FHIR at Scale Taskforce (*FAST*)

Proposed Solutions Working Document: Identity

Table of Contents

Revision History

Version	Date	Author	Description of Change
0.5	07/25/2019	Meena Jambulingam Julie Maas	Initial draft
0.6	7/26/19	Julie Maas	Minor corrections
0.71	10/25/19	Nicole Antonson, Julie Maas	Added content to work in to Solution 1 details
0.8	11/5/19	Julie Maas	Added Solution 2 details and a few clarifications to Solution 1
0.81	11/5/19	Julie Maas	Added final 2 sections to Solution 2
.9	03/08/20	Carmen Smiley	Updated based on TLC webinar feedback and team discussions
1.1	3/14/20	Julie Maas	Add to Identity section and Solution 4 details, working toward our v2.
1.2	3/31/2020	Meena Jambulingam	Updated introductory sections based on team feedback and working session with Catherine Schulten and Rita Torkzadeh
1.3	4/28/2020	Dana Marcelonis	Added solution overview/comparison matrix to introduction, added Best Practice Section at end of doc and moved content related to identity assurance, matching best practices and KPIs; moved Security overlaps/topics/to dos to Appendix; added Solution Advantages/Disadvantages to Appendix as a future 'to do' item; inserted comments from 4/22 team meeting and started resolving team comments inserted into the document
1.4	5/142020	Dana Marcelonis	Added Solution Limitations section to end of document, cleaned up tracked changes where items were moved to a different section of the doc
1.5	5/27/2020	Meena Jambulingam, Dana Marcelonis	Meena accepted tracked changes from last round of edits; Dana added Julie's clarifications to solution #4 description on page 7; inserted notes from 5/27 Tiger Team meeting; moved the task to define relevant use cases/core capabilities as a 'to do' in the appendix; re-ordered solutions so that solution #2 (collaborative identifier for patient matching) becomes solution #1)
1.6	5/28/2020	Dana Marcelonis	Incorporated revisions from team meeting 5/28

1.7	5/30/2020	Dana Marcelonis	Clarifications involving identifier language from Collaborative solution. Julie, Annelise, Catherine's changes consolidated.
1.8	6/4/2020	Dana Marcelonis	Swapped solution order so that Networked Identity Management is now solution #3 and Distributed Identity Management is now solution #4. Updated diagram numbering.
1.9	6/17/2020	Meena Jambulingam, Julie Maas	Final edits before SME Prep Session on Jun 18th 2020

Proposed Solutions: Identity

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 patient identity management. This document will outline proposed solutions to address these issues and capabilities.

Reference Documentation

- *FAST*-Technical Barriers
- *FAST*-Regulatory Barriers
- *FAST*-UC-Authentication_and_Authorization-Core_Capability-CC2
- *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

FAST FHIR AT SCALE TASKFORCE MODEL

Accelerate Use of FHIR

Identify

Barriers to adoption and opportunities for synergy:

- Endpoint Services
- Security Approaches
- Identity Resolution
- Versioning & Scale Approaches
- Testing Approaches
- Regulatory/Policy Needs

Why

Removing barriers and aligning consensus-based adoption via the network effect will accelerate adoption of FHIR for the production exchange of clinical information between providers and payers

How

Analyze **—** look, learn, understand FHIR pilots/prototypes/deployments underway

Synthesize **—** Subject Matter Expert (SME) evaluation, identify trouble spots, develop best practices and proposed solutions

Catalyze **—** through additional standards work, barrier identification, testing, pilots, and leveraging existing resources

Current State Overview

With CMS and ONC publishing final rules on May 1, 2020, (Interoperability and Patient Access rule and 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program), there is an increased emphasis on FHIR adoption for information exchange. Patients must be able to obtain their health records from providers and payers, and payers and providers need to exchange information on behalf of the patient. Solving identity management at scale becomes necessary to support these regulatory requirements. How do these patients, providers and payers identify the correct patient information to share? How can a requester and receiver participating in a data exchange using FHIR, uniquely identify the patient?

Increased need for cross-organizational matching across the industry and a lack of ecosystem-wide standards development, harmonization, and implementation, as well as publication of best practices, motivates the development of scalable solutions to this problem.

Problems to be Solved

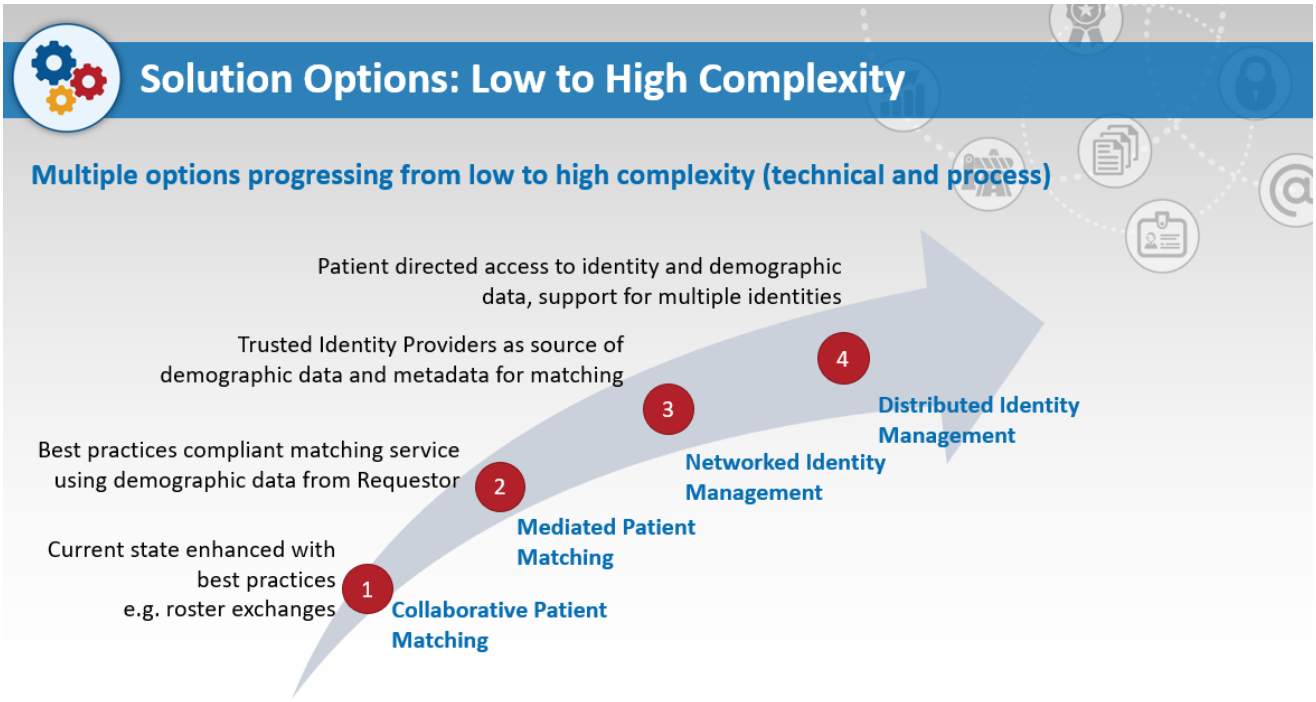
The following technical and regulatory barriers to patient identity management identified by the *FAST* Identity Tiger Team were found to impede the adoption of FHIR at scale and will be the basis for *FAST*-proposed scalability solutions. Similar challenges exist with provider identity matching, though perhaps less complex. Provider identity matching is currently out of scope for this document, but will be addressed in future versions as a separate effort.

1. **Use of Different Identifiers:** How do we know who the patient is? Patient identifiers such as medical record numbers and insurance IDs are not often meaningful beyond the boundaries of a specific organization or healthcare entity, limiting their value in patient identity matching across organizations. In our proposed solutions, we look at approaches to expand the usage of organizational identifiers to address this limitation.
2. **Custom Identity Matching Processes:** Can we rely on the consistency of identity-matching services across organizations? Most organizations utilize custom technical approaches and processes and any proposed solutions from *FAST* will need to accommodate this diversity.
3. **Cross-Walks are Not Scalable:** How do we map patient identity real-time? Small groups of organizations may exchange patient and provider rosters and/or agree on a shared minimum demographic data set, thereby building a common cross-walk for identifiers. This solution is not scalable at the national level and real-time identification may be impacted by data quality, availability, completeness and latencies in maintaining cross-walks.
4. **Minimum Demographic Data Set:** How do we know the minimum patient data to use in matching? Reliably identifying patients across organizations may require a minimum necessary set of demographic data to be included in the transaction, which may not always be available for all use cases.
5. **Metadata**: How do we know the accuracy or quality of the patient data used in matching? Metadata on patient demographic data, e.g., date of last update, characteristics of identity verification event(s) underpinning the patient demographics and the relationship between the two, may assist organizations in their matching efforts, yet may not be supported by current standards and approaches.

