The historically low rate of publication of valid Direct addresses in NPPES and the fact that only 4.3% of FHIR endpoints were valid as of 8/20/2020 is a strong indicator of the issues. The complexity of relationships (e.g., provider-organization) that determine which FHIR endpoints are relevant and the need to represent organizations other than providers (e.g., Payers) severely limits the utility of NPPES. The FHIR Endpoint directory needs to be based on a broader set of validated healthcare participants and relationships. While this solution document may pursue the interim use of NPPES to support FHIR endpoints, the longer-term solution will require a significantly more robust solution.

# Recommended Future State & Intermediate Steps

**Future State**

1. One national source for validated directory information that is available to any national or local directory workflow environment (federated access).

* The final solution may include more than one authoritative source as long as there are no overlaps (e.g., same endpoint defined in more than one authoritative national directory source) Example: all payer endpoints in one directory and all provider endpoints in a separate directory.
* The final solution has a master, main source of data to support federated replication and use.

1. Directory contains individual and entity demographics, as well as relationships between individuals and organization to determine endpoint relationships.
2. Computable endpoint information will include supported implementation guides, trust framework, accessibility requirements, validation status, meta data requirements (e.g., for routing through intermediary).
3. Issuing Organizations and Assigned Parties will contribute authoritative information to the Endpoint Directory regarding the scope and capability of the endpoints.
4. Testing and certification information shall be part of the submission information and shall be kept up to date based on the established standard for the type of endpoint.
5. FHIR standard implementation guides (IGs) shall exits (having been created, balloted and published by an accredited standards organization) for:

* the exchange of information between the validated directory and the federated directories ([see diagram](#_Directory_Architecture_and)),
* describing how to query the directory and retrieve supported FHIR endpoints, and
* how to submit attested information to the directory and validate specific items against primary sources.

1. The deployment and operations plan[[2]](#footnote-3) will determine how to ensure the quality of all information in the directory (not limed to the endpoint information) including:

* operations to support the attestation process,
* support for initial and ongoing validation of specific directory elements (e.g., triggers), and
* the process for ongoing maintenance.

**Intermediate Goals**

1. A FHIR standard implementation guide (IG) shall be created, balloted, and published describing how to query the directory and retrieve supported FHIR endpoints. This is both an intermediate goal and final solution requirement.
2. Explore the possibility to use NPPES to as a interim directory to support the declaration of FHIR endpoints associated with individuals and organizations that have been assigned NPIs.
3. Each authoritative source shall ensure that any directory to which it contributes endpoint information shall have the same current information.
4. Determine how to define patient facing applications (e.g., for Patient Access API).
5. Multiple entities may be involved in creating the interim solution.

* Provide for ongoing coordination as long-term solution is pursued.
* Consider a Payer endpoint directory as an early step in the process to address some of the endpoint identification issues raised by the CMS Interoperability Final Rule.

**Comments on the Role of the Directory in establishing “Trust” and Authentication**

1. Directory can support, for each endpoint, a “trust” framework declaration and appropriate validation artifacts (e.g., trust framework digitally signed verification).
2. When authentication occurs under the declared “trust” framework, scope/permission is set and FHIR service enforces permission.

# Proposed Directory Solution Overview

Through use case development and barrier definition, the *FAST* team has determined that the following core capabilities related to Directory needs to be satisfied to accelerate FHIR adoption at scale:

|  |  |
| --- | --- |
| **Core Capability** | **Proposed Solution(s)** |
| 1. Endpoint Discovery | One national repository for validated information related to healthcare endpoints (may include separate directories with clear boundaries – e.g., provider, payers, applications)  Validated information is available (with appropriate permission) to other directories that are integrated in workflow or provide value added services  All endpoints and critical information related to the individuals and organizations are attested, validated, and maintained |

# Overview & Description

The goal for a directory of FHIR endpoints is to incorporate the endpoints in an authoritative directory of providers (individuals and organizations), payers and other members of the healthcare ecosystem (e.g., public health, population health, service providers) that have a need to provide or exchange information directly or indirectly related to the provision for and support of patient care and healthcare delivery. Since the appropriate endpoint for an individual or organization is frequently related to the relationship between these entities, it is important to have a comprehensive validated view of the participant to allow for appropriate queries to determine the correct FHIR endpoint. There should be only one authoritative national directory or source of truth for any specific bounded group of information (e.g., provider, payers, applications). All information, with appropriate provision for any protected information, should be available to other directories to add value, distribute access, and/or integrated into specific workflows.

