FHIR at Scale Taskforce (*FAST*)

Technical barriers to FHIR solutions scalability

Tiger Team Name: All

\*\*Teams to focus first focus on A. and B., and later on C.

|  |  |  |  |
| --- | --- | --- | --- |
|  | 1. What is the technical barrier identified? | 1. Why is this a barrier to scalability? | 1. What exiting industry efforts are working to remove this barrier (if any)? |
|  | **Directory** - aka resource locator for a FHIR endpoints  **(Breakout to discrete items for DVS items captured – see slide deck)** | There is no place to look up a FHIR end point for a given physician / organization nor address the sheer number of endpoints that may eventually number in the 1000’s. How does a payer know where to find the FHIR endpoints for a given patient’s records? How does a provider know how to find the FHIR endpoint for a patient / insured information outside of their organization?  A resource locator directory solution will need to consider scale and the potential for variation across partners, including partner-to-partner and partner-to-intermediary situations.  A resource directory solution will need to Identify a way for the industry status to collect, store, and share access of FHIR APIs across multiple stakeholder definitions (payer, provider, vendor) and at multiple levels (provider, groupings of providers, network relationships, etc). |  |
|  | **Versioning** |  |  |
|  | **Scale** |  |  |
|  | **Identity –** confirming the participants in and subject of the exchange | There is no consistent way to cross-walk patient identity during a FHIR exchange. A payer likely identifies a person with an insurance ID. A provider identifies a person with some variation of medical record number. How do we crosswalk the two identities in real-time and how do we manage the risk of mis-identification?  The identity matching issue is important enough that the recent rule included an RFI to ask for potential solutions. Some aspects of a solution the FHIR task force has contemplated are:  • Developing a set of patterns (the common situations) for which person identity needs to be cross-walked. For example, a physician may need to access a payer FHIR resource using their medical record number, however, receives a “not found” because the data in the payer FHIR server is indexed by insured ID.  Use cases should include situations that drive assessment of both member identification and provider identification  • When is member/patient ID a requirement in a FHIR resource? A recommendation may be needed to update implementation guides with this requirement in order to enable identity cross-walks.  We also need to think holistically about identity, inclusive of member identifiers, provider identifiers, and the identity of others who may be requesting information.  We will need to consider how to we proof identity and a tie-off with the security tiger team will be necessary.  • Consider when identity matching can be pre-established through use of commonly accepted forms if identity, such as a license, a member ID card, a token. Solutions in this space maybe available to us vs. attempting to dynamically match at time of transaction. |  |
|  | **Security –** ensuring compliance | Today, we have limitations on our ability to ensure, in a scalable way, that the requestor of information using a FHIR based information exchange is appropriately authenticated and has the authorization to see the data requested. How do we know the FHIR consumer has permission to ask or see? We need a scalable solution that works for hundreds of millions of patients/insured and millions of requesting organizations and individual providers.  There is a significant amount of prior work in the industry that has specified security guidelines. We do not need to replicate this work. Rather, we need to apply current security rules to FHIR use and identify gaps where scale is needed including:  • Creating use cases that describe the common situations in which authentication and authorization are needed using FHIR. For example, a payer HEDIS analyst may request a quality measure or procedure lookup using a FHIR implementation guide. How do we ensure that user is from a payer? How do we ensure they are covering that person and have the right to get the answer? Use cases will need to include scenarios that drive discussion of how we validate the role of the person or organization requesting information and whether they have permission to use that information.  • Identifying current industry status security authorization and authentication processes and tools in current clinical interoperability and in advanced digital API use. Techniques like oAuth are widely accepted, but how do they scale for broad use of FHIR? What other techniques and tools are available that work at scale? How are they administered? Our industry is not new to security concerns, so we will need to harvest current best thinking, but with a practical view of implement-ability. |  |
|  | **Testing, conformance and certification** | How do we handle versioning of FHIR artifacts in a scalable environment? How do we test / validate consistently? How do we manage the problem across multiple stakeholders with varying degrees of maturity? And, most importantly how do we do so across hundreds of thousands of endpoints?  We will need to include testing and conformance gap topics such as:  • Common issues that result from lack of versioning control. For example, a payer care manager executes a FHIR call against a resource, only to find that the standard version used by the payer is out of synch with the resource. How do we anticipate this and adjust? How do we deal with backward compatibility? How do you align FHIR resources across endpoints? How do we do conformance testing and certification?  • Identifying current industry and HL7 capabilities built into FHIR for versioning and how such version controls will scale across many endpoints. What is the minimum level of conformance required to participate in a scaled FHIR ecosystem. There is likely practical implementation experience in early FHIR adopters that will need to be solicited and harvested. |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |