California Health & Human Services Data Exchange Framework

DRAFT Data Sharing Agreement Language

Distributed: January 13, 2022

PRIVACY AND SECURITY

Definition of Breach

"Breach" shall mean the unauthorized acquisition, access, disclosure, or use of PHI or PII under this Agreement or any other written data sharing agreement between Participants. "Breach" shall also mean access, use, or disclosure of PHI or PII that is not for an Exchange Purpose. With regard to California State Departments, a breach shall also mean the disclosure of PHI or PII without a signed Authorization when that disclosure is not one of the exceptions listed in California Civil Code section 1798.24 or other Applicable Law.

The term "Breach" does not include the following:

1. Any acquisition, access, disclosure, or use of PHI or PII that is encrypted in a manner that conforms with the National Institute of Standards and Technology (NIST) standards specified in Special Publication (SP) 800-57 (as revised from time to time); or

2. Any acquisition, access, disclosure, or use of PHI or PII for a legitimate business need and for a purpose either required or authorized by California Civil Code section 56 et seq. or any other Applicable Law that governs the lawful access, use, or disclosure of PHI or PII; or

3. Any good faith acquisition, access, disclosure, or use of PHI or PII by an employee or agent of a Participant for the purposes of the Participant provided that the PHI or PII is not used or subject to further unauthorized disclosure consistent with California Civil Code sections 1798.29 and 1798.82; or

4. With regard to Governmental Participants, a disclosure of PHI or PII that is required by law or permitted by California Civil Code section 1798.24 or other Applicable Law.

PRIVACY AND SECURITY

12.1. General. Each Participant shall at all times fully comply with all Applicable Law relating to this Agreement and the use of PHI and PII.

12.2. Safeguards. Each Participant shall be responsible for maintaining a secure environment that supports the operation and continued development of the Specifications. Participants shall use appropriate safeguards to prevent use or disclosure of PHI or PII other than as permitted by this Agreement, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that PHI or PII. Participants shall also be required to comply with any Specifications or Policies and Procedures adopted by the Committee, respectively, that define requirements and expectations for Participants with respect to enterprise privacy and security. Appropriate safeguards are as follows:

1. A Covered Entity, covered component of a hybrid entity, or Business Associate Participant shall use safeguards identified in the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C, as safeguards, standards, "required" implementation specifications, and "addressable" implementation specifications to the extent that the "addressable" implementation specifications are reasonable and appropriate in the Participant's environment. If an "addressable" implementation specification is not reasonable and appropriate in the Participant's environment, then the Participant must document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if reasonable and appropriate;

2. Appropriate safeguards for Governmental Participants shall be those required by Applicable Law, regulations, or policies related to information privacy and security; or

3. Appropriate safeguards for Social Services Organizations shall be those required by Applicable Law, mandatory policies such as but not limited to regulatory agency guidance, or through a legally enforceable agreement with a government entity, Governmental Participant, or other Social Services Organization.

Commented [1]: are we establishing new privacy laws by contract?

Commented [2]: Couldn't this just be summarized by saying participants are expected to protect data - and not share it except where authorized - in accordance with applicable law? (could develop appendices regarding what laws apply to whom...).

12.3. Policies and Procedures and Training. Each Participant shall, as appropriate under the HIPAA Regulations, Applicable Law, or mandatory policies such as but not limited to regulatory agency guidance, have written privacy and security policies in place by the Participant's respective Effective Date. Each Participant shall also train staff, contractors, agents, employees, and workforce members who will have access to PHI or PII under this Agreement before such access. Each Participant shall also provide refresher training consistent with each Participant's internal privacy and security policies but no less than annually.

12.4. Malicious Software. Each Participant shall ensure that it employs security controls that meet applicable industry or federal standards so that the PHI and PII being exchanged and any method of exchanging that PHI or PII will not introduce any viruses, worms, unauthorized cookies, trojans, malicious software, "malware," or other program, routine, subroutine, or data designed to disrupt the proper operation of a system or any part thereof or any hardware or software used by a Participant in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause a system or any part thereof or any hardware, software or data used by a Participant in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable. In the absence of applicable legal or industry standards, each Participant shall use all commercially reasonable efforts to comply with the requirements of this Section.

Commented [3]: Why single this out among security protections? (This is usually appropriate when you're talking about participants connecting into a central network where you need to be considered about spreading viruses to the network through malicious software

12.5. Breach Notification. As soon as reasonably practicable, but no later than two (2) calendar days after determining that a Breach has occurred and is likely to have an adverse impact on a Participant, a Participant shall provide notification to Committee and all Participants that are likely impacted by the Breach. The Participant shall supplement the information contained in the notification as it becomes available and cooperate with other impacted Participants. The notification should include sufficient information for the recipient of the notification to understand the nature of the Breach. For instance, such Notification should include, to the extent available at the time of the Notification, the following information:

Commented [4]: is this in here because we think there are endpoints that are not covered by CA's breach law? Takes up a lot of space to use a contract to impose legal requirements.