6. **FHIR Identifiers**: Can we rely on current specifications to exchange the data needed for matching? Implementation Guides and FHIR resources may not require patient identifiers needed to enable identity cross-walks, as some identifiers may be optional or not all identifiers may be supported.
7. **Privacy:** What patient data should be included in requests and returned in responses, including error messages? How do we address the misidentification risk? When is consent needed? Considerations must be applied in developing recommendations on data exchanges for various scenarios, such as attributes to include in successful responses to exact match requests, error messages, overlay scenarios, and when to permit non-exact matches. Privacy and security considerations should be analyzed in tandem with the FAST Security Tiger Team.
8. **Current Legislation:** The current legislation restricting the use of HHS funds to promulgate or adopt any final standard providing for, or providing for the assignment of, a unique health identifier of an individual until legislation is enacted specifically approving the standard forces the industry to rely heavily on demographic information, which can lead to errors, when dealing with demographic and clinical information from multiple sources. There have been improvements in probabilistic matching, but the industry should also look toward other possible solutions or combinations of solutions that may be tailored to the patient population and context, while still flexible and scalable to accommodate a wide variety of needs.

Recommended Future State & Intermediate Steps

The *FAST* Identity Tiger Team expects that the industry will be operating in a hybrid environment where there is not a one-size-fits-all approach to patient identity matching for the near-term. The team is recommending a spectrum of solution options ranging from technically simple and less scalable to complex and more scalable, with the understanding that given the current state of the industry, organizations may not be ready or capable to implement the most complex solutions. The team is providing guidance for implementers to determine when they would choose one solution over another, depending upon the current state of their technology and exchange scenarios. The benefit of documenting the proposed solutions included in this document is that implementers will be able to leverage the *FAST* team's recommendations, rather than having to perform their own analysis to get started and potentially create additional implementation variations. The goal is to provide a common set of patterns for the industry to gravitate toward. Therefore, the team has identified four solutions as best practices for achieving reliable patient identity management. These proposed solutions are not final, and will continue to be refined by obtaining industry feedback through collaboration with other industry initiatives, and *FAST*-hosted Subject Matter Expert (SME) Review Sessions.



1. **Collaborative Patient Matching:** Relies on use of pre-established patient identifiers known to both requesting and responding entities. Partner organizations may establish a unique identifier for each shared patient to be used when requesting/returning information between them.
    - Option A: Partner organizations share and pre-match their patient rosters, and determine an identifier to be used for each shared patient. The partners either…
        - define a new, unique identifier for each common patient identified through the cross-walk exercise
        - or choose to use an existing identifier as the common ID for the patient, such as an existing identifier issued by a third party but recognized by both partners, or an identifier issued by one of the partners

    For example:
    - Payer shares member roster with provider including member IDs in advance of data exchange
    - Patient shares insurance card with provider/requesting organization, provider/requesting organization passes medical record number and insurance member ID to payer, payer then has the patient's medical record number that could be used to request data from the provider regarding the same patient in the future

2. **Mediated Patient Matching:** Intermediary service or responder performs demographics-based matching at the time of each request. Key characteristics:
    - Matches are determined at the time patient information is needed; there is no pre-sharing of patient demographics among participants nor pre-matching.

- Matching is based on patient demographics. No common patient ID is established for use across participants.
- Matching may be performed by the responder or by its agent.

3. **Networked Identity Management:** Parties rely on the OpenID Connect provider's digital certificate and an OpenID identifier assigned to each user - as part of an onboarding process that includes identity proofing and establishes their real-world identity - and the validity of demographics made available for patient or provider matching. Responders validate the trustworthiness of the associated identity provider via its digital certificate and use the recorded patient or provider OpenID identifier and other verified user profile data to match on the identifier or (if the identifier is not yet known in their system) fall back to a demographics-based matching process.

4. **Distributed Identity Management:** A trusted third-party identity matching service maintains patient identities and associated identifiers assigned by different parties. During a patient information request, the requester asks the matching service to identify the patient and resolve her identity to an identifier recognized by the responder. Relies on a networked set of trusted identity providers to perform matches using patient demographic data.

The team has also outlined the following best practice recommendations to be considered and applied to all the proposed solutions:

1. Best practices for Identity Matching Services
2. Recommended Key Performance Indicators (KPIs) for Identity Matching Services
3. Best practices for Identity Assurance

Note that solutions for Consent Management at scale will be required to complete end to end solution recommendations from *FAST.* The Identity and Security Tiger Teams will collaborate on defining solution options. This work has been deferred until the initial set of proposed solutions have been reviewed by SMEs and the Technical Learning Community.

Proposed Solution Overview

The following matrix provides a comparison view of the proposed solutions described in this document to assist readers in determining which solution(s) best meet their needs for patient matching. The intent is not to describe current industry practices, but to provide a summary of the best practice solutions proposed by the *FAST* team.

	Collaborative Identifier for Patient Matching	Mediated Patient Matching	Networked Identity Management	Distributed Identity Management	Comments
Capabilities that Requestors/Responders Must Support					
Responder must support patient $match operation as well as recommended best practices	Optional	X	X	X	
Requestor must be capable of sending minimum data	X	X		X	
Exchange partners have set up steps prior to exchange (e.g., roster exchange)	X			X	
Support for digital identity			X	X	
Additional technology needed beyond FHIR (Open ID Connect, OAuth2, Tiered OAuth…)			X	X	Solution 3 – Identity propagation to every node Security team recommending support for Tiered OAuth always required?
Subject identity-proofing pre-requisites (IAL2)			X	X	**To Do:** Some of these solutions wouldn't require an IAL level, need to discuss for each solution
Entity Characteristics					
Participants in the exchange are known/discoverable to each other	X	X	X	X	

Contractual terms/ ecosystem participation agreement is in place	X	X	X	X	Regardless of solution, some kind of agreement in place
Trusted 3rd party certifier/verifier confirms compliance with contractual/ecosystem participation agreements		X	X	X	Collaborative – agreement between 2 parties; no 3rd party verifier
Data Requirements					
Type of identifiers (e.g., Tax ID, Driver's License, etc.) being used by exchange partners are recognized by each other	X	X	X	X	Need to add privacy considerations—e.g. constraints on sharing and storing SSN or any proxy thereof such as an identifier derived from SSN.
Identifiers themselves are recognized/discoverable by each exchange partner	X	N/A	X	X	Solution 1 – two partners' own business identifiers Solution 2 (mediated) – relying on demographics for the match Solution 3 (distributed) – exchange partner has to look up identity on a network node Solution 4 (networked) – identifier/name space – network participants sharing info, would know what ID is
Minimum set of patient demographic data REQUIRED	X	X	X	X	
Metadata for patient demographics RECOMMENDED (e.g., lastUpdated, level of identity verification)	X	X	X	X	Useful for adjudicating duplicates, currency of data

					Does Provenance play into this?
Problems Addressed					
Entity use of different patient identifiers	X	X	X	X	
Industry use of variety of approaches	X	X	X	X	
Exchange of patient rosters/crosswalks is not scalable		X	X		**To Do:** Is there something about solutions 1 and 3 that make the crosswalk approach more scalable? Best practice Patient IAL2 proofing establishes a stronger demographics entry in the medical record that includes a verified insurance identifier or mobile number and email address. • Not scalable today because we don't know where all the endpoints are… directory makes that easier • First initial bulk exchange, but near real-time APIs means you can trigger updates and not rely on bulk exchanges • Etc…
Minimum demographic data set not available			X		Function of workflow process (minimum demographics aren't available in clinical record) – haven't necessarily introduced a solution that makes that better?

					Need to think through whether there are any recommendations that can be made considering this
Metadata on patient demographic data not always supported			X		Assuming same as above This can be required of compliant OIDC credentials.
FHIR IGs may not require or support patient identifiers needed			X		OIDC can include identifier that references other demographics in a discoverable way.
Capability to specify an exact match	X	X	X	X	**To Do:** Do we need another matrix to identify how each solution deals with exact matches vs. not?
Scenario/Workflow Characteristics					
Payer/Payer exchange	X	X	X	X	Workflows not directly involving the patient do require that patient's ID is established in both places beforehand OR that it is established at requestor & that the identity service must answer a $match request from responder.
Provider/Provider exchange	X	X	X	X	
Payer/Provider exchange	X	X	X	X	
Patient/Provider exchange			X		
Patient/Payer exchange			X		

Key Terms and Definitions

The solutions described here use the following guidelines, terms and definitions from NIST Special Publication 800-63-3 and other NIST publications as noted.

