Working Session Summary

- Decisions
    - Identity Proofing, Authentication, Authorization, and Consent are out of scope for the Identity team
    - Align vocabulary to NIST for consistency

- Ideas for follow up
    - Rules and best practices on searching for patients – what can you send, what should be used to match
    - Should identifiers be qualified/rated based on issuing body? E.g. SSNs are better than MRNs
    - Restrict information returned to the minimum necessary. For example, return identifiers only and not demographic info.
    - Categorize recommendations and findings into Required (you must do this to match) and Optional.

- Questions for other teams
    - Security: Thoughts on context of digital identities
    - Security: Level of identity proofing that should occur prior to issuing FHIR request
    - ONC: In the case of an incorrect patient match during a FHIR exchange, who bears liability? The risk to patients depends on the context of the exchange (e.g. low risk in case of determining out of pocket expenses, high risk for care delivery)

Points for discussion

1. Where possible, we should leverage the NIST Digital Identity vocabulary
2. NIST Digital Identity guidance focuses on members, identity providers and relying parties. But, does little to define identity matching & trust in a transactional system. The opportunity is to extend the NIST framework and concepts to cover these use cases.
3. A single global identifier is unlikely
4. If 3 is true, Contextual identifier are preferred and could take the following format [Identity Provider Unique ID]:[Individual UUID assigned by identity provider] or something like 12343e3342D:99832G11Z
5. Identity providers should:
    a. allow 3rd party systems to query Identity providers with the information the requestor has available.
    b. Return only the information provided with subscribers identity in the suggested format [Identity Provider Unique ID]:[Individual UUID assigned by identity provider]
    c. Allow for registration and use of the identity provider query end point – This should be simple and relatively consistent
    d. Discovery of identity providers?
6. While the identity provider owns sufficiency and matching rules – some attempt should be made establish standard recommendations
7. Develop a framework incorporating the above, vetted against the project use cases and Da Vinci edge cases.