FHIR at Scale Taskforce (*FAST*)

Proposed Solutions Working Document: Directory (V2)

# Table of Contents

Revision History 2

Outstanding Work……………………………………………………………………………………………………………………………………2

Introduction & Background 3

Current State Overview 4

Examples of Endpoint Providing Access To:……………………………………………………………………………………………..4

Content of Future State Directory……………………………………………………………………………………………………………5

Technical Barriers ……………………………………………………………………………………………………………………………………6

Problems to be Solved 6

Recommended Future State & Intermediate Steps 7

Proposed Directory Solution Overview 8

Overview & Description……………………………………………………………………………………………………………………………8

Supporting Diagrams & Flows 9

In Scope 11

Out of Scope 12

Assumptions 13

Pre-Conditions 13

Post-Conditions 13

Solution Component Analysis 14

Key Impacts to Timeline & Costs 14

Work to be addressed…………………………………………………………………………………………………………………………….15

Proposed Next Steps………………………………………………………………………………………………………………………………15

# Revision History

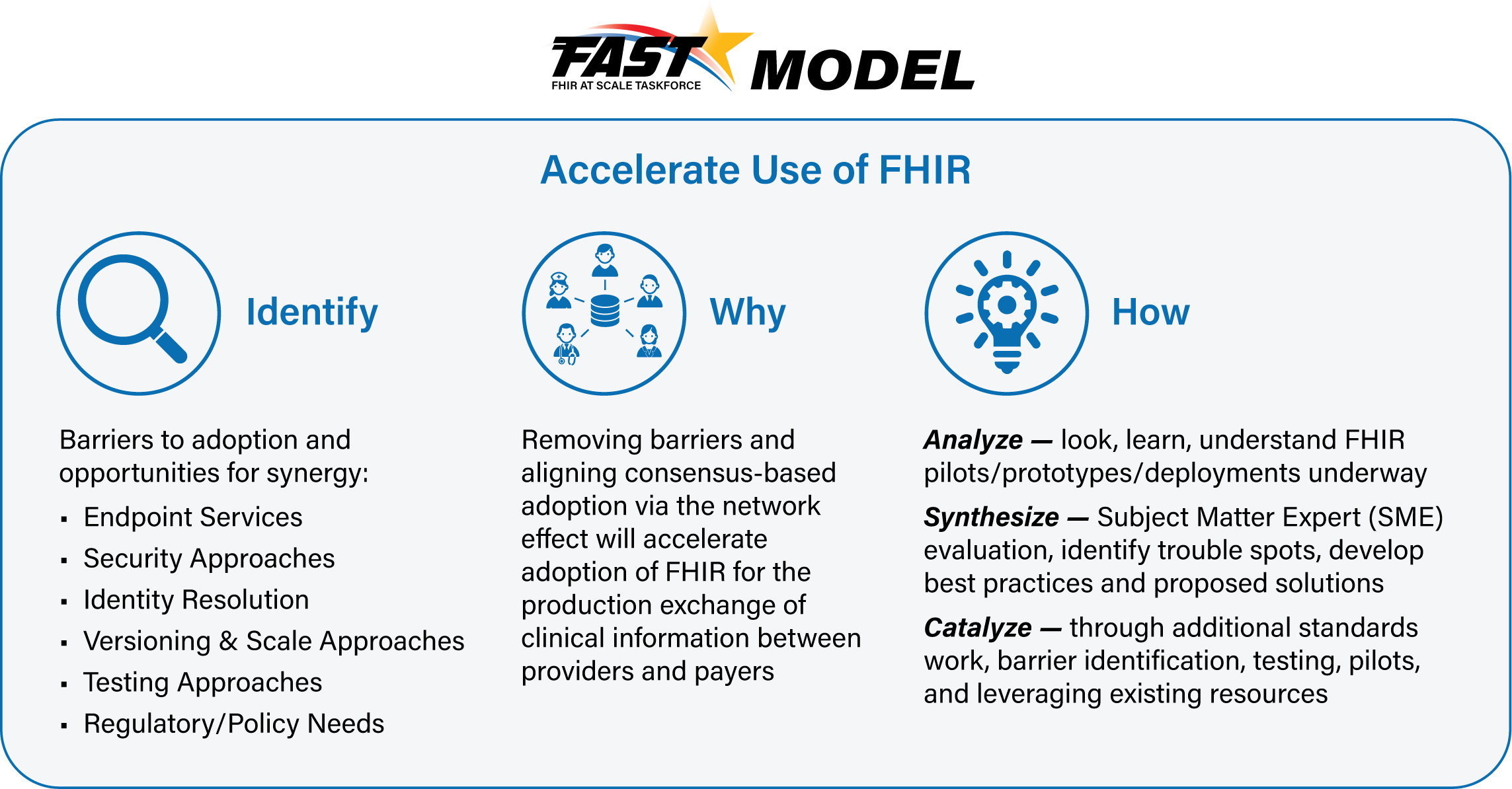
|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description of Change |
| 0.5 | 7/9/19 | Robert Dieterle | Initial draft |
| 1.0 | 8/29/19 | Robert Dieterle | Updated initial draft from tiger team review |
| 1.2 |  | Dan Chaput | Updated draft for TLC |
| 2.0 | 2/27/2020 | Robert 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 |