- **Digital Identity** is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real[1]-life identity is known.[1]

  ***Note**: In the FAST proposed solutions, digital identities involved in FHIR transactions may represent Patients, Providers, Payers, and other Healthcare actors.*

- **Identity proofing** establishes that a subject is who they claim to be.

  The degree or strength of the proofing process is expressed in terms of the **Identity Assurance Levels (IALs)** established by NIST 800-63-3:

  IAL1: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a Credential Service Provider, or CSP, asserts to an RP[2]).

  IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

  IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

  Digital Authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity. For services in which return visits are applicable, successfully authenticating provides reasonable risk-based assurances that the subject accessing the service today is the same as that which accessed the service previously.

- **Authenticator Assurance Levels (AALs)** as defined by NIST 800-63-3:

  AAL1: AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a wide

[1] The assigner must implement procedures that prevent duplicates from being created in their local system. [2] Relying Party

range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.

AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.

AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication SHALL use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device MAY fulfill both these requirements. In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

***Note**: FAST proposed Identity solutions assume that authentication at an acceptable AAL has occurred prior to the transaction.*

- **Federation Assurance Level (FAL)**: NIST SP 800-63C provides requirements when using federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application. In addition, this volume offers privacy-enhancing techniques to share information about a valid, authenticated subject and describes methods that allow for strong multi-factor authentication (MFA) while the subject remains pseudonymous to the digital service.

  FAL1: Allows for the subscriber to enable the RP to receive a bearer assertion. The assertion is signed by the IdP using approved cryptography.

  FAL2: Adds the requirement that the assertion be encrypted using approved cryptography such that the RP is the only party that can decrypt it.

  FAL3: Requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself. The assertion is signed by the IdP and encrypted to the RP using approved cryptography.

  ***Note**: FAL is applicable to the Distributed Identity Management solution and the Networked Identity Management solution. See applicable sections for recommended FAL for each.*

- **Biometric characteristics** are unique personal attributes that can be used to verify the identity of a person who is physically present at the point of verification. They include facial features, fingerprints, iris patterns, voiceprints, and many other characteristics. NIST SP 800- 63A, *Enrollment and Identity Proofing* recommends that biometrics be collected in the enrollment process to later help prevent a registered subscriber from repudiating the enrollment, and to help identify those who commit enrollment fraud.

***Note**: In the proposed solutions, biometrics are referenced only in the context of identity resolution and not in the context of Authentication.*

- **OpenID Connect** 1.0 ("OIDC") is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.[2]

- T**iered OAuth** is an extension of OpenID Connect and OAuth 2.0 that allows a Responder, faced with authenticating a user and making an authorization decision, to take on the role of client and make a "tiered" authentication request to another OIDC provider instead of relying on its own authentication system. As client, the Responder can then obtain user profile information to use in its decision to authorize access to resources it secures.[3]

[2] https://openid.net/connect/
[3] http://www.udap.org/udap-user-auth.html

Proposed Solutions

Reliable Patient Identity Management
Solution #1 Collaborative Patient Matching

Overview & Description

The solution described here applies to scenarios where two parties have agreed upon the use of mutually known identifiers, and represents the process often used between exchange partners today. The *FAST* team recommends best practices that can be applied to address gaps that currently exist within this type of exchange.

The Requestor Actor and Responder Actors can be either a provider or a payer as the solution applies to provider to provider, provider to payer, and payer to payer transactions.

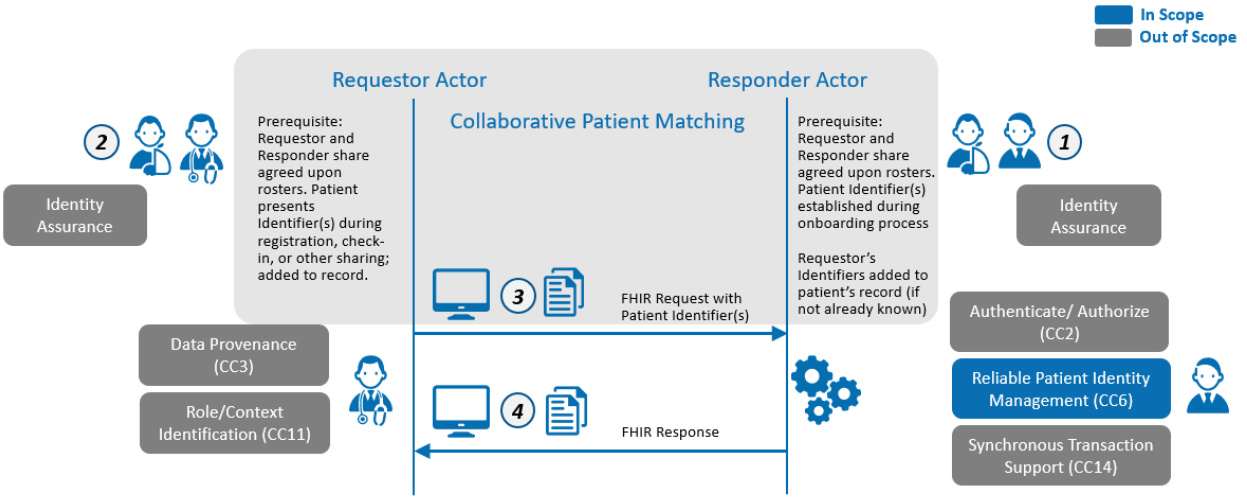
The patient's identity in this scenario is established by the Requester and Responder Actors as part of their onboarding process that includes appropriate validation, or may be established by another trusted organization. These trusted organizations have large memberships, already enumerate their members/customers, have the technical abilities to manage identities (i.e., "know your customer", identity assurance), and have the infrastructure to interoperate with relying parties who need to collect or confirm an identifier via request/response (e.g., banks, credit bureaus, associations to which the patient belongs such as AARP, etc.).

Supporting Diagrams & Flows

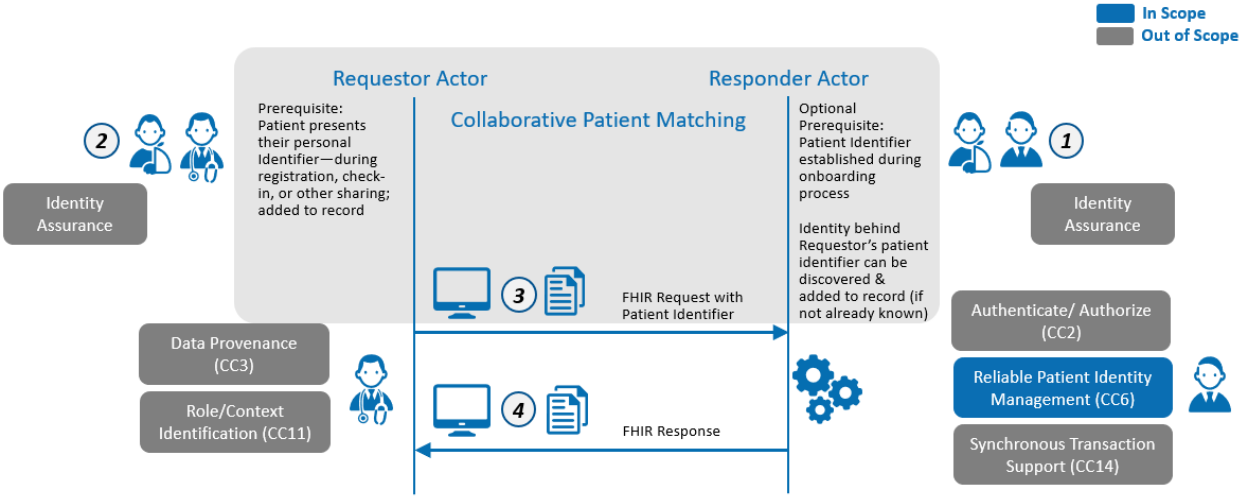
- Each locally established business identifier will have minimum metadata and verification constraints and is designed for cross-walking between the many systems necessary for successful patient matching in health information exchange.
    - Requirements:
        - Unique within organizational boundaries of the exchange partner "assigner"/number is not reusable for a different person
        - Can be stored as an identifier in FHIR Patient resource and therefore used in $match operations or searches
        - IDs with date issued, expiration date, or validity periods will contain this metadata when available.
- Patient provides their identifier(s) to a healthcare organization at registration and/or check-in, and the identifier(s) is/are then associated with the patient's record. As an alternative to in-person binding to the record, patient rosters could be shared that describe how to associate each patient medical record number and insurance identifier pairing, for example, to manage identities at scale.
- FHIR request occurs in a single transaction where the two business Identifiers (or a single identifier, defined from the two) is embedded right into the query, so there is no separate "match" step required.
- Results are returned if the responding system has content to which the requestor is authorized.

