HL7 FHIR Connectathon
HL7 FAST Infrastructure Track
Kick Off

September 13, 2022
Agenda

• Connectathon Format
• HL7 COVID Policy
• Track Goals
• Track Leads
• Track Agenda
• Testing Integration
• Track Scenarios
• Use Case Roles
September HL7 Connectathon Format

• In-person (first time since 2020)
• Each track has a table or set of tables in a large room
• Break out sessions occur in separate reserved rooms
HL7 COVID Policy for Events

• [https://www.hl7.org/events/covid.cfm](https://www.hl7.org/events/covid.cfm)

• Vaccinations:
  
  – HL7 expects all attendees to be vaccinated. *Attendees are expected to provide validation of their vaccination status.*
  
  – If you believe that you have an exception on medical or religious grounds, please share them with Charles Jaffe, MD (cjaffe@HL7.org) or Julia Skapik, MD (jskapik@nachc.com), who will treat them with the accepted standards of physician-patient confidentiality.
• **Testing:**
  - HL7 requires proof of testing *within 72 hours of attendance* at the meeting. Test must be a professionally administered PCR, Rapid NAAT, or Rapid Antigen. A self-test is not acceptable.
  - Healthcare professionals will manually review vaccine credentials and COVID test results (and, if needed, attendees may purchase a COVID test to be performed onsite).

• **Masks:**
  - As of today, masks are optional. That may change based upon the then current health department requirements
Track Goals

• Integrate AEGIS Touchstone monitoring of data exchange as a stepping stone to broader future testing capability

• Test end-to-end FAST solutions (Security, Identity, Directory, Exchange)

• Verify that the FAST infrastructure supports requirements in the CMS rules for Interoperability and Patient Access as well as Reducing Provider and Patient Burden
<table>
<thead>
<tr>
<th>Person</th>
<th>Role</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dave Hill, MITRE</td>
<td>Track Lead</td>
<td><a href="mailto:dwhill@mitre.org">dwhill@mitre.org</a></td>
</tr>
<tr>
<td>Jeff Brown, MITRE</td>
<td>Security/Identity Matching IG</td>
<td><a href="mailto:jeffbrown@mitre.org">jeffbrown@mitre.org</a></td>
</tr>
<tr>
<td>Alex Shankland, MITRE</td>
<td>Security/Identity Matching RI</td>
<td><a href="mailto:ashankland@mitre.org">ashankland@mitre.org</a></td>
</tr>
<tr>
<td>Sean Mahoney, MITRE</td>
<td>National Directory IGs</td>
<td><a href="mailto:smahoney@mitre.org">smahoney@mitre.org</a></td>
</tr>
<tr>
<td>Abigail Watson, MITRE</td>
<td>National Directory RI</td>
<td><a href="mailto:awatson@mitre.org">awatson@mitre.org</a></td>
</tr>
<tr>
<td>Bob Dieterle, EnableCare</td>
<td>National Directory Lead</td>
<td><a href="mailto:rdieterle@enablecare.com">rdieterle@enablecare.com</a></td>
</tr>
</tbody>
</table>
Break Out Sessions

• Dynamic Registration (B2C)
  – Time: Saturday, September 17, 1-2 pm
  – Location: Homeland Room (capacity 40)
  – Session Lead: Luis Maas

• Reusable Digital Identities (B2B)
  – Time: Saturday, September 17, 3-4 pm
  – Location: Homeland Room (capacity 40)
  – Session Lead: Luis Maas
Break Out Sessions (continued)

• Matching Options beyond Patient $match (B2B)
  – Time: Saturday, September 17, 4-5 pm
  – Location: Fells Point Room (capacity 25)
  – Session Lead: Luis Maas
HL7 Connectathon Agenda

Saturday, September 17:

