Privacy Standards and Security Safeguards Policy & Procedure, OPP-6, Version 1.1
DSA P&P Subcommittee Feedback, Due 06/30/23
Comments from: LA County Dept of Health Services (LAC DHS)
06/28/23

P&P Section	P&P Phrase	LAC DHS Comments
Page 2, III, 1, c, i	"Unless otherwise prohibited by Applicable Law, if the Participant is not a Covered Entity, a covered component of a Hybrid Entity or a Business Associate, the Participant shall at all times, at a minimum, comply with the following provisions of the HIPAA Regulations and all other Applicable Law with respect to any PHI and/or PII the Participant receives under the DSA"	1. What will the process be for approving non-covered entity (non-CE) participants? 2. How will compliance with this policy, including compliance with HIPAA and other Applicable Law, by CBOs/non-CEs/business associates (BAs) be verified, monitored, and enforced? 3. When does CDII expect to get enforcement authority?
Page 3, III, 2, a, i	"If the Participant is a Covered Entity, Business Associate, or a covered component of a Hybrid Entity, the Participant shall comply with the HIPAA Security Rule and all other Applicable Law."	1. A covered entity's (CE) 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 (BA), may not satisfy the requirements of HIPAA, depending on a variety of factors. 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? Attorney General? Any other State regulatory agencies? 2. The P&P is vague regarding whether the required policies and procedures will satisfy OCR and State regulatory agency requirements.
Page 3, III, 2, a, ii and (i)	"A Participant who is not a Covered Entity, Business Associate, or covered component of a Hybrid Entity shall at all times, at a minimum, comply with the	1. 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

	following provisions of the HIPAA Regulations and all other Applicable Law with respect to such PHI and/or PII, as follows: (i) The Participant shall implement appropriate administrative, physical, and technical safeguards consistent with 45 C.F.R. sections 164.306, 164.308, 164.310, and 164.312, respectively."	appropriate to report breaches under HIPAA. The Breach P&P does not address these questions. 2. It is 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. 3. Will compliance with the HIPAA Security Rule's provisions be required and verified prior to approving a CBO/non-CE/BA to participate in the exchange?
Page 4, 4, a	Policies and Procedures Training section	1. Can more specific training information be shared re: the training requirement for non-covered entity/business associates, particularly concerning the sensitivity of Part 2 and LPS?
General		1. What is the model for the HIE architecture (federated, centralized, or hybrid) and how will that impact the security risks?. In our view, if the State is going to require this, it needs to prescribe that the QHIOs who manage this will enforce security and consent management requirements. Will QHIOs be required to add anything to their agreements with CBOs/non-CEs/BAs that address these concerns? 2. The policies on privacy and security do not appear to address any special protection against viruses or malware and do not include acceptable use policies. How will security risks be mitigated?

Additional Questions related to Safeguarding Data. These are also related to breach reporting, and we recognize that the Breach P&P is finalized, but that P&P does not address these questions with specificity:

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.

1. By "other participants," does that mean the breaching participant will notify the entity whose data was compromised?
2. Will the breaching participant handle notifications to the patients? To regulatory agencies?

3. If the CE whose data is breached is required to notify its patients, is there any mechanism for the breaching participant to reimburse the costs?
4. If the breaching participant is a non-CE/BA, will that participant have the training/knowledge on what is required?
5. Could a non-CE/BA even report to OCR or CDPH? See above re: what constitutes breach for non-CE/BAs?
6. 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?
7. In the event of a breach, would a downstream vendor even know whose data was breached in order to notify the CE/participant?