7/25/19 – Directory Tiger Team

Bob Dieterle

Alix Goss

Rick Geimer

Brandon Neiswender

Patrick Murta

Alex Kontur

Welcome Brandon Neiswender (Chief Operating Officer of CRISP)

Endpoint Discovery Proposed Solution

Bob – broke out the endpoint discovery solution into a separate document, includes the Tiger Team’s bullets about current state, problems to be solved, and future/intermediate state. Still need to propose solutions and develop diagrams [first draft of diagram is below]



General workflow:

* Requesting actor authenticates to directory endpoint and asks for information about an entity’s endpoint
* Directory responds w/the endpoint address(es)
* Use the endpoint to request data

Murta – initial draft of diagram is a good start. Would like to see more detail about core capability #1 (endpoint discovery), especially to ensure that terminology is consistent. Recommend adding additional annotation to the diagram

Brandon – What is the goal? A national directory where entities will register FHIR API endpoints? Or local directories that talk to each other?

* Bob – Generally want directories to support more than just endpoint location, e.g. what version of FHIR is supported, what operations are available at the endpoint, who has the right to access the endpoint, what trust framework, etc. To the extent we have a method for validating/certifying the directory content, we’d want a national directory that is federated to local operating environments. Want to avoid a situation where different directories are doing it differently
* Brandon – so we’d have a national registry that governs certified entities to collect/obtain required information about endpoints. Federated approach to locating endpoints
* Bob – not necessarily one place for everybody to hit, but one place to register/validate. To the extent endpoints are relevant to the scope of a given domain, make that data available to the appropriate entity. Define endpoints once and make them available in a federated environment. Also have to figure out a pathway from existing state to future state (i.e. how do we optimize and improve on what we have today?)

Murta – Our goal is to capture Tiger Team’s discussions using the diagram. For example, the draft diagram requires that an actor must authenticate to the directory before identifying an entity’s endpoint. While we might require an entity to be credentialed or certified to read an endpoint, another possible approach is that the requesting actor doesn’t need credentials to discover an endpoint (e.g. the DNS model) and only authenticates when they actually hit the endpoint

* Bob – Treating the directory endpoint like any other. If you are unauthenticated or don’t have credentials, you may only have access to limited information. Authenticated access may provide additional content
* Murta – Based on the draft diagram, is authentication to the directory endpoint required?
	+ Bob – authentication isn’t necessarily required, but may be if there is restricted information
* Brandon – are you asking for information about what the endpoint does, or are you asking for credentials to call the endpoint?
	+ Bob – The request to the directory is to obtain info about the endpoint. Assuming that the right to know existence of an endpoint may be restricted (e.g. for a women’s shelter or emergency response network). E.g. on the internet you may be able to discover a URL, but you don’t necessarily know the owner, what trust framework it’s part of, etc.
	+ Murta – For example, you may be able to discover which organizations are in the directory, but obtaining the actual address of the endpoint might require authentication/credentials
	+ Brandon – Authentication requirements provide a layer of security, so I don’t have to reveal anything about my endpoints unless there is somebody on the other end that I trust
	+ Bob – If we permit unmediated access to all endpoints in the directory, we create an opportunity for bad actors. At minimum, the authentication step allows for auditability
	+ Murta – Important to document these assumptions. Should we allow anybody to access an endpoint’s conformance statement? This Tiger Team should make a recommendation
* Alix – we need to provide a reference to the Authentication core capability even though we’re talking about the endpoint discovery capability? What is the line in terms of what we should be describing in this document?
	+ Bob – we have to indicate that we are recommending providing directory capabilities for both authenticated and unauthenticated queries. How that is done falls under the purview of another Tiger Team

Alex – Do we need to indicate that the directory actor needs to be auditing certain things or has other (non-core) capabilities that aren’t currently in the draft diagram? Likewise, that the requesting actor has to establish a TLS connection or some other standard/protocol for connecting to the directory?

* Bob – Yes. Not sure if a TLS connection would be required for unauthenticated actors

Murta – Would also like to document what information the directory would return about an endpoint. E.g. the FHIR versions supported by the endpoint, which resources are available, etc. Does an endpoint listed in the directory simply give you a way to find the endpoint’s capability statement, or does it provide more information to help understand what is available at the endpoint?

* Bob – An endpoint directory should have relatively intimate knowledge about the capabilities of an endpoint. Assumes that organizations may have many endpoints with specific purposes, e.g. for quality information, patient access, etc. Hard to predict how organizations will maintain endpoints in the future, e.g. if their endpoints are for actual FHIR servers or not. At this point, I’m assuming organizations will maintain multiple endpoints

Brandon – concerned about how we are going to limit “chattiness” at national scale

* Bob – consider some of the conversations happening about using the Subscription resource. They have considered that you might send nothing to a subscriber except an ID (no PHI). The subscriber would have to check the ID, might find out it’s for an encounter, and then have to ask who the patient is, etc. May have requirements from stakeholders not to respond with PHI. At the moment, the industry doesn’t have a great solution for handling the scope of exchange vs. the number of exchanges required to solve a particular use case

Out of Scope

* Alix - Looked at prior work and problems to be solved to start a list of issues considered out of scope. May need to discuss further to determine whether they are actually out of scope:
	+ Audit requirements
	+ Manual intervention (we’ve been assuming automated processes)
	+ Non-FHIR server endpoints
	+ Integration with clinical systems
	+ Directory maintenance & other operational aspects
		- Brandon – directory maintenance is critical, so we may want to describe any requirements
		- Bob – the “what” is in scope...you have to guarantee currency, availability, etc. “How” this is done is out of scope
	+ Rules for intermediaries (have been focused on point-to-point)
	+ Legal/trust framework
		- Alix – the legal obligations for exchanging data once you have identified an endpoint
		- Bob – creation of legal/trust frameworks is out of scope, but we may identify if an endpoint is part of one
	+ Consumer facing exchanges
		- Bob – is there a reason we wouldn’t want a consumer-facing endpoint included in the directory? Consumer application endpoints should be in scope, but certification of applications should be out of scope
	+ Brandon – patient identity validation
	+ Bob – standards for versioning are out of scope, but discovery of the version supported by an endpoint is in scope