California Health & Human Services Agency
Center for Data Insights and Innovation
Data Exchange Framework Implementation Advisory Committee
Data Sharing Agreement Policies and Procedures Subcommittee
Meeting 8 Q&A Log (10:00AM – 12:30PM PT, June 27, 2023)

The following table shows comments that were entered into the Zoom Q&A by public attendees during the June 27th meeting:

Count	Name	Comment	Response(s)[1]
1	Zach Gillen, KP	Agree with Dr. Eisenberg regarding the 10 day review period being a little short. Would recommend a 30 period for review.	Thank you for your comment.
2	Laura HF Barde	'+1 to the discussion of covered v non-covered entities and California law. For CA entities, "applicable law" may require that to refer specifically to CA law, regardless of the location of the Participant, especially wrt post-Dobbs landscape. What considerations have been made in this regard, please?	Live answered
3	Deepthi Buduru	are there any restrictions on disclosing substance use disorder treatment records	Federal, state, local, and tribal law continue to apply to disclosing SUD treatment records.
4	Bmoore	Given the short time allotted in public comment, we wanted to list our questions and concerns here. We will also submit as written questions to the CDII email address.	Thank you. Wanted to also note that our intent is to release the draft Policy and Procedure for written public

[1] Responses may have been provided by various Data Exchange Framework Data Sharing Agreement Policies and Procedures Subcommittee Members or Center for Data Insights and Innovation staff.

Count	Name	Comment	Response(s)[1]
			comment outside of the public comment period at this meeting. Please watch for its release. You can of course also submit questions and concerns as you have suggested.
5	Bmoore	Given the short time allotted in public comment, we wanted to list our questions and concerns here. We will also submit as written questions to the CDII email address.	Thank you.
6	Bmoore	1. What will the process be for approving non-covered entity participants? 2. How will compliance with this policy by CBOs be verified? For example, will compliance with the HIPAA Security provisions be required prior to approving an entity to participate in the exchange? 3. How will compliance with this policy be enforced? Appears to be monitoring only at this point. When does CDII expect to get enforcement authority? 4. Will there be specifics given to non-CE/BA's regarding exactly the training required, particularly concerning the sensitivity of Part 2 and LPS? 5. The P&P is vague regarding whether the required policies and procedures will satisfy OCR and State regulatory agency requirements. 6. Not feasible to enter into Business Associate agreements with everyone who is receiving information downstream. Not only are they not the CE's business associate, but the CE likely won't even know who these entities are that are getting its data from the QHIO.	Thank you. CDII will review and consider.

Count	Name	Comment	Response(s)[1]
		7. A covered entity's participation on the exchange and provision of access to all of its PHI by entities that are not bound by law to protect such information and are not business associates, does not appear to satisfy the requirements of HIPAA. Will the State indemnify covered entity participants for their disclosure of PHI through the exchange, if it is later found that such disclosures do not comply with HIPAA? Is the State providing a legal opinion on how this exchange complies with HIPAA and CMIA? Will CDII, who is requiring compliance as an arm of the State, defend the Covered Entities with CDPH? AG? Any other State regulatory agencies? 8. Given that non-covered entities are not bound by law (other than Cal. Civil Code 1798.80 et. seq. and potentially the CCPA), how will breach reporting be handled? Under HIPAA, once PHI is disclosed to a non-covered entity, it is no longer subject to HIPAA. Therefore, it is likely not appropriate to report breaches under HIPAA. The Breach P&P is scant and does not discuss. 9. Additional questions as to breach. The DSA indicates that the breaching participant is responsible in the event of a breach, and will have to report to CalHHS and other participants. But there is no other information in the scant P&P to address how a breach would be handled. o By "other participants," does that mean the breaching participant will notify the entity whose data was compromised?	

Count	Name	Comment	Response(s)[1]
		o Will the breaching participant handle notifications to the patients? To regulatory agencies? o If the covered entity whose data is breached is required to notify its patients, is there any mechanism for the breaching participant to reimburse the costs? o If the breaching participant is a non-CE/BA, will that participant have the training/knowledge on what is required? o Could a non-CE/BA even report to OCR or CDPH? See above re: what constitutes breach for non-CE/BA's. o Or is it expected that the participant whose data is breached will be responsible for everything, including costs, even though it had no part in the breach itself and likely wouldn't have any agreements in place, or even the ability to enter agreements, with these other participants? o In the event of a breach, would a downstream vendor even know whose data was breached in order to notify the covered entity/participant? 10. The policies do not appear to address any special protection against viruses and do not include acceptable use policies. 11. What is the model for the HIE architecture (federated, centralized, and hybrid) and how that impacts the security risks. In our view, if the State is going to require this, it needs to prescribe that the HIEs who manage this enforce security and consent management requirements. Will QHIO's be required	

Count	Name	Comment	Response(s)[1]
		to add anything to their agreements with CBO's/non-CE/BA's that address these concerns? 12. Is access to data for research purposes allowed? The DSA makes it appear so, but it is unclear.	
7	Jennifer Inden (she/her)# Aliados Health (formerly RCHC)	There are many options for SRA from hand held DIY through full in person evals. Requiring an annual/attested SRA would go a LONG way for trust building of sharing PHI/PII with entities not historically shared with.	Thank you Jennifer.
8	Lucy Johns	+1 to Devan. Essential for public credibility and for state to affirm it's done every best practice for security and privacy. Sorry to put here but chat disabled for observers.	Thanks for your comment.
9	Asharma	Thank you to Devan for sharing the OCR risk assessment tool. My question are the SRA findings applicable to CMIA as well?	Thanks for your comment and question for further consideration.
10	Lucy Johns	+1 Louis. How does checking on consent figure into Response, how much and how fast? I would hope more thought about this! ;-)	
11	Lucy Johns	What does "digital identities" refer to?	That term is not used in any P&P and is therefore not defined in the Glossary, but is discussed in the Strategy for Digital Identities and in the Person Matching portion of the Technical Requirements for Exchange P&P. We will consider defining the term and including it in the Glossary.
12	Lucy Johns	Purely editorial: …person *who*… Not that. ;-)	Thank you.

Total Count of Zoom Q&A comments: 12