CMS HL7 FHIR Connectathon
HL7 FAST Infrastructure Track Kickoff

June 17, 2022
Agenda

• Connectathon Format
• Track Goals
• Track Agenda
• Track Leads
• Track Scenarios
• Use Case Roles
• Sample Data Required
CMS Connectathon Format

- Participant focused
- Demonstration opportunities – reward testers
- Track Highlights to focus on workflow / use case
- Short, focused testing sessions for each track with three pairs of well-prepared test participants
Track Goals

• 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
CMS Virtual Connectathon Agenda

Tuesday, July 19, 2022
9:00 AM ET – 5:00 PM ET  
Policy Updates / Test Tools

Wednesday, July 20, 2022
8:00 AM ET – 5:00 PM ET  
Track Tools / Testing / Office Hours

Thursday, July 21, 2022
9:30 AM ET – 4:00 PM ET  
Track Highlights – typically 20 minutes
HL7 FAST has 1 hour

*Lunch Break daily from 12:00 PM ET to 1:00 PM ET
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 AM - ET</td>
<td>Welcome from the CMS Administrator</td>
</tr>
<tr>
<td>9:10 AM</td>
<td>Centers for Medicare &amp; Medicaid Services Update</td>
</tr>
<tr>
<td>9:50 AM</td>
<td>Office of the National Coordinator for Health IT (ONC) Update</td>
</tr>
<tr>
<td>10:40 AM</td>
<td>HL7 Implementation Division</td>
</tr>
<tr>
<td>11:10 AM</td>
<td>CMS Support of FHIR For Healthcare Directories</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>FHIR Advancements for Prior Authorization</td>
</tr>
<tr>
<td>1:00 PM</td>
<td>Afternoon Kickoff with the Deputy CIO</td>
</tr>
<tr>
<td>1:30 PM</td>
<td>Opening the Digital Front Door</td>
</tr>
<tr>
<td>2:15 PM</td>
<td>Preparing for the No Surprises Act</td>
</tr>
<tr>
<td>3:00 PM</td>
<td>Delivering Health Equity</td>
</tr>
<tr>
<td>3:30 PM</td>
<td>CMS Electronic Clinical Quality Measures</td>
</tr>
<tr>
<td>4:00 PM</td>
<td>FHIR Connectathon Testing Kick Off and Closing Announcements</td>
</tr>
</tbody>
</table>
Track Demo/Testing - 7/20/2022

• Session 1: 30 – 60 minutes: Scenario / Test Overview
  – Focus on showing observers at a high level what they are about to see from your scheduled testers
  – Point developers to testing resources (RI, test scripts)

• Session 2: 3 20-minute sessions
  – Prepare in advance 3 sets of peer-to-peer testers to test against each other, test tools, or both

• Session 3: 30 minutes: Tester wrap up
  – Who was successful
  – What needs addressed (by the IG / by the participant)
  – Plan what they will demo at the Track Highlight

• Session 4: 60 minutes: Office Hours for participants with questions or who are interested in onboarding to the test tools
Track Schedules – 7/20/2022

• Morning Tracks
  – CARIN BB
  – Burden Reduction
  – CDex
  – Gravity
  – National Directory / Plan-Net
  – Risk Adjustment

• Afternoon Tracks
  – CMS Blue Button
  – Clinical Quality
  – Patient Cost Transparency
  – PDex / Formulary
  – **FAST Infrastructure**
  – Member Attribution
### Track highlights - 7/21/2022

<table>
<thead>
<tr>
<th>START</th>
<th>END</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:30</td>
<td>9:40</td>
<td>Da Vinci Burden Reduction</td>
</tr>
<tr>
<td>9:40</td>
<td>10:00</td>
<td>Da Vinci Clinical Documentation Exchange (CDex)</td>
</tr>
<tr>
<td>10:00</td>
<td>10:20</td>
<td>Da Vinci Member Attribution Track</td>
</tr>
<tr>
<td>10:20</td>
<td>10:40</td>
<td>Da Vinci Patient Cost Transparency</td>
</tr>
<tr>
<td>10:40</td>
<td>11:00</td>
<td>Da Vinci Payer Data Exchange (PDex STU2 inc. Payer-to-Payer)</td>
</tr>
<tr>
<td>11:00</td>
<td>11:20</td>
<td>Da Vinci Payer Data Exchange Formulary and Plan-Net</td>
</tr>
<tr>
<td>11:20</td>
<td>11:40</td>
<td>Da Vinci Risk Adjustment</td>
</tr>
<tr>
<td>11:40</td>
<td>12:00</td>
<td>LUNCH BREAK</td>
</tr>
<tr>
<td>12:00</td>
<td>1:00</td>
<td>FHIR at Scale Taskforce FAST</td>
</tr>
<tr>
<td>1:00</td>
<td>2:00</td>
<td>Blue Button</td>
</tr>
<tr>
<td>2:00</td>
<td>2:20</td>
<td>Gravity SDOH Exchange</td>
</tr>
<tr>
<td>2:20</td>
<td>2:40</td>
<td>PACIO Integration of Post-Acute Care IGs</td>
</tr>
<tr>
<td>2:40</td>
<td>3:00</td>
<td>Clinical Quality Improvement</td>
</tr>
<tr>
<td>3:00</td>
<td>3:30</td>
<td>Connectathon Wrap Up / Final Session</td>
</tr>
</tbody>
</table>