# Supporting Diagrams & Flows

#### Directory Architecture and Workflow

#### 

This document defines federated as applying to the ability to have more than one directory instance that maintains a copy of all or part of the Validated HealthCare / Endpoint Directory information to provide discovery of and/or access to endpoints to the application population they serve.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Description of Directory Architecture/Workflow** | **Notes** | **FHIR Implementation Guide** |
| 1-2 | Entity submits attested information | Attested information includes declaration of relationships between individuals and entities such as providers and care setting | FHIR IG to support submission of attested information and validation of the information against primary source |
| 3-5 | Validation against primary source |  |
| 6-7 | Issuing and assigned parties declare Endpoint information |  |
| 8-10 | Endpoint information is validated against primary sources |  |
| 11-12 | Federated directory subscribes to specific scope of information | Scope determined by Data Use Agreement (DUA) for other than “public” information | FHIR IG to support the exchange of validated directory information with a federated directory |
| 13-14 | Updated information is pushed to the subscribing directory |  |
| 15-16 | Request by application for endpoint information |  | FHIR IG to support endpoint query against federated directories |

#### Access to Endpoint Directory

#### 

|  |  |  |
| --- | --- | --- |
| **ID** | **Description of Access to Endpoint Directory** | **Notes** |
| 1 | Requester sends request to the endpoint directory |  |
| 2 | Endpoint directory authenticates the requestor (if required) |  |
| 3 | Endpoint directory performs the requested query |  |
| 4 | Requestor receives the one or more endpoints associated with the scope of access they are allowed and the search criteria |  |
| 5 | Requester uses directory endpoint information to connect to the responder endpoint and send request |  |
| 6 | Responder authenticates requestor |  |
| 7 | Responder process request and returns results |  |
| 8 | Requestor receives response from responder |  |

# In Scope

1. Specification for base directory content including all items indicated in Future State section of this document including

* Individual providers with persistent relevant attributes (e.g., degrees, licenses, languages)
* Provider organizations with persistent relevant attributes (e.g., locations, certifications, availability)
* Location relevant attributes (e.g., addresses, contact information, availability)
* Relationships between providers, organizations, and respective locations
* Support for non-traditional providers and organizations (e.g., Meals on Wheels)
* Consumer application, public health, and clinical research endpoints

1. Accommodation for both FHIR endpoints (e.g., FHIR server or FHIR service) and FHIR related endpoints (e.g., CDS-Hooks, Bulk Data: SFTP)

* Compliance of endpoint with FHIR and RESTful standards for error responses (as part of testing and certification or attestation)

1. Compliance of directory with FHIR and RESTful standards for error responses
2. Support for non-FHIR endpoints (e.g., Direct)
3. Available as part of endpoint directory

* Trust framework information
* API certification
* Application certification
* FHIR version(s)

1. Directory architecture: attestation, validation, and federated access model
2. Authentication and authorization as it relates to endpoint discovery
3. Specification for directory query payload and exchange
4. Availability specification – e.g., SLA and hours of operations

# Out of Scope

1. Manual access (e.g., portal)
2. Integration with clinical systems
3. Directory maintenance (how, not what)
4. Intermediary rules
5. Creation of trust framework (in scope: recording and presenting as part of discovery)
6. Certification of applications (in scope: recording and presenting as part of discovery)
7. Version support standards (in scope: discovery of version of endpoint)
8. Detailed architecture (in scope: high level architecture— model(s) -- enough for sr. architect to do detail)
9. Authentication and Authorization for the general FHIR ecosystem is out of scope (in scope: 1) as it relates to access to endpoint discovery and 2) recording and presenting as part of endpoint discovery)
10. An entity’s internal processing to request or respond to endpoint requests –(in scope: payload and exchange)
11. Specific support for non-FHIR related endpoints (e.g., XDS or XCA, Direct Project) (other than provision to include in directory endpoint information) – (in scope: FHIR endpoints (e.g., FHIR server or FHIR service) and FHIR related endpoints (e.g., CDS-Hooks, Bulk Data: SFTP))
12. Monitoring availability (in scope: support availability specification – e.g., SLA and hours of operations)
13. Merge/unmerge; dynamic updates should pull most current end point. Assumption that an organization would adopt a new endpoint or deactivate no longer valid endpoints caused by organization or system changes
14. Capability of the federated directories to provide additional services (e.g., search, matching)
15. Dynamic information (e.g., provider schedule availability)
16. Local information (e.g., only required in a delivery organization or regional service)