9:00-9:30  Connectathon Kickoff
9:30-11:00 Track Kickoff
10:30-11:30 Reference Implementation Overview
11:30-12:00 Testing Prep
1:00-2:00  Break out session (Dynamic Registration)
1:00-5:00  Testing
3:00-4:00  Break out session (Reusable Digital Identities)
4:00-5:00  Break out session (Matching options beyond $match)
5:00-5:30  Daily Wrap Up
HL7 Connectathon Agenda (continued)

Sunday, September 18:

- 9:00-10:00: Testing
- 10:00-11:00: Recording Session
- 11:00-12:00: Track Report Out Prep
- 1:00-4:00: Track Report Outs
Testing Integration

All requests and responses should pass through an AEGIS Touchstone proxy.

Richard "Rick" Lisseveld: richard.lisseveld@aegis.net
HL7 FHIR At Scale Taskforce (FAST)

National Directory Exchange
Endpoint Query
Attestation and Validation
Security
Identity Matching
Hybrid/Intermediary Exchange
Scenarios

• **Scenario 1:** Make endpoint query, add and attest to organizational information and endpoints

• **Scenario 2:** Patient visits Hospital for an appointment; Hospital identity proofs the Patient and collects information during patient registration

• **Scenario 3:** PCP has a need for information held by Hospital, with or without Intermediary
  – Scenario 3a – negative test: Try same process with Patient B, who exists, but does not have authorization
Scenarios (continued)

- **Scenario 4:** Patient Directed Exchange by Patient authorizing exchange using UDAP Tiered OAuth instead of JWT-based Authentication
Scenario 1: Make Endpoint Query, Attest to Organizational Information and Endpoints

**Prerequisites**

- New National Directory entry data, certificates

**Client**

1. Looks up the FHIR endpoint to confirm existence
2. Requests to add a new directory entry

**Directory**

**Security**

**Mitre**

3. Receives transaction, validates requestor, validates version
4. Authenticates FHIR user’s role
5. Verifies the new directory entry information and stores it if valid
6. Generates & returns FHIR response

**Conformance & Verification**

**Security**
Scenario 1

- **Overview:** Connect to the National Directory and make a public endpoint query, then attest to organizational information and endpoints
  - *(Find an endpoint)* Access unsecured directory to identify public URL for a different organization (without intermediary)
  - *(Attest to data)* Register (UDAP Security - Dynamic Client Registration) and Authenticate (UDAP Security - B2B) to Directory and attest, writing their data to directory
    - Success criteria: data is successfully written to directory
  - *(Directory to directory exchange)* Register (UDAP Security - Dynamic Client Registration) and Authenticate (UDAP Security - B2B) to the National Directory, accessing sensitive data to directory
  - Directory RI allows and validates writes by trusted clients (Practitioner, PractitionerRole, Restriction)
  - Per policy, some orgs may not be authorized to write sensitive data, or to write data at all
Scenario 2: Patient visits Hospital for an appointment; Hospital identity proofs Patient and collects information during patient registration through intermediary

**Prerequisites**

Patient identity verification & minimum demographics collection by Payer per Guidance on Identity Assurance, Patient Matching
Optional: Create Digital Identity
Optional: Record attribute verification status

**HOSPITAL**

1. Looks up the FHIR endpoint for identity matching server
2. Requests information for patient

**PAYER**

3. Receives transaction, validates requestor, validates version
4. Performs Patient Matching and sends back Not Found if unable to do so

**DIRECTORY**

5. Generates & returns FHIR response

**SECURITY**

6. Requesting system receives data

**IDENTITY**

- UDAP Security added when a partner/affiliate is used
Scenario 2

- Overview: Patient visits Hospital for an appointment; Hospital identity proofs Patient and collects information during patient registration
  - Prerequisite: other testing participants know Patient details, which can be shared on this worksheet
  - Minimum attributes collected:
    - Full legal name (the name that the person was officially known by at the time of issuance of the supporting evidence; not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names)
    - home address
    - date of birth
    - email address
    - mobile number (preferred, and consider that there are free services to create one since having one facilitates matching and credential management; if a mobile number is not available, collect an alternative number for the individual)
Scenario 2 (continued)