(Note to editors: ensure standard front matter content is current and accurate. Changes in Reference Documentation need to be carried over to Support Documentation and Flows section)

|  |
| --- |
| Reference Documentation |
| * *FAST*-Technical Barriers * *FAST*-Regulatory Barriers * *FAST*-UC-Endpoint\_Discovery-Core\_Capability-CC1 * *FAST*-UC-Authentication\_and\_Authorization-Core\_Capability-CC2 * *FAST*-UC-Version\_Identification-Core\_Capability-CC3 * *FAST*-UC-Patient\_and\_Provider\_Identity\_Management-Core\_Capability-CC4 * *FAST*-UC-Patient\_Information\_Request\_Plan\_to\_Provider * *FAST*-UC-Patient\_Information\_Request\_Provider\_to\_Plan * *FAST*-UC-Documentation\_Templates\_and\_Rules\_Processing * *FAST*-UC-Event\_Based\_Alerts * *FAST*-UC-Quality\_Reporting * *FAST*-UC-Push\_Patient\_Information * *FAST*-UC-Shared\_Care\_Planning * *FAST*-UC-Consults\_and\_Referrals * *FAST*-UC-Care\_Team\_Coordination * *FAST*-UC-Scheduling |

# 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 to provide context)

1. Multiple places to find endpoints (Sequoia, Commonwell, HIEs, DirectTrust, etc.) – may require tribal knowledge to determine where endpoint is defined
2. 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://build.fhir.org/ig/HL7/davinci-pdex-plan-net/>

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 no 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 medical records
2. Scheduling
3. Payer, provider Directory
4. Formulary
5. Member access to EOBs (e.g. BlueButton)
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.

# Content of Future State Directory (building on the prior work noted above)

Bob to reorganize this section

1. Endpoint information
   1. Address (URL/URI)
   2. Type (FHIR Server, Operation endpoint, CDS Hooks, …)
   3. FHIR version(s) supported
   4. Trust framework(s)
   5. Trust artifacts (e.g. digital certificates)
   6. IGs supported (e.g. PDex)
   7. Certification and Testing information
2. Individual Provider Information (e.g. demographics, licenses, identifiers)
3. Healthcare Provider Organization Information (e.g. demographics, licenses, identifiers)
4. Healthcare Payer Information (demographics, identifiers)
5. Relationships between (individual providers, provider organizations and payers)
6. Public Health Entity Information
7. Clinical Research Organizations
8. Applications (Identifier, description, certification, …)
9. Note: endpoints may be associated with any of the above (including in context of relationships and trust framework\*)

\*define trust framework

# Technical Barriers

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 specifies and supports additional endpoint attributes (i.e., trust framework, authentication requirements, FHIR version(s), supported services, certification and testing).
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 endpoint directory information.
4. **Restricting Access to Endpoint Information:** Certain endpoints may not be generally available (regardless of authentication) and any directory service may need to restrict discoverability for those specific endpoints. This may be necessary to minimize attacks on these endpoints by malicious third parties.

# Problems to be Solved

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 specifies and supports additional endpoint attributes (i.e., trust framework, authentication requirements, FHIR version(s), supported services, certification and testing).
3. **Currency & Accuracy of Directory Endpoint Information:** Currently there is no agreed upon source or standard process for maintaining endpoint information and validating its accuracy. This creates uncertainty and the potential for inconsistent endpoint directory information.
4. **Restricting Access to Endpoint Information:** Certain endpoints may not be generally available (regardless of authentication) for reasons such as privacy or safety concerns and any directory-service may need to restrict discoverability for those specific endpoints. This may be necessary to minimize attacks on these endpoints by malicious third parties.
5. **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 current low rate of publication of Direct addresses in NPPES is a strong indicator of the issues.

# 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) – 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.
2. Directory contains individual and entity demographics to determine endpoint relationships.
3. Computable endpoint information will include supported implementation guides, trust framework, accessibility requirements, validation status, meta data requirements (e.g. for routing through intermediary).
4. Issuing Organizations and Assigned Parties will contribute authoritative information to the Endpoint Directory regarding the scope and capability of the endpoints.
5. 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.
6. A FHIR standard implementation guide (IG) shall be created, balloted and published describing how to query the directory and retrieve supported FHIR endpoints.
7. The deployment and operations plan will determine how to ensure the quality of the information in the directory (including, but not limed to, the endpoint information) including: a) attestation process, b) how and when elements of the directory are validated (e.g. triggers), c) the process for validation and d) process for ongoing maintenance.