* Subject to change
Track Leads

- Jeff Brown, MITRE  jeffbrown@mitre.org
- Bob Dieterle, EnableCare  rdieterle@enablecare.com
- Abigail Watson, MITRE  awatson@mitre.org
- Sean Mahoney, MITRE  smahoney@mitre.org
- Alex Shankland, MITRE  ashankland@mitre.org
HL7 FHIR At Scale Taskforce (FAST)

- National Directory Exchange
- Endpoint Query
- Attestation and Verification
- Security
- Identity Matching
- Hybrid/Intermediary Exchange

National Directory
Scenario 1

Patient visits Primary Care Physician (PCP)

PCP needs information from Payer

Payer receives PCP request

**Requesting System**

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

**Identity**

7. Requesting system receives data

**Directory**

**Intermediary**

Optional: Forwards the Exchange

3. Receives transaction, validates requestor, validates version
4. Performs Patient Matching and sends back Not Found if unable to do so
5a. Authenticates FHIR user's role
5b. Filters out data that does not have consent
6. Generates & returns FHIR response

**Conformance & Certification**

**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

PCP views patient information

Patient visits Primary Care Physician (PCP)

PCP needs information from Payer

Payer receives PCP request
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 allow 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 Primary Care Physician (PCP)

PCP needs information from Payer

Payer receives PCP request

**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

**IDENTITY**

**REQUESTING SYSTEM**

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

**INTERMEDIARY**

Optional: Forwards the Exchange

3. Receives transaction, validates requestor, validates version
4. Performs Patient Matching and sends back Not Found if unable to do so
5a. Authenticates FHIR user’s role
5b. Filters out data that does not have consent
6. Generates & returns FHIR response

**RECEIVING SYSTEM**

7. Requesting system receives data

**CONFORMANCE & CERTIFICATION**

SECURITY
Scenario 2

- **Overview:** Patient A visits Organization B for an appointment; Organization B identity proofs Patient A and collects information during patient registration
  - Prerequisite: other testing participants know Patient A details, which can be shared on this worksheet
  - [Scenario may define specific ID proofing levels for A/B, or one of the orgs proofs according to the IG and the other doesn’t; this can be indicated in the authorization extension object or user profile data; layer on more specifics once Identity IG offers attribute validation grammar]
  - 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 A's identity at a target level of assurance as per Guidance on Identity Assurance within [Identity IG](#)
  - Patient A 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 A 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 (B2B with or without Intermediary)

<table>
<thead>
<tr>
<th>REQUESTING SYSTEM</th>
<th>INTERMEDIARY</th>
<th>RECEIVING SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prerequisites</strong></td>
<td><strong>Optional:</strong> Forwards the Exchange</td>
<td><strong>Optional:</strong> Generates &amp; returns FHIR response</td>
</tr>
<tr>
<td>Patient identity verification &amp; minimum demographics collection by Payer per Guidance on Identity Assurance, Patient Matching. Optional: Create Digital Identity. Optional: Record attribute verification status.</td>
<td>Receives transaction, validates requestor, validates version</td>
<td>Filters out data that does not have consent</td>
</tr>
<tr>
<td><strong>Requesting System</strong></td>
<td></td>
<td><strong>Identity</strong></td>
</tr>
<tr>
<td>PCP needs information from Payer</td>
<td>Performs Patient Matching and sends back Not Found if unable to do so</td>
<td><strong>Identity</strong></td>
</tr>
<tr>
<td>Patient visits Primary Care Physician (PCP)</td>
<td></td>
<td><strong>Payer receives PCP request</strong></td>
</tr>
<tr>
<td>Formulates FHIR request</td>
<td>Authenticates FHIR user's role</td>
<td><strong>Payer views patient information</strong></td>
</tr>
<tr>
<td>Looks up the FHIR endpoint for recipient</td>
<td></td>
<td><strong>Requesting system receives data</strong></td>
</tr>
<tr>
<td><strong>Receiving System</strong></td>
<td></td>
<td><strong>PCP needs information from Payer</strong></td>
</tr>
<tr>
<td>Payer views patient information</td>
<td></td>
<td><strong>Generates &amp; returns FHIR response</strong></td>
</tr>
<tr>
<td><strong>Optional:</strong> Performs Patient Matching and sends back Not Found if unable to do so</td>
<td></td>
<td><strong>Generates &amp; returns FHIR response</strong></td>
</tr>
</tbody>
</table>

