5/23/19 - Meeting Notes

5-23-19 - Directo...eeting Slides.pdf

Bob Dieterle

Rick Geimer

Ed Martin

Patrick Murta

Matt Becker

Tim Young

Dan Chaput

Technical Barriers - Scaling

Murta – need to increase provider services?

- Bob – if you are going to have increased volume of transactions, payer and provider services will have to scale. Not just scaling of infrastructure but scaling of the individual endpoints
- Murta – increase to both capacity and services

Bob – within the models, do we need to discuss any concerns/constraints with respect to intermediaries?

- Matt – in our experience [Epic], intermediaries present an additional risk, especially for EHR-EHR transactions. Because there are a greater number of potential points of failure
- Bob – intermediaries create additional points of failure and need to address real-time support for defined services
    - Bob – as we add additional segments to any transaction, we introduce the need to manage each as a potential point of failure and performance constraint. Additional intermediaries may add interoperability challenges and require technology that is not necessary for point-to-point connections (i.e. the point-to-point connections that work between two partners might not be sufficient for end-to-end reliability, open service connections, performance requirements, etc. when intermediaries are involved)
    - Murta – may be more difficult to maintain synchronicity and state
- Existing efforts:
    - Murta – able to maintain state through “hops” over the Availity network
    - Bob – Clearinghouses in general? (Murta – yes); some intermediaries (e.g. clearinghouses) offer ability to maintain state end-to-end (unclear whether this is possible when multiple intermediaries are involved)

Capability Mapping

Murta

- Working w/Use Case Tiger Team to determine “level 1 capabilities” so we don’t spend too much time focused on the language of the use cases…want to move from set of use cases to a set of actionable capabilities. Goal has always been to distill into core technical capabilities that are common across use cases.

- The table indicates which use case primarily defines each capability, e.g. the endpoint discovery capability is primarily defined by the endpoint discovery use case (even though it is used by many other use cases)
- Updated capabilities:
    - Data provenance was added as a capability, but subsequently removed – because it isn't an infrastructure capability, rather a functional component of use cases
    - Event/message/topic subscription/publication was added – capability for a subscriber to listen for certain types of events
    - Role/context identification was added – driven by shared care planning, care team, and coordination use cases; different participants may have different rights (e.g. read vs. write)
- The Tiger Team assignments columns represent an initial assignment of capabilities for Tiger Teams to review. Does not mean that other Tiger Teams will not review the capabilities later

Bob

- In many cases, our Tiger Team will need to work jointly with other Tiger Teams to review capabilities, because we have identified dependencies; e.g. the Testing/Certification Tiger Team will need to validate resource version identification
- All capabilities on the list will need to be piloted (Pilot Tiger Team)
- Endpoint discovery
    - No testing/certification around the discovery per se, but there testing/certification around validation of the endpoint itself
    - Endpoint may be restricted and/or involve other security issues. Therefore will need to deal with the identity of whoever is asking for information, and will need security on the endpoint itself
- Provenance
    - Recognized that provenance is a data attribute, not an interoperability service that we need to worry about for scaling.
    - The ability to assign provenance to an item is done at the source (e.g. note that a medication was ordered by this provider from this organization on this date). When I pass that to somebody else, the provenance goes as metadata. If they pass it to somebody else, they need to add the fact that they had control of it, and must also share the provenance info. Provides a chain of trust. Do we need to comment on that as a scaling issue?
- Authentication/authorization
    - DVS Tiger Team doesn't need to comment on it, although may be used in cases where we have secured endpoints
- Reliable patient identity management
    - DVS Tiger Team doesn't need to comment
- Reliable provider identity management
    - Part of requirements for directories
    - Testing/certification should be validating
- Event/message/topic subscription/publication
    - Endpoints potentially need to support these services and/or make these capabilities known
        - Matt – also a scaling challenge in whether endpoints can support volume of notifications
    - Should be validated
- Guaranteed message delivery
    - Implies an ability to respond (e.g. delivery notification)
    - Geimer – HTTP status code returned over RESTful API, more complicated when an intermediary is involved
    - Testing/certification - need to validate whether an endpoint has the capability
    - Do we need to include standards to indicate how an endpoint responds to a message delivery? E.g. an operations endpoint wouldn't have the respond the same way
- Role/context identification
    - DVS Tiger Team doesn't need to comment
- Readiness credential
    - Directory must support the capability
- Standards-based endpoint access
    - Do we need certification/testing of the directory itself, or only the endpoints?
        - Geimer – for the endpoints, as well as internal testing
    - Synchronous transaction support & asynchronous transaction support
        - Need to identify as part of endpoint definition
        - Testing/certification – need to validate