1/10/19 - Directory Tiger Team Meeting Notes

Bob Dieterle

Tony Little

Tim Young

Rick Geimer

Jason Walonoski

Dan Chaput

Alex Kontur

Use Case – Authentication & Authorization

- Overview & description
  - Typo – “focuses on the ability to authentication and authorize”
  - Bob – is this just the ability to access an endpoint, or is it broader and includes ability to access specific data?
- In scope
  - Bob – need to indicate that we are talking about authorization not only to an endpoint, but to specific resources/queries
  - Tony Little – just authorization of the requestor, or the request as well?
    - Bob – probably both, e.g. if you have the right to a record, what parts of the record can you see?
- Assumptions
  - “or provider and provider for a patient…”
    - Bob – does the patient need to have a treating relationship with both providers?
  - 3 – “the primary goal of the use case…”
    - Bob – add language about “access to specific information”
- Types of requestors and responders
  - Bob – add “payer system”, indicate provider systems other than EHRs may be a requestor/responder
- Stakeholders & Interests
  - 2 – “responder – has interest…”
    - Bob – modify language: “…and ensure that only authorized requesters have access to permitted data”
- Pre-conditions
  - Tony Little – would the requesting/responding systems have to pre-coordinate in some fashion? Not like anybody is going to be able to hit a FHIR server any time they wanted. E.g. may pre-coordinate to establish a trusted relationship
    - Bob – “precoordination between requestor and responder may be required and potentially satisfied by a mutually adopted trust framework”
- Post conditions
  - Bob – generally need to indicate scope covers the endpoint and data at the endpoint
  - 1 – “Requestor has established…”
    - Alex – may want to drop the word “responder”, in case the responder is an intermediary and doesn’t actually own the endpoint
- Requirements & Main Success Scenario
  - Bob – generally need to indicate scope covers the endpoint and data at the endpoint
  - 3 – “as a responder to the ecosystem, and if the FHIR endpoint…”
    - Alex – may want to remove the “if the FHIR endpoint is for patient data”. Implies that there may be other data available, but that the responder doesn’t need to validate that the requestor has appropriate rights and approvals
  - 4 – “as a responder in the ecosystem, I need to conform to HIPAA…”
    - Bob – rephrase: “To the extent necessary, both parties should limit the request and response to meet any applicable HIPAA minimum necessary guidelines”
- Supporting Diagrams & Flows

- Bob – the authorization workflow occurs with each request for information and not only with the initial request
  - Geimer – should authenticate once (e.g. OAuth bearer token) and pass token with each request