# Assumptions

1. To minimize the need for providers, organizations and healthcare associated entities (e.g., Payers) to maintain essential directory data and endpoints with multiple organizations, we need one authoritative national source of truth
2. To address the need to have this information available in multiple contexts (e.g., State HIE, Payer network) the resulting information must be federated
3. Validation should be automated and not manual wherever possible
4. Directory will work for patient mediated models for exchange, but the directory will not contain either patients or their non- licensed caregivers (e.g., not an MPI)
5. Testing and Certification requirements applied to entities submitting data.
6. Adherence to established health care regulations and laws related to protecting, securing, and exchanging health information

# Pre-Conditions

1. Standard FHIR specification (e.g., implementation guide) for directory query
2. Standard FHIR specification (e.g., implementation guide) for Endpoint information
3. Standard FHIR specification (e.g., implementation guide) for exchange between the validated directory and the federated directories
4. Standard FHIR specification (e.g., implementation guide) for attestation and validation to the validated directory
5. Actor has the authority to access the directory for controlled access endpoints and related information
6. Determination of policies regarding submission, maintenance and sharing of endpoint information
7. Standard trust framework definitions and process for validation
8. Testing and Certification process defined
9. Authentication and Authorization processes defined

# Post Conditions

1. Ability to retrieve FHIR endpoints and meta data using standard FHIR queries to automate the connection to FHIR APIs
2. Ability to participate in Trust Frameworks to avoid point to point agreements between entities
3. Ability to call a service to discover endpoint directory details via broker or direct connection to authoritative directory

# Solution Component Analysis

The following new components or modifications to existing components are required to address current gaps and support the proposed solution:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Component** | **New/ Existing** | **Proposed Build/Modifications** | **Owner** |
|  | Validated Directory | New |  | CMS |
|  | Exchange standard | Modification of Existing VHDir Standard |  | FAST/HL7 |
|  | Query standard | New |  | FAST/HL7 |
|  | Attestation and Validation Standard | New |  | FAST/HL7 |
|  | Update NPPES | Existing (needs update) | To Support validation of FHIR endpoints for interim solution | CMS |

# Key Impacts to Timeline & Cost

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Component** | **Level of Effort** | **Comments** |
|  | Validated Directory | Jumbo |  |
|  | Exchange standard | Moderate |  |
|  | Query standard | Low |  |
|  | Attestation and Validation Standard | Medium/High |  |
|  | Update NPPES | Moderate |  |

# Appendix

#### Work to be Addressed *(not necessarily in this solution document)*

1. Resource will exist that allows an organization to determine:

* all endpoints that have a particular patient/member record and
* all endpoints that are currently participating in that patient/member care (this is not a directory issue but rather a record locator service / MPI)

1. Intermediaries, such as clearinghouses and health information exchanges, will support future state functionality especially as it relates to end point information (and supports scaling).
2. Need to resolve issues of associating endpoints with individuals (who maintains)
3. Note that clinical research is not excluded. Seems more focused on the Identity Tiger Team, especially for deidentified datasets. Question related to bulk data and whether we should be tackling it even with bulk data use cases being addressed within FHIR community. Could be endpoint capabilities statement or throughput / response time related statement. ADD TO SCALING DISCUSSION - avoid timeout issue considerations. (should this be a definition for an endpoint or just part of a capability statement) backlog?
4. Note: to address scaling of authentication of the requester, describe how a trust framework and role associated with authentication will support the authorization processes
5. More detail – annotation to existing drawings expand the text in the “blue boxes” (defer)
6. Endpoint actor should maintain log/ audit of access to endpoints (for implementation/ deployment)
7. TLS required (current version – see NIST) for authenticated access (security) (need to consider if mutual TLS is a requirement)
8. Revocation rules and actions will be established by the overseer or maintainer of the “master” directory and carried forward to federated directories.
9. Test environment for endpoint directory

#### Proposed Next Steps:

1. Identify owner/operator of the validated directory (Deployment Plan)
2. Define staging of final solution to avoid need for all at one time build
3. Explore incentives to utilize the proposed architecture (Deployment Plan)
4. Identify any additional standards, process and regulatory authority required (Deployment Plan)
5. Need to clarify intermediate steps to support transition from current environment

1. A Trust Framework is a specification of the identity, security, privacy, data protection, and data use policies to which participants in a community of interest agree to conform. [↑](#footnote-ref-2)
2. Deployment and operations plan should be established by the organization(s) that will build and maintain the directory. [↑](#footnote-ref-3)