June 20th:

Advancing Future State Requirements and Solutioning Discussion:

* Priorities within Technical and Regulatory

Directory (future state):

Vision for endpoint discovery and related directory services:

1. Available to any user, with appropriate identity, authentication and authorization
2. Known method/standard (e.g. one URL or multiple URL’s discoverable through DNS) or easily discoverable endpoint for the “directory” itself
3. Any complexity (e.g. architecture, implementation) behind the directory model is hidden to the requestor
   1. Issues related to more than one directory (source of truth, different information)
   2. Issues with endpoints that are not owned by the proposing/representing source (is solution that only source of endpoint registration is the owner)
   3. Issue with reporting non-functioning endpoints – how, process, dispute process (ebay approach or private process with validation (remember to address this as a requirement)
4. Ability to discover a FHIR associated electronic endpoint using a standard directory endpoint query that supports search criteria (e.g. name, specialty, location, NPI) that are reasonably known by the requestor
5. Relationship between provider and endpoint (e.g. endpoint owned by organization where provider has a relationship)
6. Endpoints have standard “metadata” that defines, for each endpoint
7. Owner (managing organization)
   1. Contact information
8. Permission/onboarding process
9. Version(s) of FHIR
10. Type of exchange/service (e.g. RESTFUL, operation, CDS Hooks, …)
11. Type of endpoint (FHIR service, Testing, Test, Production, ….)
12. response (not real time data) (could this be a part of d?)
13. Supported profiles and IGs (may include capability statement)
    1. (bullets c, d, e, f, and g similar and are these the right buckets? Overlapping items not clear and think about how to clean it up)
14. Support for mixed models (see Scale section for three models – currently in brainstorming document and will be carried over to Scale section of this document once created)
15. Trust framework(s)
16. publicly available data versus privately held data (for example CMS Medicare model vs. Commercial Payer model)
17. pre-coordination or registration requirements among trading partners versus no advance registration requirements
18. Support for multiple trust frameworks (e.g. Federal Bridge, FICAM, Direct Trust, DURSA)
19. Proof of testing/certification
20. Status of endpoint
21. Services supported (e.g. population services (e.g. deidentified data))
22. Implementation guidelines adopted covering:
23. Testing and production environments
24. Acknowledgement responses (failures, delays, no content available)
25. Authentication
26. Authorization
27. Payload receipt capabilities
28. Super protected data
29. Service level agreements (availability, response times)

10/18:

* Address overlap or intersection potential with TEFCA (common agreement/dursa need and implications)