1. One or two sentence description of the Breach;

2. Description of the roles of the people involved in the Breach (e.g. employees, service providers, unauthorized persons, etc.);

3. The type of PHI or PII Breached;

4. Participants likely impacted by the Breach;

5. Number of individuals or records impacted/estimated to be impacted by the Breach;

6. Actions taken by the Participant to mitigate the Breach;

7. Current status of the Breach (under investigation or resolved); and

8. Corrective action taken and steps planned to be taken to prevent a similar Breach.

12.6. Notwithstanding Section 12.5 above, Participants agree that (a) within one (1) hour of learning that a Breach occurred and that such Breach may involve a Participant that is a Governmental Participant, it shall alert the Governmental Participant in accordance with the procedures and contacts provided by such Governmental Participant and (b) that within twenty-four (24) hours after determining that a Breach has occurred and is likely to have an adverse impact on other Participants that are Governmental Participants, Participants shall provide a notification to all such Governmental Participants that are likely impacted by the Breach in accordance with the procedures and contacts provided by such Governmental Participant.

12.7. Law Enforcement Exception. Notwithstanding Section 12.5 above, regarding PHI only, if a Participant is notified, in writing or by oral statement by any law enforcement official or by any other governmental agency (e.g. Federal Trade Commission), that a Breach notification would impede a criminal investigation or cause damage to national security, and the statement has been documented consistent with 45 C.F.R. part 164.412(b), then the Participant shall delay the Breach notification for the time period specified by the law enforcement official.

12.8. This Agreement shall not relieve Participants from any other Breach reporting requirements under Applicable Law including those relating to consumer notifications.

TECHNOLOGY AGNOSTIC

TECHNOLOGY AGNOSTIC

5.1. The parties agree that this Agreement is intended to be technology agnostic, meaning that no particular technology or method to exchange data is preferred. Participants may use various technology solutions, applications, interfaces, software, platforms, clearinghouses, and other information technology (IT) resources to support exchange of PHI or PII. The parties intend that each individual party shall be entitled to choose which method of exchange best suits that individual party. However, each party shall engage in meaningful health and social services information exchange either through execution of an agreement with an entity that provides data exchange or through use of their own technology.

Commented [5]: Is this going to work? Feels like we may need to specify a particular menu of options - people should have to choose something recognizable and able to facilitate exchange with others.

5.2. Each party shall agree to exchange information to the extent the party is technologically ready and able. The parties recognize that some Participants may execute this Agreement and be willing to exchange information but may not be technologically able or ready. The parties agree to the following:

1. Participants that are health information networks, health information organizations, health information service providers, or use certified electronic medical record systems shall exchange information in accordance with this Agreement and any other information sharing agreements they are parties to;
2. Participants that are health care providers, physician organizations and medical groups, skilled nursing facilities, general acute care hospitals, acute psychiatric hospitals, clinics, laboratories, Health Plans, and disability insurers shall exchange information in accordance with this Agreement and any other information sharing agreements of which they are parties to the extent they are technologically able and ready. Notwithstanding Section 7 Requirement to Respond, Participants that are health care providers, physician organizations and medical groups, skilled nursing facilities, general acute care hospitals, acute psychiatric hospitals, clinics, laboratories, Health Plans, and disability insurers may access information in accordance with this Agreement but are

not required to disclose information until they are technologically able and ready;

3. Participants that are Governmental Participants shall exchange information in accordance with this Agreement and any other information sharing agreements of which they are parties to the extent they are technologically able and ready. Notwithstanding Section 7 Requirement to Respond, Governmental Participants may access information in accordance with this Agreement but are not required to disclose information until they are technologically able and ready;
4. Participants that are Social Services Organizations shall exchange information in accordance with this Agreement and any other information sharing agreements of which they are parties to the extent they are technologically able and ready. Notwithstanding Section 7 Requirement to Respond, Social Services Organizations may access information in accordance with this Agreement but are not required to disclose information until they are technologically able and ready.

5.3. In no event shall a party use technology as a justification for failure to meaningfully participate in this Agreement. Participants must meaningfully participate in information exchange. Meaningful participation means that a Participant will comply with Section 7 Requirement to Respond and will contract with another entity to provide information exchange services if the Participant is not technologically able to perform those services itself. Notwithstanding the above or Section 7, a Social Services Organization is not required to exchange PHI, contract with another entity to provide information exchange services, or make itself technologically able or ready to exchange PHI.

Commented [6]: If we come up with a menu of options that everyone should be able to implement, we shouldn't need this provision - otherwise creates a massive loophole.

Commented [7]: Agree - but I don't see how this can be reconciled with what is above.

