FHIR AT SCALE TASKFORCE

FHIR at Scale Taskforce *(FAST)*

SME Session Summary Report

National Standards Based Approaches
for Individual Identity Management

Session 1: June 24, 2020
Session 2: July 16, 2020

Meeting Introduction

The FHIR at Scale Taskforce (*FAST*) obtained industry subject matter expert (SME) input to further refine the Taskforce's proposed solutions to FHIR scalability challenges.

Eighteen SMEs from across the healthcare ecosystem participated in the *FAST* Identity Management Proposed Solution Expert Panel on June 24, 2020, providing feedback based on their individual expertise and domain knowledge. The scalability needs and challenges of a broad range of stakeholders were represented, including medical and quality associations, interchange associations/Health Information Exchanges (HIEs), identity vendors/developers in both healthcare and non-healthcare industries, cloud identity vendors, The Office of the National Coordinator for Health Information Technology (ONC), providers, payers, electronic health record (EHR) vendors, researchers, and credit bureaus. The SMEs shared their expertise and input with ONC *FAST* facilitators concerning proposed solution approaches for patient matching and identity management; open questions and discussion topics specific to each solution; as well as learnings from the SMEs' individual and organization implementation experiences. Not only did the *FAST* team receive positive feedback on this session, but the participating SMEs decided it would be productive to meet a second time, on July 16, 2020, to continue the discussion.

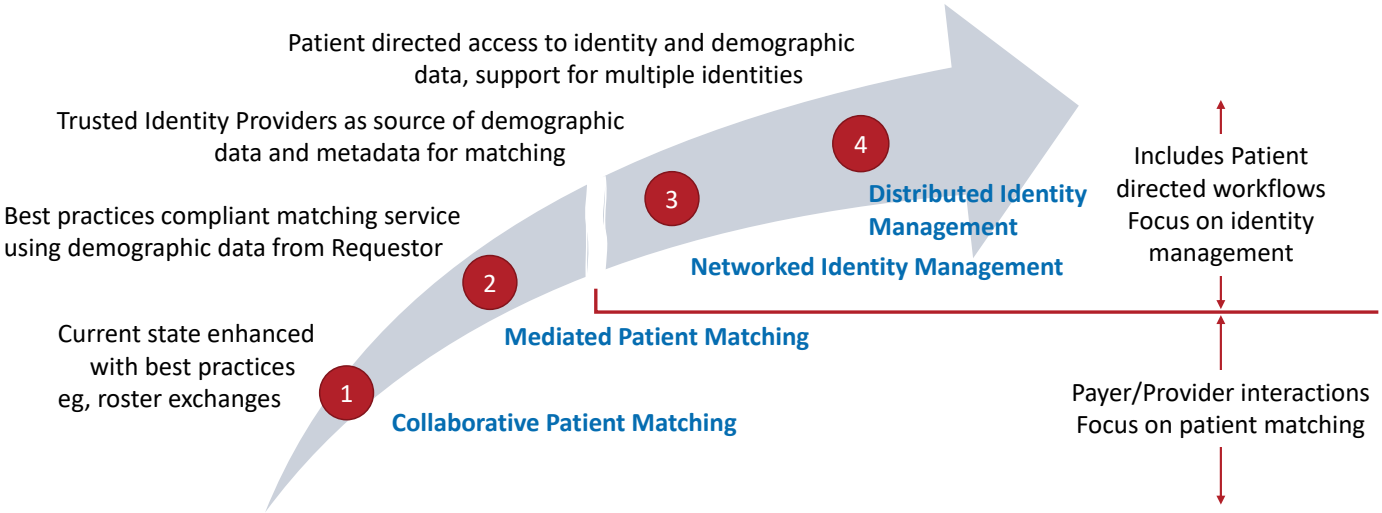
Feedback received through the SME Sessions will advance the Taskforce's proposed solutions into actionable recommendations and support the development of the *FAST* Action Plan. The *FAST* Action Plan is intended to define and communicate Taskforce proposed solutions and next steps to the industry.

To learn more about the *FAST* solutions development process as well as the objectives and meeting materials for each SME Session, please visit the ***FAST* Proposed Solutions – Subject Matter Expert Panel Sessions** Confluence pages.

Solution Overview

The *FAST* team reviewed four proposed solutions that fall within a continuum from lower to higher complexity. The first two solutions, (1) Collaborative and (2) Mediated Patient Matching, focus on payer/provider interactions and patient matching. The second two solutions, (3) Networked and (4) Distributed Identity Management, include patient-directed workflows focusing on identity management.