Proposed Solutions: Identity

Proposed Solution 1a: Collaborative Patient Matching – Roster



Proposed Solution 1b: Collaborative Patient Matching – Known ID



ID	Description	Notes
1	As a foundational pre-cursor, the Requestor Actor and Responder Actor must verify the patient's identity to the best of their ability. Please refer to the Best Practices for Identity Assurance section. Identifier will have minimum metadata and verification constraints and is designed for cross-walking between the many systems necessary for communications and management of patient care. Requirements: • Identifier should be a UUID - unique between organizational boundaries of the involved exchange partners and over time • These UUIDs should not be reassigned (Identifiers such as insurance IDs, MRNs are often used in matching today, but this can be a problem due to their reuse. The recommendation is not to soley rely on an identifier that is reusable for a different person) • UUID should include a prefix associated with the entity that assigned the identifier so that systems can easily route requests for ID confirmation to the right entity, and reduce/remove the chance for identifier collision (e.g., AARP applies prefix 'RP', TransUnion applies prefix "TU", and Capital One applies prefix "T1") Generate an Identifier (+ Assigner) available in FHIR Patient resource for use in a one-pass query for records, or used as one or two elements along with other required demographics in a $match operation or search • Note: Diagram shows identifier being issued at responder and then used by requestor, however the converse also works when the patient presents the identifier to both entities.	To Do:

2	Patient associates their record with the Identifier at registration and/or check-in, or presents their identifier to a healthcare organization that then associates the identifier with the patient's record. As an alternative to in-person binding to the record, patient rosters could be shared that describe how to associate patients with these identifiers at scale.	
3	FHIR request occurs in a single transaction where the Identifier is embedded right into the query workflow, so no separate "match" step is required. Refer to Solution 2 for $match details.	
4	Results are returned if the responding system has content to which the requestor is authorized.	•

Pre-Conditions

- Identity Assurance has occurred at either IAL1 or IAL2. Note: even with IAL2, it is possible that while the identity has been established in the real world, the data associated with that identity may not always be the most current e.g. the patient's proofed address may be different than their current address due to a recent move.

In Scope

- Identity matching using FHIR transactions involving mutually agreed on, known identifier(s)

Out of Scope

- Security capabilities such as Authentication and Authorization
- Service and endpoint discovery
- Patient as requestor or responder

Assumptions

- The Requestor Actor and Responder Actor have an established business relationship
- The Requestor Actor and Responder Actor have access to a mutually agreed upon list of Patient Identifiers.
- Responders should be able to handle $match request
- Patient Identifiers are issued as part of onboarding process. Patient presents identifier during registration and/or check-in
- Patient interacts with both payer and provider; provider interacts with both healthcare organization and payer; leverage proofing done by both exchange partners to increase match confidence, obviating need for probabilistic match
- Not all patients have insurance

Complexity Rating

- **Medium**: Builds on existing technology solutions, but requires significant process changes and integration requirements

Proposed Solution Status: In Progress

- Requirements for Patient Identifiers to be used in this solution
  - Validated
  - Identity proofing process at a minimum establishes that a unique individual is represented by each Identifier
  - Unique for all time within the assigner's system
- Identifier (combination of medical record # plus insurance # OR email address + mobile) can't be reassigned to a different individual and patient onboarding process requires that patient assert uniquely represents them
  - FHIR-ready
  - Assigner recognizes this identity for patients in its system as a Patient.identifier resource element and responds to queries that use this Identifier as a search parameter
  - Additional Patient attributes to include along with the Identifier when querying
    - First, Last, DOB
- Requestor's Identifier
  - In the "separate business identifiers" model; for later queries in the other direction

Open Items

- Define namespaces and identifiers for Assigners (how to express & use in HL7 FHIR)
- Security considerations and data protections for the Identifier
  - See Solution 4 for criteria to step up one of these local business identifier to a trusted identity.
- Other general best practices & building blocks for use of collaborative matching
  - Support for FHIR Match operation by health systems, to validate medical record numbers and by payers to validate insurance identifiers
- Roster sharing practices/minimum metadata when matching
- Workflow for using these identifiers in Individual Access request, Meaningful Choice, Consent
- Additional properties of the Identifier

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
Map to annotated diagram components above	List components proposed in solution diagrams above	New or if Existing, what is the existing component	If new, describe what needs to be built. If existing, describe what needs to be modified or enhanced.	Who owns building the new component or making the proposed

				modifications?
1	Onboarding; issue identifier	New/May exist and need to be utilized differently	Perform any required identity verification and establish identifier meeting requirements	Payer, Provider, or 3rd party service
2	Identifier presented	New	Participants need to build accommodation for new identifiers and assigners. Patient confirms association of identifier or is associated with identifier through a shared roster (other matching steps may be embedded within this roster exchange)	All Participants
3	FHIR Query	New	FHIR services must accommodate new identifier/assigner	
4	FHIR Response	Existing		

Key Impacts to Timeline & Cost

<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
1	Onboarding; issue identifier	Small/Medium	Depends on identity verification, data element verification requirements
2	Identifier presented	Medium	Point of care and insurance onboarding systems will need to add new identifier entry and storage
3	FHIR Query	Small	FHIR systems will need to accommodate new identifiers
4	FHIR Response	None	This should be no change from how FHIR resources are returned today

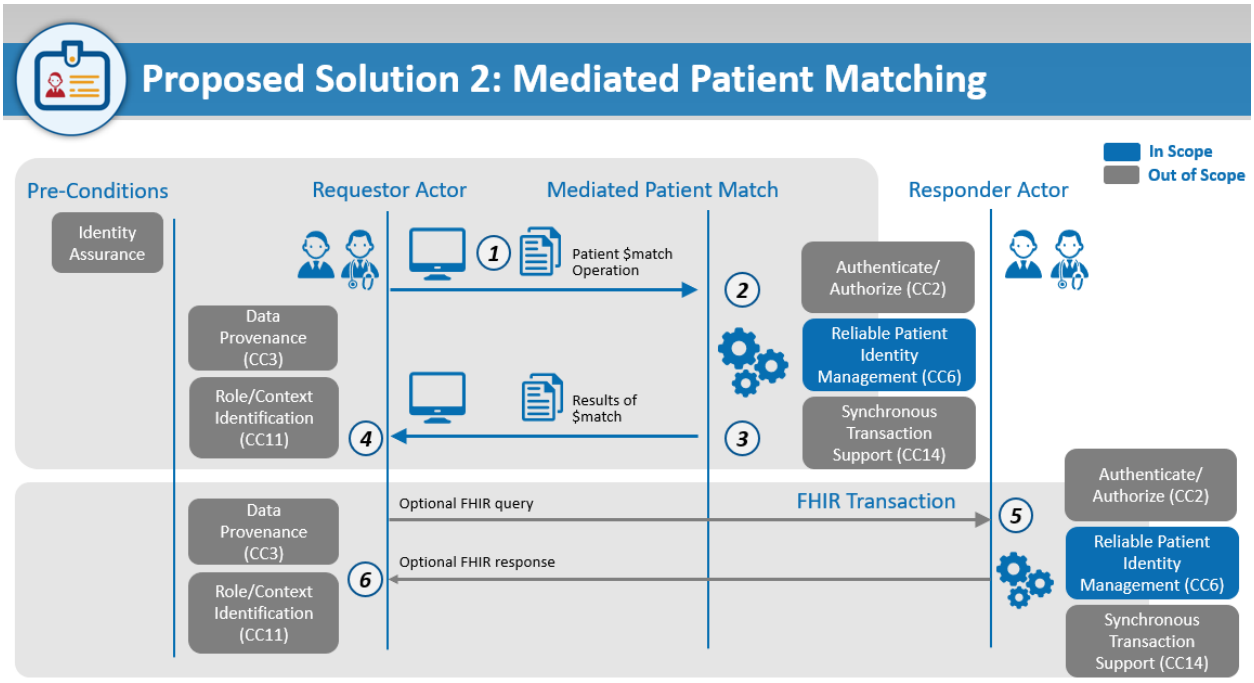
Reliable Patient Identity Management
Solution #2 Mediated Patient Matching

Overview & Description

The solution described here covers patient identity matching in near real time during FHIR transactions. The Requestor and Responder Actor pairs can be represented by provider/provider, provider/payer, and payer/payer pairings. When two entities exchange data, the requestor is responsible for sending the minimum required patient demographic data set to be used for matching, and the responder is

accountable for matching identities of the patients involved. If the responder does not have this capability, they can outsource to a third party.