### Requesting System
- **PCP needs information from Payer**
- **Generates & returns FHIR response**

### Receiving System
- **Payer receives PCP request**
- **Payer views patient information**
- **Generates & returns FHIR response**
Scenario 3

- Overview: Organization A has a need for information held by Organization B. Organization B uses an intermediary (Organization C) to receive FHIR requests on its behalf.
- Note: Intermediary w/ transparent reverse proxy only; this same workflow can also be tested without an intermediary
  - 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 3 (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)
  • 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
— 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
Scenario 4 (Patient Directed Exchange)

**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
4. Receives transaction, validates requestor, validates version
5a. Performs patient authentication via Digital Identity, Patient Matching & sends back patient ID or Not Found
5b. Authenticates FHIR user's role
6. Filters out data that does not have consent (patient authorization)

**RECEIVING SYSTEM**
- Generates & returns FHIR response

**IDENTITY**

**PCP views patient information**

**Payer receives PCP request**

**Patient visits Primary Care Physician (PCP)**

**SECURITY**

**CONFORMANCE & CERTIFICATION**
Scenario 4 (Patient Directed Exchange)

- **Overview:** B2C scenario with UDAP Tiered OAuth, with Identity IG's Digital Identity including an OpenID Connect credential (with an 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 and with JWT-based Authentication B2C (instead of B2B)
  - 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 endpoint (UDAP Security - Registration)
  - Organization B’s 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

  - Validating that the listing obtained from the Directory is in fact from the entity via UDAP Server Metadata IG
  - Bonus Point: Organization B has records for Patient A via exact match on Patient A’s Digital Identifier (e.g. Patient A had previously registered their Digital Identity and this Digital Identifier issued by Organization A at Organization B)
  - Bonus Point: Organization B has records for Patient A via single high confidence match on demographics in the ID token from Organization A commensurate with those required in IDI Level 1

- Organization B returns token response and intermediary routes back to Organization A

- Organization A requests health data from Organization B’s endpoint
  - Intermediary receives request and routes to Organization B’s private endpoint
Scenario 4 (continued)

- Bonus point: ID token includes insufficient demographics or Digital Identifier is unknown and is returned with an informative error and no results
- Bonus point: requestor provides demographics with verification status in ID token and responder's system appropriately scores match input and uses as input to response policy engine
- Bonus point: Organization B performs other out of band interaction with Patient A that enables use of their Digital Identity to access health data

  - 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 user profile includes account-level identity and/or authentication level of assurance
  - Bonus point: OIDC user profile includes verified demographics as in Identity IG
Scenario 5 (B2B-Mediated Patient Access via Authorization Extension Object)

**REQUESTING SYSTEM**

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

**INTERMEDIARY**

3. Optional: Forwards the Exchange
4. Receives transaction, validates requestor, validates version
5a. Performs Patient Matching via Authorization Extension Object & sends back Not Found if unable to do so
5b. Authenticates FHIR user’s role
6. Filters out data that does not have consent
7. Generates & returns FHIR response

**RECEIVING SYSTEM**

Payer receives PCP request

**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

**IDENTITY**

PCP views patient information

**SECURITY**

Patient visits Primary Care Physician (PCP)

PCP needs information from Payer

Payer receives PCP request

**CONFORMANCE & CERTIFICATION**

PCP views patient information
Scenario 5 (B2B-Mediated Patient Access via Authorization Extension Object)

