CommonSpirit Health Recommendations

for the

California Health and Human Services Data Exchange Framework: Single Data Sharing Agreement

May 5, 2022

Section	Summary	Comment
4	Use of Health and Social Services Information	This section does not contain any information about data ownership and licensing of data for the entities sharing information. Suggest inclusion of such language to clarify data ownership and licensing of shared data.
4(a)	Policies and Procedures will define the purposes of data use for HSS data.	Purposes of data use are fundamental to the relationship and should be defined at least at a high level in the contract itself.
5(a)(i)	Policies and Procedures may be changed.	At the very least, a statement should be added that the contract controls in case of a conflict with Policies and Procedures, because the purpose of a contract is predictability and stability. It would also be advisable to place contractual parameters around the amount the Policies and Procedures can change, or even to introduce a mechanism for obtaining consent from Participants before changing the Policies and Procedures.
5(a)(ii)	Specifications may be changed.	Same as previous comment.
6	Authorizations	This section should address not just authorized disclosures of Health and Social Services Information, but also permitted disclosures. In other words, Participants can rely on an authorization to make a disclosure, but they can also rely on a permitted purpose to make a disclosures, and both should be addressed.
7	Participants will exchange HSS info as set forth in the Policies and Procedures.	The contract should provide some parameters on the scope and type of required participation, in order for all signatories to enter the relationship with their eyes open. Because Policies and Procedures are subject to change over the life of the contract, the contours of the sharing should be defined in the stable contract terms.

Section	Summary	Comment
8(d)	Malicious Software	No entity can warrant that security controls will block all malicious software. Language revised to reflect HIPAA Security Rule requirements.
8(e)	Participants must comply with breach notification requirements in the Policies and Procedures.	These requirements should be subject to *contractual* parameters, not subject to change. For example, will the cost burden or timelines deviate significantly from the HIPAA default? (Separately, we do have a concern with the timelines and burden of breach reporting as laid out in the Policies.)
11(b)	Individual Access	Individuals have the right to access their own PHI or PII. Use or disclosure by Individuals is not the issue here, as such use or disclosure is not governed by Applicable Law.
11(e)	Access Requests	This section mentions HIPAA covered entities and business associates only. How will other entities comply?
12(a)	This section requires Participants to cooperate with other Participants' consultants, contractors, vendors, employees, etc.	A new section 12(a)(vi) should be inserted, requiring Participants to protect the confidentiality of all third parties connected to another Participant.
12(d)	Prohibition of discriminatory limits on exchange of HSS information.	This broad prohibition on unfair or unreasonably limits on interoperability should be made more specific, in order to provide enforceably useful guardrails, and to avoid confusion on its meaning later. Further, discriminatory effect should not be enough to trigger breach of contract (because no neutral process for evaluating impact is defined); an intent element should be added. Here is what more specific language could look like: "A Participant shall not intentionally discriminate against a legally protected class under California or Federal law or intentionally restrain trade in California, by unfairly or unreasonably limiting exchange or interoperability with any other Participant or Individual User. Such discrimination shall include, for example, burdensome testing requirements that are intended and applied in a discriminatory manner…"
13	No information blocking	This section should be deleted; compliance with applicable Federal law is already implicitly and explicitly required.

Section	Summary	Comment
14(a)	Monitoring and auditing	1) The Governing Entity's rights should be limited to auditing, not "monitoring," unless monitoring is defined more specifically. 2) Parameters on audits should be set in the contract, not deferred to the Policies and Procedures. For instance, parameters could include the following: "Notwithstanding the Policies and Procedures, such audits shall be reasonable in scope, limited to one (1) issue of inquiry in any twelve (12) month period, shall not disrupt normal business operations of Participants, shall be at the expense of the Governing Entity, and shall not be performed by a third party contractor paid in proportion to any damages or fines assessed.
15(f)	Requirement that third party technology connecting Participants to the exchange be subject to the same privacy and security standards applicable to the Participant.	The requirement should be that tech vendors are subject to "similarly rigorous" privacy and security standards, because large technology vendors do not generally customize their security practices with great specificity.