Multiple Options Progressing From Lower to Higher Complexity (Technical and Process)



The team explained that given the current state of the industry (ie, current regulatory and policy requirements, missing core technical capabilities, and ineffective patient matching methods), they are proposing a set of patterns and best practices that the industry can adopt to reduce the variations that exist today, rather than recommending a single solution. Though this session focused on individual identity management, the *FAST* Identity team is also considering extending these patterns and best practices to consider identity management for provider and payer organizations in the future.

To learn more about the proposed solutions, please review the pre-reading and presentation materials available on the *FAST* Individual and Organizational Identity Management Proposed Solution - Expert Panel Discussion Confluence page.

There was extensive group discussion as the team presented each of the four proposed solutions. SMEs noted that it would be helpful to identify and understand the use cases that each proposed solution is intended to solve. That is especially important for business-to-business (B2B) versus business-to-consumer (B2C) scenarios where the the ideal solution(s) may differ. They agreed that Collaborative and Mediated Patient Matching (solutions 1 and 2) are primarily suited for B2B use cases, while Networked and Distributed Identity Management (solutions 3 and 4) include opportunities for consumer involvement.

SMEs raised concerns regarding security and privacy related to B2C workflows throughout the discussion, though the primary goal of this session was to focus on patient matching and identity management. The *FAST* Security team held a separate session to obtain SME input on security issues, and that feedback is summarized in the *FAST* Security Team's summary report. However, the *FAST* Identity and Security teams acknowledged that further coordination is needed to ensure the *FAST* proposed identity and security solutions are aligned.

SMEs generally agreed that it will be a big leap for most industry stakeholders to progress from Collaborative and Mediated Patient Matching (solutions 1 and 2) to Networked and Distributed Identity Management (solutions 3 and 4). The group noted the mechanisms for digital identity management are still being defined by the industry and there are some components of solution 4 (Distributed Identity Management) that may not be ready for widespread adoption until scalability and security challenges are addressed. SMEs gravitated toward Networked Identity Management (solution 3) as an aspirational, near-term solution, which would then allow organizations to incrementally implement components of Distributed Identity Management (solution 4) in the future.

Discussion Topics

The group spent two sessions (for a total of 5 hours) discussing various requirements for the proposed patient matching and identity management solutions. The discussions were wide-ranging, but deliberations coalesced around seven main discussion topics, which are summarized below.

1. Patient Matching

SMEs reported ubiquitous challenges with patient matching due to the quality of the data and the accuracy of the information provided by patients, as well as the types of data and level of detail being collected by healthcare organizations.

SMEs generally agreed that the more data you have to match patient records on, the better your chances of accurately matching patient records and identifying potential duplicate patient records. Some SMEs then debated the notion that there should be a minimum required data set for patient matching, arguing that systems should leverage any and all data available to assist their patient matching efforts. Some SMEs agreed that the patient matching approaches taken today could be enhanced with biometrics and other verified data, but there may be different combinations of minimum data sets required, depending upon the matching context or use case. For example, in-person or human-mediated workflows may require a lower standard because provider staff act as intermediaries to verify a patient's identity, whereas automated systems may need stricter controls in place to prevent error.

SMEs suggested that the team consider recommending a minimum identity assurance level (IAL), or at a minimum require the requestor to convey IAL to the responder so they can make appropriate matching and access control decisions. The National Institute of Science and Technology (NIST) has issued guidance that may be useful as a starting point.

SMEs also discussed that additional data standardization could improve the accuracy of matching, for example, using United States Postal Service Publication 28 for addresses. One suggestion was for the *FAST* team to include standardization of data structure and related requirements as an additional base-level requirement for solutions.

2. Key Performance Indicators

SMEs discussed that there are typical performance measures such as false positive match rate and false negative match rate, but the key is to keep up regular patient matching algorithm performance assessments using a representative curated data set. The group suggested that an industry-wide matching benchmarking service could be beneficial, with a certification body to manage that process.

3. Biometrics

The *FAST* team introduced the concept of biometrics with solution 2, Mediated Patient Matching, acknowledging a centralized service or set of services is required for scalability. It was for this reason that biometrics was not considered as a potential enhancement to solution 1, Collaborative Patient Matching, which is coordinated point to point, and therefore not scalable.

SMEs agreed that biometric data would be valuable as an additional trait that can be used for patient matching, though it may be more appropriate for B2C scenarios. SMEs cautioned that user acceptance is needed to implement biometrics, and low acceptance could be a barrier within B2B scenarios where patients may be concerned about their data being shared without their knowledge or consent.

SMEs also suggested that in exchange scenarios between clinical entities, other information from the medical record could be used to validate that exchange partners are referring to the same patient, though there has been pushback on this concept due to concerns about disclosing clinical data prior to correctly identifying and matching the patient. SMEs agreed that matching on clinical information for non-sensitive data would be a positive step forward, potentially yielding fewer errors than solely relying on patient demographic data.

