Rim – I have copied the questions you had in the DxF AG Presentation deck of 04/07/22, slide 59.

1) Is this an appropriate first step? Will this strategy help us meet the vision of the Data Exchange Framework?

   CPCA question: What is the strategy?
   Tokenizing based upon the following from slide 46?
   - Patient Demographics − Name − Date of birth − Address − Previous address(es) − Phone number(s) − Email address(es)
   - Additional unique identifiers − Identifiers from health-related federal and state programs − Identifiers from social servicesrelated state programs − Local identifiers related to health

   Or, is the strategy essentially summed up on slide 50? (under the slide header "Permitted Uses")
   Or is the strategy on slide 57, "Summary"?

2) Is there value in specifying attributes in the absence of a statewide index? Will use of a common set of attributes and the standards used to specify them improve exchange?

   CPCA: No questions/comments.

3) Must we adopt national standards even if they don't meet our needs? For example, Patient Discovery standards require that gender be specified, but we may remove it as an attribute for privacy reasons

   CPCA feedback: following USCDI seems logical. UCSDI v1 includes "Sex (Assigned At Birth)". USCDI v3 (which may be draft presently) includes "Sex (Assigned At Birth)", "Sexual Orientation", and "Gender Identity".

4) Should the state operate the statewide index (if created)? Will consumers trust the state with information about them?

   CPCA feedback: Not sure. Recommend that the answer to the first question #4 be covered in DSA and any governance that is adopted under the DxF. As to the second part of question #4. No, consumers will not trust (be it the state or other entity). Not the American way.

I have reached out to CPCA's HIT Peer Network, hoping to provide some additional feedback that is likely akin to what you (Rim) might have been hearing in your Focus Groups. Unfortunately I likely will not hear from many before close of business tomorrow. However, below is feedback from one tech savvy Chief Quality Officer from a health center. He also shared an excellent article about Digital Identity in Estonia. Albeit a small country (probably fewer people than San Jose up to southern border of SF), but a great read. Estonia's 20 year history of using digital identities

- concerns about a digital health identity because the American data culture is based on the opposite of these principles (trust thru transparency, cybersecurity, and citizen data ownership)
- Despite HIPAA protections, health care industry has been experiencing cyberattacks, increasingly
- how are we going to protect CA patients against committed threat actors intent on exposing and misusing the digital identity?

DeeAnne McCallin
Director of Health Information Technology
California Primary Care Association