- Verify Patient's identity at a target level of assurance as per Guidance on Identity Assurance within Identity IG
  - Patient is sent through a workflow using demographics they specified above plus acceptable identity evidence required to meet the desired level

- Demographics (and later: optional validation status) are ready to be used in a $match request as per UDAP Security, Identity IG

- Bonus point: create a Digital Identifier with associated OpenID Connect Credential and authenticator for Patient as per Digital Identity within Identity IG

- Bonus point: capture verification status at attribute, encounter, or record level (not yet specified in Identity IG; prior work exists for encounter-level use in SMART Health Cards).
Scenario 3: Clinician has a need for information held by Hospital and accesses Hospital records using Dynamic Registration and UDAP Security

**Prerequisites**
- Patient identity verification & minimum demographics collection by Payer per Guidance on Identity Assurance, Patient Matching
- Optional: Create Digital Identity
- Optional: Record attribute verification status

**CLINICIAN**
1. Looks up the FHIR endpoint for payer
2. Requests identity match for patient

**DIRECTORY**

**HOSPITAL**
3. Receives transaction, validates requestor, validates version
4. Performs Patient Matching and sends back Not Found if unable to do so

**SECURITY**

**IDENTITY**

**CONFORMANCE & CERTIFICATION**

**SECURITY**

Generates & returns FHIR response
Scenario 3: B2B with or without intermediary

- Overview: Clinician has a need for information held by Hospital. Hospital uses an intermediary to receive FHIR requests on its behalf.
- Note: Intermediary w/ transparent reverse proxy only; this same workflow can also be tested without an intermediary
  - Clinician accesses endpoint directory (National Directory Endpoint Query) to identify public URL for Hospital
    - Hospital’s public endpoint resolves to intermediary, leveraging National Directory Exchange IG to service Hospital's FHIR requests
    - Show accessing public endpoint
  - Bonus point: Register (UDAP Security - Registration) and Authenticate (UDAP Security - Authorization and Authentication - B2B) to Directory and obtain a sensitive endpoint (e.g., women's shelter, other record not publicly listed)
    - Directory RI will populate and secure a sensitive endpoint (Practitioner, PractitionerRole, Restriction)
  - Clinician dynamically registers at Hospital public endpoint (UDAP Security - Registration)
    - Hospital’s public endpoint resolves to intermediary leveraging National Directory Exchange IG
    - FHIR server answering initial discovery request is going to provide the location of its registration endpoint as publicly accessible URL
Scenario 3 (continued)

  - Validating that the listing obtained from the Directory is in fact from the entity via UDAP Server Metadata IG

- Clinician requests $match against Hospital’s public endpoint (FAST Identity)
  - Intermediary receives match request and routes to Hospital’s private endpoint
  - Bonus point: request includes Level 1 IDI
  - Bonus point: response includes Responder’s System Match Output Quality Score from Identity IG in lieu of locally-computed match confidence
  - Bonus point: requestor provides insufficient demographics and is returned with an informative error and no results
  - Bonus point: requestor provides demographics with verification status in $match request and responder’s system appropriately scores match input and uses as input to response policy engine

- Hospital responds with match(es) & associated patient ID(s) and intermediary routes response back to PCP

- Clinician requests patient information from Hospital public endpoint, using returned patient ID
  - Intermediary receives request and routes to Hospital’s private endpoint

- Success criteria: Clinician obtains health data from Hospital
Scenario 4: Patient Directed Exchange by Patient authorizing exchange using UDAP Tiered OAuth instead of JWT-based Authentication

**Prerequisites**
- Patient identity verification & minimum demographics collection by Payer per Guidance on Identity Assurance, Patient Matching
- Optional: Create Digital Identity
- Optional: Record attribute verification status

