PEMC and user centric information

THE TEST = What does the Verifier say to the wallet so that the Holder says yes?

THE QUESTION = does the current IPCQ document align with the PEMC requirements.

232 2.1 Consent and Choice

233 ORGANIZATIONS SHALL ONLY PROCESS PERSONAL INFORMATION WITH THE CONSENT AND CHOICE OF THE INDIVIDUAL.

260 2.1.1 Obtain Consent for Verifier Processing

261 Verifiers shall only process personal information from Holders with valid consent or as required by law.  
263 NOTE: Verifiers should obtain a Holder’s consent in response to the Notice provided to the Holderby the Verifier.

265 Establish the Context for User Consent

266 Verifiers shall establish valid consent at or before the Holder presents any information from a Mobile Credential (tj – not sure what this means)

291 2.1.5 Ensure active Holder Engagement.  
292 Providers shall ensure credential data is only requestable and released after/with active Holder engagement. The Holder shall act before releasing data to the Verifier.

308 2.2 Purpose Legitimacy and Specification

309 ORGANIZATIONS SHALL ONLY PROCESS PERSONAL INFORMATION FOR SPECIFIED AND LEGITIMATE PURPOSES

330 2.2.1 Inform Holder of Verifier Policies (tj retention is the only one spec’d)

331 Wallet Providers (i.e., Holder Agent) shall communicate to the Holder any electronically received attestations about data use associated with a Verifier in the transaction context.

333 NOTE: To inform Holders of a Verifier's retention policy and the data requested, the Provider should communicate to Holders how the Verifier has claimed they will use the data and for what duration they expect to retain it

373 2.3.1 Verifiers collect for identified purposes

374 Verifiers shall not request more than the personal information necessary to provide their services.

429 2.5.1 Retain with consent

430 Verifiers shall not store personal information unless the Holder consents to it, or the storage is required by law

534 2.8.2 Holder access from Verifiers

535 The Verifier shall allow the Holder to access their information and participate in decisions about processing it unless a law prohibits it.

503 2.7.3 Verifier provides transparency for Mobile Credential data

504 Verifiers shall give the Holder clear and easily accessible information about their policies, procedures and practices concerning Mobile Credentials

571 2.9.2 Provide contextually appropriate Verifier Identification

572 Verifiers shall identify themselves with the Holder with enough details about the transaction to help the Holder decide whether to proceed.

607 2.10.1 Use Encrypted Channels for Transactions

608 All identifying data shall be transacted through encrypted channels. To protect the confidentiality of Holders, Issuers, Providers, and Verifiers shall only transact identifying data through encrypted, secure channels to prevent exposure to third parties.