Supporting Diagrams & Flows



ID	Description	Notes
1	Patient $match request: Requestor Actor calls a Patient $match operation provided by the Responder Actor or a trusted intermediary of the Responder Actor. The $match request will use Patient resource in the request. As a foundational pre-cursor to the $match, the Requestor Actor and Responder Actor must verify the patient's identity to the best of their ability. Please refer to the Best Practices for Identity Assurance section.	
2	Authentication and Authorization are considered Out of Scope for this Solution.	

	Only allow authorized transactions previously defined or discoverable/validatable. Security is separately addressed so that only authorized $match requests may occur.	
3	Patient $match: The operation will return a bundle containing a single patient record, a set of patient records representing potential matches, or an empty set in the case of no matches. Optionally, it may include an OperationOutcome resource with additional information about the search results. A single patient record may be returned if it meets or exceeds the high threshold on a probabilistic match. A set of patient records may be returned if they meet or exceed the low threshold, but none meet or exceed the high threshold, on a probabilistic match. An empty set or a single response of zero matches found may be returned if no patient records meet or exceed the low threshold. The operation must support synchronous transactions.	
4	$match Results: The Requestor Actor may receive a single patient record, a set of patient records, or an empty set in the case of no matches. In both instances where at least one potential match is identified, there may be optional OperationOutcome resources with further information to assist with the adjudication and selection of an accurate match. The result set returned is based on the values of “onlyCertainMatches” and “count” in the request.	To Do: Additionally, as a learning network, the Responder Actor should create a placeholder (e.g., with at least one patient ID) and be prepared to answer requests for this patient in the future.
5	Results Processing: The Requestor Actor will consider the overall context in interpreting the $match response and determining a subsequent course of action.	Assumes purpose of use captured elsewhere (outside of core capability).

	This next course of action could be a FHIR query to fetch additional data or metadata of demographic information for highly probable matches to support adjudication and confirmation of accurate match, or could be a retry of the $match operation with different data elements.	
6	FHIR query results returned	

Pre-Conditions

- Identity Assurance has occurred at either IAL1 or IAL2. Note: even with IAL2, it is possible that while the identity has been established in the real world, the data associated with that identity may not always be the most current e.g. the patient's proofed address may be different than their current address due to a recent move.

In Scope

- Contractual agreements in place between Requestor and Responder Actors.
- The Requestor Actor has prior knowledge of and is using agreed minimum data set or the ability to discover the Patient Match service. Has patient demographic data and other information for the operation.
- The Responder Actor either has Patient Match capabilities in-house or has outsourced it to a partner organization.
- Identity Assurance is in scope for this solution, done to the level possible for the data exchange scenario. IAL2 is recommended. Please refer to the Best Practices for Identity Assurance section.

Out of Scope

- Contractual agreements in place between Requestor and Responder Actors.
- The Requestor Actor has prior knowledge of and is using agreed minimum data set or the ability to discover the Patient Match service. Has patient demographic data and other information for the operation.
- The Responder Actor either has Patient Match capabilities in-house or has outsourced it to a partner organization.
- Authentication/Authorization are not in scope for *Patient* Identity. While in scope for Requestor and Responder Actors, it will be addressed by the *FAST* Security Tiger Team and is not in scope for this document.

Assumptions

- Contractual agreements are in place between Requestor and Responder Actors.
- The Requestor Actor has prior knowledge of and is using agreed minimum data set or the ability to discover the Patient Match service. Has patient demographic data and other information for the operation.

- The Responder Actor either has Patient Match capabilities to support the $match request in-house or has outsourced it to a partner organization.

Complexity Rating

- **Medium**: Builds on existing technology solutions, but requires significant process changes and integration requirements

Proposed Solution Status: In Progress

- Requestor Actor has sufficient patient information(e.g., mutually known identifiers) to proceed with the FHIR queries necessary for the transaction in the case of 'certain matches'.
- Create a learning network responder
- Unknown patients added
- Prepares responder to answer requests for person in the future
- If the operation was unsuccessful, then an OperationOutcome may be returned along with a BadRequest status Code (e.g. security issue, or insufficient properties in patient fragment - check against profile)

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
Map to annotated diagram components above	List components proposed in solution diagrams above	New or if Existing, what is the existing component	If new, describe what needs to be built. If existing, describe what needs to be modified or enhanced.	Who owns building the new component or making the proposed modifications?
1	Initial Entry		Submit match attributes to service	
2	Match		Actual patient match	
3	Results		Matching result returned & stored	
4	Prepare for Query		Convert patient resource to FHIR if needed; reconcile/store received bundle and prepare for use in subsequent query	
5	FHIR transaction request using identifier		Submit query--use details from the patient bundle to perform additional optional FHIR query(ies)	
6	FHIR results returned		Query result returned & stored/processed	

Key Impacts to Timeline & Cost

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

ID	Component	Level of Effort	Comments
1	Initial Entry	Small	Right to aggregate data
2	Match	Large/Jumbo	Best practice matching is challenging to get done right; level of effort depends on whether insourcing or outsourcing
3	Results	Small	
4	Prepare for Query	Potentially large	If no resources to convert match results to FHIR, integrate results into FHIR
5	FHIR transaction request using identifier	Small	FHIR resources designed to be easy to build apps for, perhaps even extra small for experienced team.
6	FHIR results returned	Small	FHIR resources designed to be easy to consume

Reliable Identity Management
Solution #3 Networked Identity Management

Overview & Description

This solution applies to scenarios where two parties have agreed upon the use of digital certificates and OpenID Connect identifiers for the purpose of a) accessing one's own data, when the OpenID credential was not issued by the Responder (patient is both Requestor and Subject), b) a provider requesting data about a patient (using OpenIDs for both Requestor and Subject), c) like b but Requestor (provider) authenticates via client credentials and only the Subject's OpenID is used, for identity matching (in both b and c, the patient is not involved unless they are contacted out of band for identity reolution by Responder), or d) professional access to bulk data FHIR transactions.[4] Such a credential may be issued by the Requestor or Responder Actor or by another trusted party.[5] The Requestor Actor and Responder Actor can be a patient, provider, or payer as the solution applies to patient to provider, patient to payer, provider to provider, provider to payer, and payer to payer transactions.

The OpenID identifier is bound to an individual at IAL2 and any attributes listed in the Patient Demographics section of USCDI that are made available for discovery in the user's profile must have been verified at or above that level of assurance (with the exception of gender, race, ethnicity, and preferred language, which may be self-asserted).

Responder validates the trustworthiness of the Identity Provider before relying on authentication by the Identity Provider's authorization server, and/or on its user profile information. To authorize the transaction and complete a matching step, Responder evaluates the Identifier by:

- Retrieving attributes in real-time from trusted Identity Provider (when the OpenID identifier is used to authenticate Requestor as part of UDAP Tiered OAuth or when the patient is asked to authenticate out of band, e.g. to provide consent or other information, or to complete an identity verification or resolution process; if Responder has previously bound the OpenID identifier to an IAL2 identity, then this step is not needed); and
- Evaluating attributes within the Identity Provider's associated digital certificate, to verify that the Identity Provider is trusted.