**REQUESTING SYSTEM**
1. Formulates FHIR request
2. Looks up the FHIR endpoint for recipient

**INTERMEDIARY**
3. Optional: Forwards the Exchange
- Receiving system receives data

**RECEIVING SYSTEM**
4. Performs patient authenticatio via Digital Identity, Patient Matching & sends back patient ID or Not Found
5a. Authenticates FHIR user's role
5b. Filters out data that does not have consent (patient authorization)
6. Generates & returns FHIR response

**CONFORMANCE & CERTIFICATION**

**SECURITY**
Scenario 4: Patient Directed Exchange

- **Overview:** B2C scenario with UDAP Tiered OAuth expected in future, with Identity IG's Digital Identity including an OpenID Connect credential, authenticator, and Digital Identifier within the user profile.

- **Workflow similar to Scenario 3 except a Client application’s access to data at Organization B is authorized by Patient A in consumer-directed exchange via UDAP Tiered OAuth instead of through JWT-based Authentication.**
  - Organization A accesses endpoint directory (National Directory Endpoint Query) to identify public URL for Organization B.
    - Organization B’s public endpoint resolves to intermediary, Organization C leveraging National Directory Exchange IG to service Organization B’s FHIR requests.
    - Show accessing public endpoint.
  - Bonus point: Register (UDAP Security - Registration) and Authenticate (UDAP Security - Authorization and Authentication - B2B) to Directory and obtain a sensitive endpoint (e.g., women’s shelter, other record not publicly listed).
    - Directory RI will populate and secure a sensitive endpoint (Practitioner, PractitionerRole, Restriction).
Scenario 4 (continued)

- Organization A dynamically registers at Organization B public endpoint (UDAP Security - Registration)
  - Organization B’s public endpoint resolves to intermediary leveraging National Directory Exchange IG
  - FHIR server answering initial discovery request is going to provide the location of its registration endpoint as a publicly accessible URL

  - Validating that the listing obtained from the Directory is in fact from the entity via UDAP Server Metadata IG

- Organization A requests $match against Organization B’s public endpoint (FAST Identity)
  - Intermediary receives match request and routes to Organization B’s private endpoint
  - Bonus point: request includes Level 1 IDI
  - Bonus point: response includes Responder’s System Match Output Quality Score from Identity IG in lieu of locally-computed match confidence
Scenario 4 (continued)

- Bonus point: requestor provides insufficient demographics and is returned with an informative error and no results
- Bonus point: requestor provides demographics with verification status in $match request and responder's system appropriately scores match input and uses as input to response policy engine

- Organization B responds with match(es) & associated patient ID(s) and intermediary routes response back to Organization A
- Organization A requests patient information from Organization B public endpoint, using returned patient ID
  - Intermediary receives request and routes to Organization B’s private endpoint
- Success criteria: Organization A obtains health data from Organization B
- Bonus point: the OAuth sign in page allows user to authorize sharing of the Digital Identifier per Identity IG or other PII from user profile directly to Organization B
- Bonus point: OIDC account created in Scenario 2 at Organization A is used to access data at a different system representing Organization B
- Bonus point: OIDC user profile includes account-level identity and/or authentication level of assurance
- Bonus point: OIDC user profile includes verified demographics as in Identity IG
Use Case Actors

• **Endpoint directory**
  – UDAP FHIR Server with Server Metadata
  – Certificate
  – Collects Attestations → directory writes
  – Directory read access - some public and some sensitive endpoints
  – Auth server with UDAP JWT-based authentication + policy logic for writes and sensitive data access

• **Organization A - UDAP FHIR client (Requestor)**
  – Client Requesting FHIR data
  – Certificate
Use Case Actors (continued)

- **Organization B - FHIR server B (Responder)**
  - UDAP Server Metadata
  - Registration server
  - Auth server
  - Token endpoint
  - Certificate
  - Serviced by Intermediary when Intermediary is in scope

- **Organization C (Intermediary)**
  - Certificate
  - When present, performs some of the roles for B
Use Case Actors (continued)

- **Patient A**
  - OpenID Connect credentials from Organization A
  - Has received care at Organization B

- **Patient B**
  - Does not have the necessary credentials (negative test)

- **Identity Services (one or more of the following roles)**
  - Remote (online) Identity verification
  - Support of an in-person Identity verification process
  - Authenticate a user and provide an ID Token to the Responder as a trusted OIDC IdP in UDAP Tiered OAuth
## Use Case Roles (Who can do what?)