**Intermediate Goals (make this part of the SME discussions)**

1. A directory/registry should be established that points to a qualified directory that contains authoritative FHIR endpoints.
2. A FHIR standard implementation guide (IG) shall be created, balloted and published describing how to query the directory and retrieve supported FHIR endpoints.
3. Each authoritative source shall ensure that any directory to which it contributes the endpoint shall have the same current information.
4. Need to determine how to define patient facing applications (endpoint extension vs. device resource)

**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 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 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.

# SME discussion points

# Multiple entities may be involved in building the solution (focused on the interim solution)

# Issues related to “pushing” updates to the federated directories

# Supporting Diagrams & Flows

# Directory Architecture and Workflow

# 

# Change local to federated access

|  |  |  |
| --- | --- | --- |
| **ID** | **Description of Directory Architecture/Workflow** | **Notes** |
| 1-2 | Entity submits attested information | Attested information includes declaration of relationships between individuals and entities such as providers and care setting |
| 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 |
| 13-14 | Updated information is pushed to the subscribing directory |  |

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 |  |

Additional work and implementation/deployment items from TLC / review

1. More detail – annotation to existing drawings expand the text in the “blue boxes” (defer)
2. Add detail and justification for unauthenticated and authenticated access (use women’s shelter and emergency response network access points) detail of authentication and authorization is out of scope for this use case (move into content requirements)
3. Endpoint actor should maintain log / audit of access to endpoints (for implementation/ deployment)
4. TLS (not mutual) required (current version – see NIST) for authenticated access (security)
5. Revocation rules and actions will be established by the overseer or maintainer of the “master” directory and carried forward to federated directories.
6. Test environment for endpoint directory

# In Scope

1. FHIR endpoints (e.g. FHIR server or FHIR service) and FHIR related endpoints (e.g. CDS-Hooks, Bulk Data: SFTP)
   1. Compliance of endpoint with FHIR and RESTful standards for error responses (as part of testing and certification or attestation)
2. Compliance of directory with FHIR and RESTful standards for error responses
3. Consumer application, public health and clinical research endpoints
4. Available as part of endpoint directory
   1. Trust framework information
   2. API certification
   3. Application certification
   4. FHIR version(s)
5. Directory architecture: high level architecture— federated access model
6. Authentication and Authorization:
   1. as it relates to access to endpoint discovery
   2. as part of end point discovery
7. Specification for directory query payload and exchange
8. 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. Non-FHIR related endpoints (e.g. XDS or XCA, Direct Project) – (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)

# 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 nor their not licensed caregivers’ “addresses” (not an MPI)

# Pre-Conditions

1. Technology Standard specification for directory query
2. Technology Standard specification for Endpoint information
3. Actor has the authority to access the directory for controlled access endpoints and related information
4. Determination of policies regarding submission, maintenance and sharing of endpoint information
5. Standard trust framework definitions and process for validation
6. Certification and Authentication processes defined

# Post Conditions

1. Ability to retrieve FHIR endpoints and associated information using standard queries to automate the connection to FHIR APIs
2. Ability to participate in Trust Frameworks to avoid point to point agreements between entities

# Solution Component Analysis (SME conversation—slide content)

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** |
|  | *Endpoint Directory* | *New* |  |  |
|  | Endpoint query and exchange standard | Modification of Existing Standard |  |  |
|  |  |  |  |  |

# Key Impacts to Timeline & Cost (SME conversation—slide content)

*<FAST team to identify the key components listed above that will have the most impact on timeline and cost. Include rough order of magnitude for level of effort and comment on any known blockers or dependencies.>*

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Component** | **Level of Effort** | **Comments** |
|  | *Endpoint Directory* | *Jumbo* |  |
|  | Endpoint query and exchange standard | Medium |  |
|  |  |  |  |

# Work to addressed (not necessarily in this solution document)

1. Resource will exist that allows an organization to determine 1) all endpoints that have a particular patient/member record and 2) all endpoints that are currently participating in that patient/member care (this is not a directory issue – record locator service / MPI)
2. Intermediaries, such as clearinghouses and health information exchanges, will support future state functionality especially as it relates to end point information (and supports scaling).
3. Need to resolve issues of associating endpoints with individuals (who maintains)
4. Note that clinical research is not excluded. Seems more Identity TT, 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?
5. Note: to address scaling of authentication of the requester, describe how a trust framework and role associated with authentication will support the authorization processes

# Proposed Next Steps:

1. Identify owner/operator of the validated directory (Deployment Plan)
2. Explore incentives to utilize the proposed architecture (Deployment Plan)
3. Identify any additional standards, process and regulatory authority required (Deployment Plan)
4. Need to clarify intermediate steps to support transition from current environment