4. Digital Identity Management

The *FAST* Identity team explained that Networked Identity Management (solution 3) would allow organizations to move toward using a digital identifier for patients, thus reducing the complete reliance on demographic information to identify and match a patient and introducing the possibility of re-using that credential in other contexts or workflows.

SMEs discussed the role of a Credential Service Provider (CSP) in this solution, and questioned which entity or entities would be appropriate to fill this role. SMEs noted that all actors across the industry, including patients, would need to be aware that the CSP will store all patient credentials, as well as data indicating which providers or other entities exchanged these credentials and the associated patient data at exchange. Having multiple interoperable CSPs could reduce that risk, but an umbrella entity may be required to support this interoperability (eg, a government entity and/or a trust framework).

SMEs noted that credit bureaus have already set the precedent for crosswalks between CSPs, but the government would likely need to set standardization and certification requirements for all organizations to meet before they may participate. Again looking to the financial industry as an example, SMEs argued that with standards and operating rules, interoperability can occur between multiple CSPs. One example of this in the financial industry is when consumers can use any bank branded credit card across multiple merchants.

5. Potential Solution Limitations for Certain Patient Populations

The group discussed that there are limitations to current patient matching and identity management solutions for certain segments of the population who are more likely to have limited, out of date, or inaccurate demographic data or limited physical documentation to prove their identity.

These populations include but are not limited to children, the homeless, the undocumented, and migrants. There are other populations, such as the incarcerated and those suffering cognitive decline, that also present unique, complex matching and identity challenges. Additionally, there are patients who don't wish to be identified.

The SMEs noted that patient matching and identity management for these groups is complex and likely to involve a combination of in-person methods, technical solutions, and business process engineering.

6. Regulatory Considerations

The group did not spend much time on this topic, though feedback regarding potential regulatory implications was focused on Solutions 3 and 4 (Networked and Distributed Identity Management), with specific attention to B2C workflows. If the market is heading toward digital health identity, the group questioned whether it will settle on a top-down, centralized approach, or a bottom-up approach where a combination of various standards are being used and entities regulate themselves? SMEs considered whether regulation could potentially support greater interoperability between identity service providers, EHRs, and other patient-focused systems to facilitate patient interactions with the healthcare system.

Another challenge noted, is that identity and privacy legislation can differ from state to state, thus adding complexity when considering identity management solutions.

7. Creating & Maintaining Industry Guidance

SMEs provided input on the appropriate "home" for creating and maintaining industry guidance on the proposed solutions.

The group noted the importance of having a neutral convener who could further develop requirements, but also consider operational aspects of the solutions to achieve real-world use. The need to engage professional societies, the government (eg, ONC), and standards development organizations (eg, HL7) was also discussed.

Moving Forward

After two productive SME sessions, the *FAST* Identity Tiger Team is analyzing the feedback they received and working to incorporate what they learned into the next iteration of their solution documentation. As the team further develops their action plan, they will take the following SME recommendations into account:

Immediate Next Steps

- Map solutions to use cases (ie, context is important - when would the team recommend using each solution?)
- Make recommendations to improve matching (even if not perfect)
    - Standards development and standardized data normalization based on current best practices
    - Explore including identity proofing in the match request based on demographics and data inputs
- Consider any lessons learned from existing financial processes (eg, credit bureaus, credit card transactions, etc.) that could potentially be applied to the healthcare identity process
- Consider whether additional patterns/use cases suggested are in scope
    - Identity solution providers are not currently interoperable with each other
    - Identity theft ("anti-pattern")
- Determine level of additional development needed before Solution 4: Distributed Identity Management could be implemented

- Further evaluate the proposed solutions for any patient matching and identity limitations for segments of the population who may have limited identity documentation and/or demographic data, and consider how to address (eg, the homeless, the incarcerated, the undocumented, or those who don't wish to be identified but still need care)
- Further coordinate with the *FAST* Security Tiger team to ensure the proposed identity and security solutions are aligned

Path Forward

- Explore concept of benchmarking matching services and the types of entities that have the appropriate resources and skills to perform this function
- Explore how operational processes could support technology to ensure successful applications of the proposed patterns in the real world
- Consider existing market challenges related to identity and any potential policy implications
- Explore recommended options that could be pursued in a long-term path to execution of the proposed solutions and continue to obtain input from industry stakeholders
- Explore pilot suggestions where real world applications could be explored and lessons learned can be gleaned from these experiences
    - Consider focus on pilot scenario(s) including patients with chronic conditions who interact with multiple providers to demonstrate solution value
- Identify and potentially address the operational issues that could support and enhance technical solutions
- Engage professional associations and a broader range of industry stakeholders for additional solution feedback