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Participant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Directory</td>
<td>FHIR API to find all FHIR endpoints of entities in the National Directory and their associated capabilities and attributes</td>
<td>Directory RI, …</td>
</tr>
<tr>
<td>Organization A – UDAP Client</td>
<td>Used by Primary Care Physician to retrieve patient data from Organization B (payer)</td>
<td>UDAP Security RI, EMR Direct, …</td>
</tr>
<tr>
<td>Organization B – Registration* Server</td>
<td>Registers clients to access payer data</td>
<td>UDAP Security RI, Meditech, EMR Direct, …</td>
</tr>
<tr>
<td>Organization B – Auth Server*</td>
<td>Determines whether client is authorized to access requested data</td>
<td>UDAP Security RI, Meditech, EMR Direct, …</td>
</tr>
<tr>
<td>Organization B – Token Endpoint*</td>
<td>Issues token to client for payer data access</td>
<td>UDAP Security RI, Meditech, EMR Direct, …</td>
</tr>
</tbody>
</table>
## Use Case Roles (continued)

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Participant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization C – Intermediary</td>
<td>Distributed access endpoint directory</td>
<td>Directory RI, …</td>
</tr>
<tr>
<td>Patient A - Client</td>
<td>Patient</td>
<td>Identity Matching RI, EMR Direct, …</td>
</tr>
<tr>
<td>Patient B – Client</td>
<td>Patient</td>
<td>Identity Matching RI, EMR Direct, …</td>
</tr>
<tr>
<td>Identity Service – Remote Identity Verification</td>
<td>Authenticate a user and provide an ID Token to the Responder as a trusted OpenID Connect Identity Provider in UDAP Tiered OAuth</td>
<td>Identity Matching RI, …</td>
</tr>
<tr>
<td>Identity Service – In-person identity verification process</td>
<td></td>
<td>Identity Matching RI, …</td>
</tr>
<tr>
<td>Sample Data</td>
<td>Description</td>
<td>Participant</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Endpoint directory - Attestations</td>
<td>Data for new directory entry</td>
<td></td>
</tr>
<tr>
<td>Organization B – Patient A care data</td>
<td>Historical care data for Patient A provided by Organization B</td>
<td></td>
</tr>
<tr>
<td>Identity Service – Credentials</td>
<td>Credentials to authenticate a user</td>
<td>Prior participants: Reuse July credentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New participants: Contact the UDAP Team at</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://www.udap.org/index#contact">https://www.udap.org/index#contact</a></td>
</tr>
</tbody>
</table>
What is the National Directory?
- Provides a generally available method to find all FHIR endpoints and their associated capabilities and attributes, as well as a common process for maintaining the information and validating its accuracy

Objectives
- One national source for validated directory information that is available to any national or local directory workflow environment
- Individual and entity demographics to determine endpoint relationships, computable endpoint information such as accessibility requirements, metadata for routing, trust framework, implementation guides and certification status
- Federated access by HIEs, state directories, EHRs
- FHIR standard implementation guide(s) for use of the directory
National Directory

Validated Healthcare Directory IG (International)

PDex Plan Net IG (US Realm) (Payer Network)

National Directory Exchange IG (US Realm)

Directory Query IG (US Realm)

Attestation and Validation IG (US Realm)
National Directory

- FHIR R4 Base
- US Core
- Endpoint Query (Minimum)
- Enhanced Query
- National Directory

Less Restrictive

More Restrictive
National Directory

- FHIR R4 Base
- US Core
- Endpoint Query (Minimum)
- Enhanced Query
- National Directory

MiHIN

Add IG names
Reference to USCDI

Less Restrictive

Location.new patients

Location.new patients 0..1

Location.new patients 0..1 MS

More Restrictive
National Directory Exchange

• **What is FAST National Directory Exchange?**
  – FHIR API to exchange directory information between the Validated Healthcare / Endpoint Directory and the Federated Healthcare / Endpoint Directories.