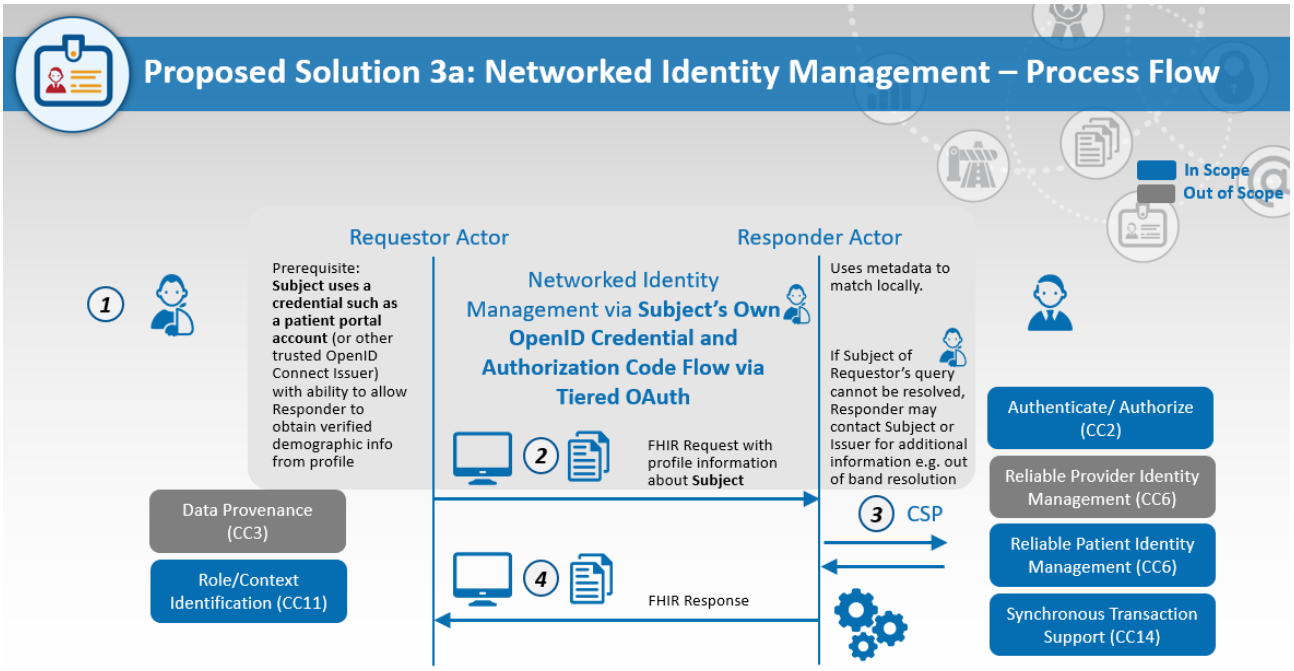
Supporting Diagrams & Flows

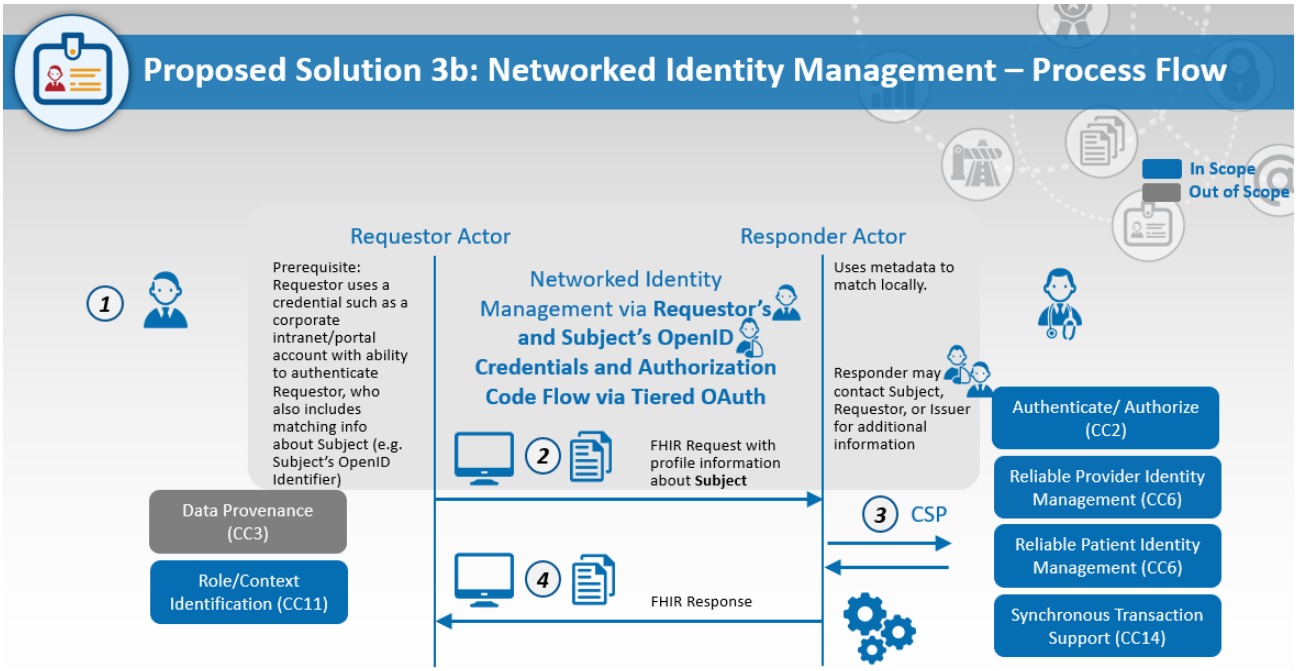
- Results are returned if the Responder has content to which the Requestor is authorized.

[4] For example, as a prerequisite to initiating the client credentials workflow.

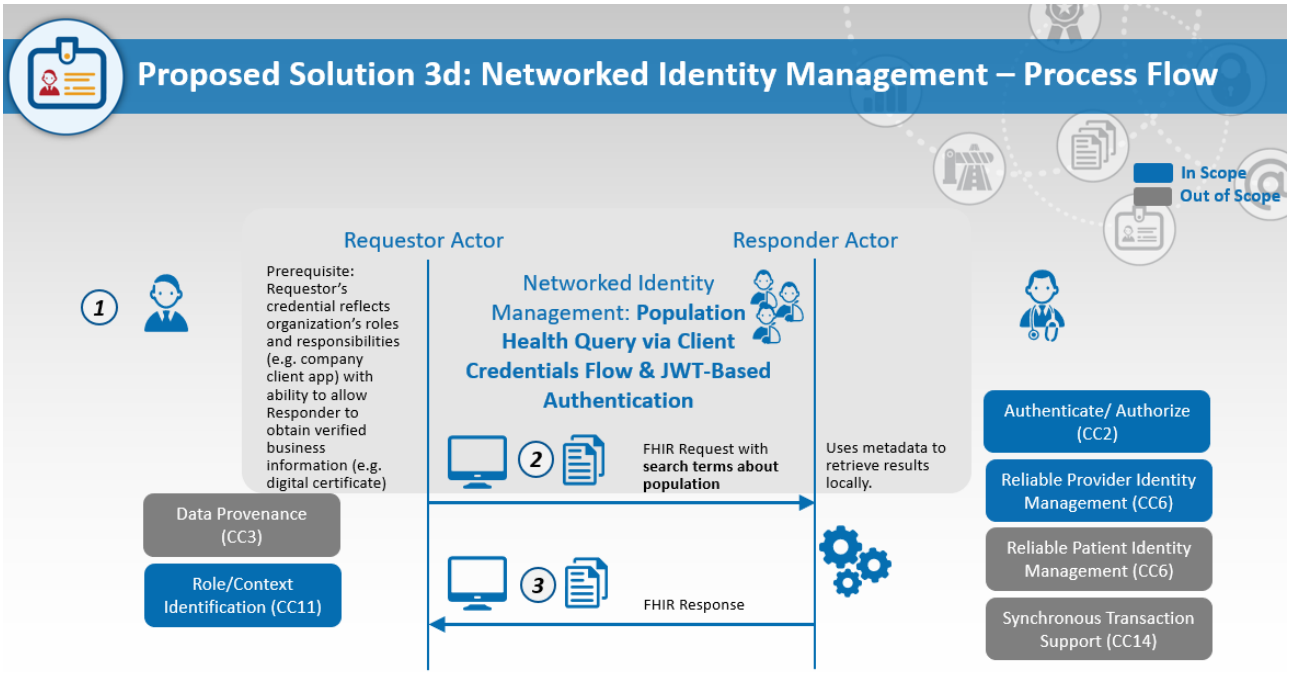
[5] The Security Tiger Team has established a mechanism for dynamically verifying trust with such an Identity Provider via JWT-Based Authentication and UDAP Tiered OAuth.

