November 27, 2023

John Ohanian
Chief Data Officer
California Health and Human Services Agency
1205 O Street
Sacramento, CA 95814
E-Mail: CDII@chhs.ca.gov

SUBJECT: Comments on Draft Policy and Procedure: Individual Access

Dear Mr. Ohanian:

Thank you for the opportunity to provide feedback on the following draft Policy and Procedures:

- Breach notification

On behalf of our more than 400 member hospitals and health systems, the California Hospital Association (CHA) respectfully offers the following comments.

The requirements set forth in the P and P seem overly broad. Any notification obligations to CDII or other participants should focus on security events only, to the extent that these would impact CDII or other participants. As currently written, if a Participant has an event, notifying other participants and the CDII doesn't relieve the Participant of any other notification obligations such as HIPAA, CMIA and other laws. As such, it is difficult to justify why it is then appropriate to further circulate and share the PHI/PII for the impacted individuals with other Participants and CDII if it is only to make them aware that a Participant has had an event. Further, CDII should consider limiting the scope of the policy to cover only incidents where a Participant's system was used to directly abuse/steal information and/or other security related events.

In addition, it is unclear when this policy applies and when it does not. For example, if Participant A obtains data from Participant B, and Participant A incorporates the information into their records, and then Participant A's records are breached, it would seem to follow that CDII or other DxF participants may want to be informed of that breach. However, the P and P as currently drafted does not provide any guidelines or boundaries related to this use case.

Further, if it is only limited to breaches between two Participants, and any information has not been incorporated into a Participant's records, then it might be more appropriate for Participant A to notify the individual whose information is involved. The draft, however, is written in a way that suggests that a receiving Participant would still have breach notification obligations as it is not clear who owns what part of the process.

We would also like clarification on the following:

- Unencrypted data - Does this mean Participants will be required to report misdirected faxes or things dropped in our parking lot? Do we need to report misdirected unencrypted emails? We recommend clarifying the following statement: "Participant will report any breach of EHI that is acquired by an unauthorized individual in the course of exchanging information through an HIE."
- Scope of reporting to CDII - Does this cover any breach? As healthcare entities are already reporting to CMIA, OCR, and State Attorneys General, what is the State's need to receive reports of all breaches vs. breaches related to DxF Participants?
- Notifications of all Participants - What is the proposed mechanism for notification? Does this mean all DxF Participants, or those that have provided information to the Participant who is reporting the breach?
- Participant expectations - What are Participants expected to do with the notifications they receive?

In addition, when a QHIO is the facilitator of data exchange, we would recommend a P and P that is more structured, specific, and timely, similar to the DURSA language.

Thank you for your consideration. If you have any questions, please contact me at tgonzalez@calhospital.org.

Sincerely,

Trina A. Gonzalez
Vice President, Policy

cc: DeeAnne McCallin, Deputy Director, Data Exchange Framework, CDII