- **Overview:** Test sharing demographic attributes within an authorization extension object in UDAP Security's JWT-based authentication B2B (and as per Carequality FHIR IG) in a Patient Access workflow not requiring patient credentials at the responder’s organization
  - 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
  - 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)
  - 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)

Organization A requests access token for Organization B’s public endpoint (UDAP Security - Authorization and Authentication - B2B) with verified minimum required demographics for the carequality_user that uniquely specify an individual that is the patient user (FAST Identity) included in the Authorization Extension Object (Carequality FHIR IG)

- Validating that the listing obtained from the Directory is in fact from the entity via UDAP Server Metadata
- Intermediary receives token request and routes to Organization B private endpoint

Organization B returns an access token if the user is an exact match and intermediary routes response back to Organization A; otherwise an error is returned

- Bonus point: requestor provides insufficient demographics and is returned with an informative error and no results
- Bonus point: requestor includes Digital Identifier in Authorization Extension Object and responder’s system matches on this identifier on its own or in addition to other demographics

Organization A performs a $match operation against Organization B public endpoint and obtains patient ID(s)

- Organization B will only return patient ID(s) for patients that the user is authorized to see

Organization A requests health data for the patient from Organization B public endpoint

Intermediary receives request and routes to Organization B private endpoint

- Success criteria: Organization A obtains health data from Organization B
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

• **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, …</td>
</tr>
<tr>
<td>Organization B – Registration* Server</td>
<td>Registers clients to access payer data</td>
<td>UDAP Security RI, …</td>
</tr>
<tr>
<td>Organization B – Auth Server*</td>
<td>Determines whether client is authorized to access requested data</td>
<td>UDAP Security RI, …</td>
</tr>
<tr>
<td>Organization B – Token Endpoint*</td>
<td>Issues token to client for payer data access</td>
<td>UDAP Security RI, …</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
<td>Participant</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<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, …</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>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>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></td>
</tr>
</tbody>
</table>
## Test Sessions

<table>
<thead>
<tr>
<th>Test Session</th>
<th>Time</th>
<th>Tester 1</th>
<th>Tester 2</th>
<th>What to demo?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test session 1</td>
<td>2:00 – 2:20pm ET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test session 2</td>
<td>2:20 – 2:40pm ET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test session 3</td>
<td>2:40 – 3:00pm ET</td>
<td></td>
<td></td>
<td></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

FHIR R4 Base

US Core

Endpoint Query (Minimum)

Enhanced Query

National Directory

MiHIN

Add IG names
Reference to USCDI

Location.new patients

Location.new patients 0..1

Location.new patients 0..1 MS

Less
Restrictive

More
Restrictive

HL7 International
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 (Pre-ballot)
  - https://build.fhir.org/ig/HL7/fhir-directory-exchange

- 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

- Test Scripts
  - https://github.com/HL7-FAST/test-scripts

- Confluence
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 (Pre-ballot)
  – http://build.fhir.org/ig/HL7/fhir-directory-query

• 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

• Test Scripts
  – https://github.com/HL7-FAST/test-scripts

• 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 (Pre-ballot)
  — http://build.fhir.org/ig/HL7/fhir-directory-attestation

• 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

• Test Scripts
  — https://github.com/HL7-FAST/test-scripts

• 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.
FAST Security

• Implementation Guide (STU1)
  – https://build.fhir.org/ig/HL7/fhir-udap-security-ig/

• Hosted Reference Implementation
  – Under development

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

• Test Scripts
  – https://github.com/HL7-FAST/test-scripts

• 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 (Pre-ballot)
  - https://build.fhir.org/ig/HL7/fhir-identity-matching-ig/
- Hosted Reference Implementation
  - Under development
- Reference Implementation Code (Apache 2.0 license)
  - https://github.com/HL7-FAST/identity-matching
- Test Scripts
  - https://github.com/HL7-FAST/test-scripts
- Confluence
  - 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)

• Hosted Reference Implementation
  – TBD

• Reference Implementation Code
  – TBD

• Test Scripts
  – TBD

• Confluence
Questions

• Jeff Brown, MITRE  jeffbrown@mitre.org
• Bob Dieterle, EnableCare  rdieterle@enablecare.com
• Abigail Watson, MITRE  awatson@mitre.org
• Sean Mahoney, MITRE  smahoney@mitre.org
• Alex Shankland, MITRE  ashankland@mitre.org

Zulip Stream: https://chat.fhir.org/#narrow/stream/323104-FAST

Track Page: https://confluence.hl7.org/pages/viewpage.action?pageId=94659608