• **Objectives**
  – Allows validated directory information to be shared with federated directories for scalability and regional use
National Directory Exchange

• Implementation Guide (September 2022 Ballot)

• Hosted Reference Implementation
  – Server: https://vhdir.meteorapp.com/
  – Client: https://vhdir.meteorapp.com/

• Reference Implementation Code (Apache 2.0 license)
  – https://github.com/HL7-FAST/national-directory

• Confluence
Endpoint Query

• **What is FAST Endpoint Query?**
  – FHIR API to find all FHIR endpoints of entities in the National Directory and their associated capabilities and attributes

• **Objectives**
  – Provide a common, standard method for client applications and systems to find the FHIR endpoints for the entities with which they need to interact
Endpoint Query

• Implementation Guide (September 2022 ballot)
  ─ http://hl7.org/fhir/us/directory-query/2022Sep/

• Hosted Reference Implementation
  ─ Server: https://vhdir.meteorapp.com/
  ─ Client: https://vhdir.meteorapp.com/

• Reference Implementation Code (Apache 2.0 license)
  ─ https://github.com/HL7-FAST/national-directory

• Confluence
**Attestation and Verification**

**What is FAST Attestation and Verification?**

- FHIR API and workflow process for submitting, updating, and attesting and verifying the accuracy of the National Directory information

**Objectives**

- Verifies the accuracy of information submitted to and updated in the National Directory
- Ensures that information distributed to Federated Directories and client applications has been verified to be accurate
Attestation and Verification

- Implementation Guide (September 2022 ballot)

- Hosted Reference Implementation
  - Server: https://vhdir.meteorapp.com/
  - Client: https://vhdir.meteorapp.com/

- Reference Implementation Code (Apache 2.0 license)
  - https://github.com/HL7-FAST/national-directory

- Confluence
FAST Security

• What is FAST Security?
  – Identifying scalable solutions for security authorization and authentication processes.

• Objectives
  – Identifying current industry status security authorization and authentication processes and tools in current clinical interoperability and in advanced digital API use.
  – Building a proof of concept that demonstrates the critical architectural and technical capabilities required to implement user authorization and authentication at point of request and the ability to administer granting and maintaining credentials at scale in multi-stakeholder environments.
  – Creating appropriate national standards and documentation for securing resources and data used in the exchange model.
• Implementation Guide (STU1)
  – https://build.fhir.org/ig/HL7/fhir-udap-security-ig/
• Hosted Reference Implementation
  – URL to be announced
• Reference Implementation Code (Apache 2.0 license)
  – https://github.com/HL7-FAST/udap-security
• Test Scripts
  – https://www.udap.org/UDAPTestTool/
• Confluence
  – https://confluence.hl7.org/pages/viewpage.action?pageId=130482809
**FAST Identity Matching**

**What is FAST Identity Matching?**
- Identify identity-proofing and patient-matching solutions across multiple types of users.