EXCHANGE PURPOSES

Definition of Exchange Purposes

"Exchange Purposes" shall mean one or more of the following reasons for which Participants may legitimately exchange PHI or PII:

1. Treatment;
2. Payment activities, including but not limited to Utilization Review, to the extent permitted or required by Applicable Law;
3. Health Care Operations, including but not limited to Quality Assurance and Improvement, Business Planning and Development to the extent permitted or required by Applicable Law;
4. Benefits Determinations;
5. Health and social services public benefit determinations, applications, certifications, recertifications, and enrollment to the extent permitted or required by Applicable Law;
6. Public Health Activities and reporting to the extent permitted or required by Applicable Law;
7. Any purpose to demonstrate meaningful use of certified electronic health record technology by the (i) Submitter, (ii) Recipient or (iii) Covered Entity on whose behalf the Submitter or the Recipient may properly Transact Message Content under this Agreement, provided that the purpose is permitted by Applicable Law, including but not limited to the HIPAA regulations. "Meaningful use of certified electronic health record technology" shall have the meaning assigned to it in the regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102;
8. Uses and disclosures pursuant to an Authorization consistent with the HIPAA Regulations or other Applicable Law;
9. To an Individual User or for Individual Access Services; or
10. With regard to Governmental Participants, uses and disclosures permitted by California law, including Civil Code section 1798.24; or

11. As otherwise permitted or required by Applicable Law.

Definition of Public Health Activities

"**Public Health Activities**" shall mean an access, use, or disclosure permitted under the HIPAA Regulations and any other Applicable Law for public health activities and purposes, including an access, use, or disclosure permitted under 45 C.F.R. part 164.512(b) and 45 C.F.R. part 164.514(e). Public Health Activities excludes activities related to oversight or enforcement of laws, regulations, or rules by Governmental Participants.

REQUIREMENT TO RESPOND

REQUIREMENT TO RESPOND

7.1. All Participants that request, or allow their respective Participant Users to request, PHI for Treatment, Utilization Review, Quality Assurance and Improvement, Business Planning and Development, Public Health Activities, Individual Access Services, uses and disclosures pursuant to an Authorization, and Benefits Determination shall have a corresponding reciprocal duty to respond to requests for PHI for these purposes. A Participant shall fulfill its duty to respond by either (i) providing the requested PHI, or (ii) responding with a standardized response that indicates the PHI is not available or cannot be exchanged. All responses to requests for PHI shall comply with Specifications, this Agreement, any other data exchange agreements, and Applicable Law.

7.2. Participants may, but are not required to, exchange PHI or PII for an Exchange Purpose other than Treatment, Utilization Review, Quality Assurance and Improvement, Business Planning and Development, Public Health Activities, Individual Access Services, uses and disclosures pursuant to an Authorization, and Benefits Determination. Nothing in this Section 7 shall require a disclosure that is contrary to a restriction placed on PHI by a patient pursuant to Applicable Law.

Commented [8]: to the extent permitted by law (unclear why this first sentence would be needed - could also frame as "contract may not be interpreted to prohibit the sharing of information for other purposes permitted by law".

AUTHORIZATIONS

AUTHORIZATIONS

14.1. Participants shall disclose PHI or PII to another Participant with a legally valid Authorization.

14.2. In order to fulfill Section 14.1 above, Participants shall engage in one of the below activities:

1. Participants may accept another Participant's representations that a legally valid Authorization has been received. A Participant who has received an Authorization shall be responsible for ensuring the Authorization complies with all Applicable Law. Participants who have received an Authorization are responsible for maintaining documentation as required under Applicable Law and shall make such documentation available to other Participants in the event of a complaint, litigation, or other dispute. Participants may rely on documentation for a legally valid release of information submitted by third parties who are not Participants. Documentation may be submitted physically, electronically, or by facsimile. A Participant who provides assurances that an Authorization is legally valid shall indemnify and hold harmless a Participant who reasonably relied upon the assurances. Participants shall comply with the Policies and Procedures related to providing assurances.

2. Before disclosing PHI or PII, Participants may request a copy of an Authorization and shall evaluate the Authorization to ensure it is legally valid within a reasonable time. Once a Participant has determined the Authorization is legally valid, it shall disclose PHI or PII consistent with the Authorization and with the request for PHI or PII. A Participant who chooses not to provide assurances that an Authorization is legally valid shall not be liable to another Participant that acts upon the Authorization for the lack of legal validity of the Authorization.

14.3. Legally insufficient Authorizations. If a Participant has determined that an Authorization is not legally valid or has been revoked, the Participant shall not disclose PHI or PII but shall inform the Participant requesting PHI or PII that the Authorization is

Commented [9]: This opens up another category of mandated disclosures because its any time someone gets the authorization of the patient. Do we really want to use this agreement to do that? Feels like we should use this agreement to mandate disclosures for specific purposes we want to assure are promoted by this effort, vs. essentially opening this up to every request where the requestor managed to get the patient to authorize it.

Commented [10]: What's the scenario envisioned here?

legally insufficient. In no case shall a Participant disclose PHI or PII if an Authorization has been revoked or is legally insufficient.

14.4. Participants shall comply with the Policies and Procedures/Specifications for Authorizations.