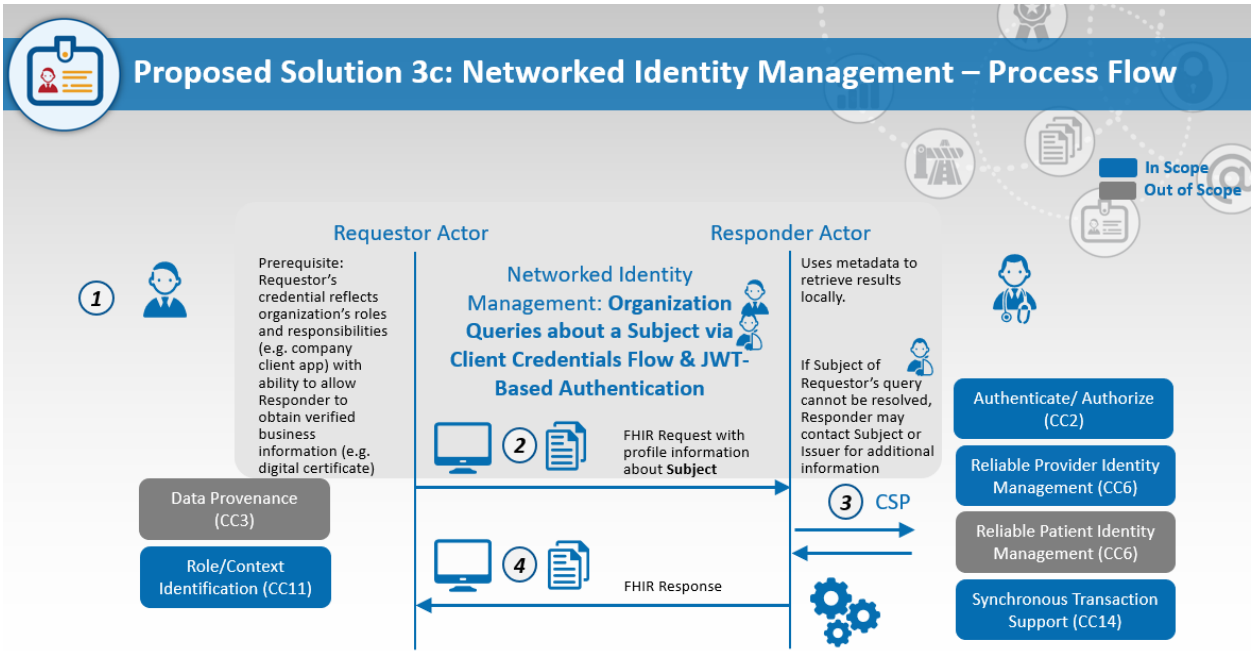
Proposed Solutions: Identity





Proposed Solutions: Identity





ID	Description	Notes
1	Issue or associate OpenID identifier with person	
2	FHIR request using identifier	
3	Authentication & optional profile retrieval	Out of band contact with the subject may also occur, if needed.
4	FHIR Response using identifier	

In Scope

- Authentication and/or identity matching using FHIR transactions involving an Identifier issued by a trusted Identity Provider
- Individual Identity Management allowing for discovery of verified personal attributes such as name, address, DOB, email address, and telephone number
- Trusted certificate indicates assigning entity, which may be a healthcare industry organization
- Future: Identity Services authenticate their own users; trusted metadata allows responding parties to make authorization decisions accordingly.
- Patient access use case

Out of Scope

- Authorization (depends on local policy as well as applicable state and federal laws)
- Service and endpoint discovery

Assumptions

- Contractual agreements in place between ecosystem participants including identity service providers.
- All identity service providers in the network support a grammar for expressing when minimum identity assurance is met.
- Responders should be able to handle $match request

Complexity Rating

- **Medium**: Builds on technology that is not widely adopted for cross-organizationational use; significant process changes, some community specific policy and integration requirements

Proposed Solution Status: In Progress

- Verified patient or provider attributes can be discovered
- It's common to use these attributes as business identifiers in online retail and financial service accounts
- Consumer-friendly option

- Email addresses tied to many patient portal accounts today; provides built-in notification option
- Building in contact points from the start facilitates individual involvement in consent, account activity tracking, and management of privacy preferences.

Open Items

- Best practice guide on how an OpenID identifier can be used with validated attributes
- Collaboration with Security Team to layer on authentication (minimum bar) using Tiered OAuth
- Recommended Federation Assurance Level (FAL)

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
Map to annotated diagram components above	List components proposed in solution diagrams above	New or if Existing, what is the existing component	If new, describe what needs to be built. If existing, describe what needs to be modified or enhanced.	Who owns building the new component or making the proposed modifications?
1	Issue or associate OpenID identifier with person	New	FHIR system for handling a new type of healthcare identifier and using it as a search parameter in a FHIR transaction.	FHIR client apps and servers
2	FHIR request using identifier	New	FHIR system for handling a new type of healthcare identifier and using it as a search parameter in a FHIR transaction.	FHIR client apps and servers
3	Authentication & optional profile retrieval	Existing	OpenID Connect systems build on trust validation capability	OpenID Connect services
4	FHIR Response using identifier	New	FHIR system for handling a new type of healthcare identifier and using it as a search parameter in a FHIR transaction.	FHIR servers

Key Impacts to Timeline & Cost

ID	Component	Level of Effort	Comments
1	Issue or associate OpenID identifier with person	Medium	Point of care and insurance onboarding systems will need to add new identifier to their systems
2	FHIR request using identifier	Small	
3	Authentication & optional profile retrieval	Small	Usual authentication process plus advertising digital certificate to enable trust validation
4	FHIR Response using identifier	Small	FHIR resources designed to be easy to build apps for, perhaps even extra small for experienced team. FHIR resources designed to be easy to consume.

Reliable Patient Identity Management
Solution #4 Distributed Identity Managment

Overview & Description

Patient matching through a network of trusted identity matching services.
Requestor and Responder Actors pairs can be represented by patient/network services, provider/network services, payer/network services.

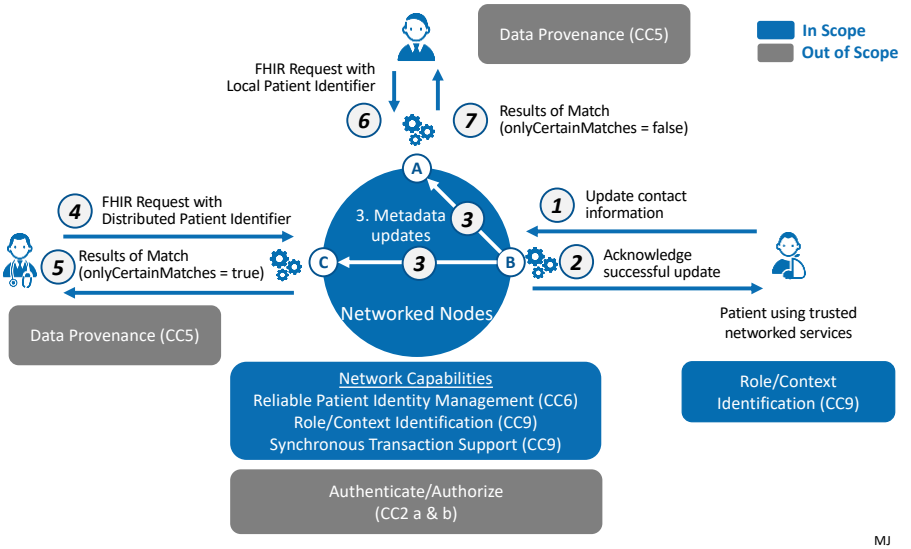
Supporting Diagrams & Flows

Service providers support $match operation and extensions to existing credentials that allow authentication and introspection of healthcare-specific data elements such as insurance identifier and medical record number. May also provide a way for patients to submit consent/IRA request/declare a meaningful choice, receive notifications, participate in identity resolution, or view/control activity associated with the identity.

Note that this solution could be implemented in tandem with solution #2, Mediated Patient Matching, where the responder's matching service is a third party. The third party could be a network of service providers operating under a set of best practices and guidelines. The team is not recommending any specific technology/infrastructure that third party service providers need to implement for this solution.

Key Features

- Emerging solution based on Blockchain
- Supports decentralized identifiers and verified claims with agents to manage services
- Networked nodes have local copies of data
- Updates are propagated to all nodes in the network
- Supports multiple contextual digital identities with different metadata for a single real-world identity



23

MJ

Pre-Conditions

- Identity Assurance has occurred at either LoA-3 or IAL2. Note: even at these levels, it is possible that while the identity has been established in the real world, the data associated with that identity may not always be the most current e.g. the patient's proofed address may be different than their current address due to a recent move.

In Scope

- Patient Identity Matching using a FHIR Match operation
- Support for local and global identifiers in the FHIR Match operation
- Extend solution pattern to cover provider and payer identity matching (future)

Out of Scope

- Security capabilities such as Authentication and Authorization
- Service discovery

Assumptions

- Contractual agreements in place between identity matching service providers participating in the network.
- All identity matching service providers in the network support Patient FHIR Match operations.
- The Requestor Actor has prior knowledge of or the ability to discover the network's Patient Match services.
- Responders should be able to handle $match request

Complexity Rating

- **High:** Requires contractual agreements among multiple Parties and significant integrations to propagate Patient demographic updates throughout the network.