**Objectives**
- Identify appropriate national standards for individual and organizational identity matching.
- Define approach to implementation and testing.
- Identify best practices for reconciliation of identification across multiple sources. (e.g., patient matching)
- Build a proof of concept that demonstrates the critical architectural and technical capabilities required to implement identity cross-walk in real-time during the course of a FHIR transaction.
**FAST Identity Matching**

- Implementation Guide (May 2022 Ballot)

- Hosted Reference Implementation
  - URL to be announced

- Reference Implementation Code (Apache 2.0 license)
  - [https://github.com/HL7-FAST/identity-matching](https://github.com/HL7-FAST/identity-matching)

- Test Scripts
  - [https://github.com/HL7-FAST/identity-matching-test-kit](https://github.com/HL7-FAST/identity-matching-test-kit)

- Confluence
  - [https://confluence.hl7.org/pages/viewpage.action?pageId=130482809](https://confluence.hl7.org/pages/viewpage.action?pageId=130482809)
FAST Hybrid / Intermediary Exchange

• What is FAST Hybrid/ Intermediary Exchange?
  – Guidance enabling one or more intermediaries to participate in FHIR REST interactions, using a passive intermediary approach

• Objectives
  – Provide a unified model that supports both point-to-point interoperability without intermediaries and one in which one or more intermediaries exist – a “hybrid environment”
  – Don’t impose any requirements on the initiating client; the client doesn’t need to be aware that an intermediary is participating
  – Ensure compatibility with other FAST solutions including Security and Directory
FAST Hybrid / Intermediary Exchange

• Implementation Guide (STU 1)

• Confluence
  - https://confluence.hl7.org/pages/viewpage.action?pageId=130482798
Scenario 5: Sharing demographic attributes and/or Digital Identifier within an authorization extension object in UDAP Security's JWT-based authentication
Scenario 5: B2B Match via Authorization Extension Object

• **Overview:** Test sharing demographic attributes and/or Digital Identifier within an authorization extension object in UDAP Security's JWT-based authentication (and as per Carequality FHIR IG)
  - Organization A accesses endpoint directory (National Directory Endpoint Query) to identify public URL for Organization B
    • Organization B’s public endpoint resolves to intermediary, Organization C leveraging National Directory Exchange IG to service Organization B’s FHIR requests
    • Show accessing public endpoint
  - Bonus point: Register (UDAP Security - Registration) and Authenticate (UDAP Security - Authorization and Authentication - B2B) to Directory and obtain a sensitive endpoint (e.g., women’s shelter, other record not publicly listed)
    • Directory RI will populate and secure a sensitive endpoint (Practitioner, PractitionerRole, Restriction)
  - Organization A dynamically registers at Organization B public endpoint (UDAP Security - Registration)
    • Organization B’s public endpoint resolves to intermediary leveraging National Directory Exchange IG
    • FHIR server answering initial discovery request is going to provide the location of its registration endpoint as publicly accessible URL
Scenario 5 (continued)

  • Validating that the listing obtained from the Directory is in fact from the entity via UDAP Server Metadata IG (to confirm with Exchange this is correct?)

Organization A requests $match against Organization B’s public endpoint (FAST Identity) using the Authorization Extension
  • Intermediary receives match request and routes to Organization B’s private endpoint
  • Bonus point: request includes Level 1 IDI
  • Bonus point: response includes Responder’s System Match Output Quality Score from Identity IG in lieu of locally-computed match confidence
  • Bonus point: requestor provides insufficient demographics and is returned with an informative error and no results
  • Bonus point: requestor provides demographics with verification status in $match request and responder’s system appropriately scores match input and uses as input to response policy engine
Scenario 5 (continued)

- Organization B responds with match(es) & associated patient ID(s) and intermediary routes response back to Organization A
- Organization A requests patient information from Organization B public endpoint, using returned patient ID
  - Intermediary receives request and routes to Organization B’s private endpoint
- Success criteria: Organization A obtains health data from Organization B
- Bonus point: the OAuth sign in page allows user to authorize sharing of the Digital Identifier per Identity IG or other PII from user profile directly to Organization B
- Bonus point: OIDC account created in Scenario 2 at Organization A is used to access data at a different system representing Organization B
- Bonus point: OIDC user profile includes account-level identity and/or authentication level of assurance
- Bonus point: OIDC user profile includes verified demographics as in Identity IG