Proposed Solution Status: New

- This is an emerging solution in Identity Management in Healthcare and beyond
- Vendor solutions and open source technology platforms exist in this space and require further exploration

Open Items

- Deep dives on industry approach to distributed identity management
- Security and Privacy considerations for storing and handling PII/PHI in the solution
- Recommended Federation Assurance Level (FAL)

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
Map to annotated diagram components above	List components proposed in solution diagrams above	New or if Existing, what is the existing component	If new, describe what needs to be built.	Map to annotated diagram components above

Key Impacts to Timeline & Cost

<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
1	Onboarding; issue identifier	Small/Medium	Depends on identity verification, data element verification requirements
2	Identifier presented	Medium	Point of care and insurance onboarding systems will need to add new identifier entry and storage
3	FHIR Query	Small	FHIR systems will need to accommodate new identifiers
4	FHIR Response	None	This should be no change from how FHIR resources are returned today

Best Practice Recommendations

Best Practices for Identity Matching Services

Mutually Known Identifiers

The Requestor and Responder Actor, as data exchange partners, assign the patient an identifier as part of their onboarding process that includes validation. Data exchange partners cross-walk their business identifiers either via:

- Mutually agreed upon lists (e.g. roster exchange between payer & provider);
- Patient provides reliable and up-to-date identification containing the agreed upon identifier:
  - Insurance card with payer member ID at encounter check-in,
  - IAL2/LoA-3 proofing process w/ member ID as one Fair/financial piece of evidence and medical record number as the 2nd Fair, or
  - Validating those 2 Fairs subsequent to existing proofing process.
- Without a cross-walk IF identifier consists of verified personal mobile number and/or email address bound to a unique identity through an established process.
- FHIR transaction includes required identifiers that, by design, represent a unique patient
- If using a universal identifier, it should be protected, similar to SSNs
- TBD: Policies around implementation, e.g. identifier never used entirely on its own to match but along with a set of minimum fields such as first+last and/or DOB.

Match Request

Required Minimum Set of Patient Demographic Data Elements
Patient first name, last name, date of birth, full street address*, and administrative/birth sex.

USCDI Patient Demographics:

- First Name
- Last Name
- Previous Name
- Middle Name (including middle initial)
- Suffix
- Birth Sex
- Date of Birth
- Race
- Ethnicity
- Preferred Language
- Current Address
- Previous Address
- Phone Number
- Phone Number Type
- Email Address

Add administrative gender (different from birth sex)

*Best practice recommendation to normalize addresses through the USPS API

Optional Attributes

The inclusion of additional optional attributes is recommended if available, but not required: Patient IDs (including but not limited to insurance member ID, group/plan/policy number, Medicare number, driver's license number, RealID), patient's middle name or initial, phone number, patient's previous name, patient's previous address, patient's email address, patient's phone number designation, multiple birth indicator, payer entity name, metadata on certain identifiers (e.g., date stamp of payer member ID), birth order, patient's mother's maiden name, patient's name suffix, and patient's emergency contact name.

Where Addresses are used for Patient identity resolution, we recommend that Addresses should be standardized and verified against USPS – that it is a valid address, not necessarily that it is tied to that Patient.

Verify phone numbers and email addresses are valid (this is not MFA, it is verification)

"Only Certain Matches"

The attribute "onlyCertainMatches" will be set to true and Count=1 for use cases involving patient care delivery.

To Do: List use cases where onlyCertainMatches must be set to true for use cases involving patient care delivery, coverage determination, and other operations. Lower threshold or lower score allowed in response to public health than patient access? Additionally, only one exact match may be returned in the case of patient requests.

- Patient care delivery, coverage determination, and billing/operations at at minimum

Confidence Intervals

To Do

Match Response/Results

Required Minimum Set of Patient Demographic Data Elements

Refer to minimum set of patient demographic data elements to be returned, given regulatory and privacy considerations.

Threshold Scores

To Do: Consider additional request from Requester Actor to Responder Actor for additional data or metadata of demographic information for highly probable matches to support adjudication and confirmation of accurate match.

To Do: Consider threshold scores and/or number of potential matches for $match operations to ensure consistency and reliability across different implementers.

To Do: Determine best practices for requesting additional data or metadata for single patient with a high match score.

OperationOutcome

To Do: Determine best practices for including OperationOutcome resources when no matches are found.

Error Responses

Error rubric based on metadata element types included; example error reasons:
-Nickname not determined
-Required minimum attributes not included
-Address could not be normalized

Retrying Operations

To Do: Determine best practices for retrying $match operations with a different combination of data elements.

Recommended Key Performance Indicators (KPIs) for Identity Matching Services

Consensus on KPIs for evaluating proprietary matching solutions

To Do: Consider other data quality and algorithm performance metrics to be returned in response.

To Do: Determine best practices for data quality assessment and normalization/standardization by Responder Actor, intermediary,or other 3rd party application.

Best Practices for Identity Assurance

Identity Assurance is essential for accurate patient, provider, and payer identity matching and is foundational to all proposed solutions. Identity Assurance may have some overlap with matching data elements and associated assertions. In determining the IAL for proposed solutions, the following considerations apply for the matching process:

- Resolve a claimed identity to a single, unique identity within the context of the population of users the assigner (e.g. a credential service provider) serves[6];
- Validate that all supplied evidence is correct and genuine (e.g., not counterfeit or misappropriated) and is consistent with the claimed identity;
- Validate that the claimed identity exists in the real world; and
- Verify that the claimed identity is associated with the real person supplying the identity evidence.

Based on these considerations, we propose as a best practice that, at a minimum, IAL2 identity verification is completed as an important first step in all proposed solutions, as allowable by policy and practices addressing identity management for transient and other vulnerable populations. Patient and provider identity matches performed when the identity of the individual has been verified at IAL2 can proceed forward with a strong degree of confidence that both the Requester and Responder Actors are referring to the same person and the records that get exchanged belong to that person.

We understand that not every patient identity, under every circumstance, can be resolved to IAL2. For example, a homeless patient who does not have a fixed address and doesn't have any identity documentation can be proofed to IAL1 and may require a trusted referee to establish greater identity assurance.

As long as the Requestor and Responder Actors in the matching exercise know this, then they can proceed forward with that in mind (e.g., Collaborative Matching). In the real world, homeless and other transient populations are often successfully matched based on their available demographic data elements. It is recommended that additional care is taken when reviewing potential record matches included in a response when identity attributes submitted in the match request do not indicate the best practice IAL2 level of assurance (e.g. a patient is proofed to IAL1).

Draft best practices for IAL1 and IAL2 scenarios (e.g., IAL1 is allowable for transient and other vulnerable populations when both the Requester and Responder Actors are aware of the level of identity assurance for each actor).
Recommendations for records that potentially match and included in response when a patient is identity proofed to IAL1.

Best Practices for Biometrics

TODO

[6] The assigner must implement procedures that prevent duplicates from being created in their local system.

Solution Limitations

1. **Population Exclusions** (e.g., groups who don't have sufficient documentation such as homeless, immigrants, pediatric patients, etc.)

   To Do: May need to recommend an alternate solution to address these populations

Appendix

Additional Solutions Considered and Not Selected

None

Relevant FAST Ecosystem Use Cases or Core Capabilities

To Do: Team to map FAST use cases to each solution

Security Topics/Overlaps with *FAST* Security Tiger Team

Potentially deferred to future discussions…

Topic	Reference/Related Solution(s)	Comments
What AAL does the FAST Security Tiger Team recommend for most use cases? Identity solutions assume that authentication at an acceptable AAL has occurred prior to the transaction.	All	
Verify if Security Tiger Team has this (authenticating and authorizing the match) in scope.	Solution #2: Mediated Patient Matching	
Consider consent best practices in the scope of patient access and the sharing of sensitive information. Discuss both with Security Tiger Team.	Solution #2: Mediated Patient Matching	
Breaking the glass based on clinical or other need?	Solution #2: Mediated Patient Matching	
Identifier metadata will carry any requisite consent information – Identity/Security team responsible for these requirements?	Solution #1: Collaborative Identifier for Patient Matching	
Include in transaction an assertion re: process used to associate identifier with patient on requestor side?	Solution #1: Collaborative Identifier for Patient Matching	
Include in transactions leveraging these identities an assertion re: the process used to associate identifier with patient on requestor side? Similarly, re: the	Solution #1: Collaborative Identifier for Patient Matching	

process used to verify patient on issuer side?		
Security considerations and data protections for the Identifier • How to step up the separate business identifiers approach to combine with contact-based approach • Capable of digital signatures?	Solution #1: Collaborative Identifier for Patient Matching	
Security and Privacy considerations for storing and handling PII/PHI in the solution	Solution #4: Distributed Identity Management	
Future: Identity Services authenticate their own users; trusted metadata allows responding parties to make authorization decisions accordingly.	Solution #3: Networked Identity Management	
Collaboration with Security Team to layer on authentication (minimum bar) using Tiered OAuth	Solution #3: Networked Identity Management	
Identity Assurance – Security or Identity team owns this topic?	All	

Additional Topics/Gaps to be Dicsussed

- Record Locator Services (RLS)
- Provider and Payer Identity Management Requirements for Future Consideration
  - Required minimum set of provider demographic attributes: NPI, Tax ID, first name, last name, and date of birth
  - The inclusion of additional optional attributes is recommended if available, but not required: Middle name or initial, previous name, previous address, email address, phone number designation, metadata on certain identifiers (e.g., date stamp of Provider ID), and suffix
  - FHIR transaction includes required identifiers: 1 NPI if payer or provider
  - Verify organizational identity
  - Verify that individual is a provider