|  |  |
| --- | --- |
| Requested Information | *Guidance on how to provide the requested information* |
| Commenter's Name (first name, last name) | *Robby Franceschini* |
| Commenter's Organization Name (full name) | *Connecting for Better Health* |
| Date That Comments Were Prepared | *June 1, 2022* |
| Comment File Name | *Connecting for Better Health\_Final \_060122.* |

## Data Exchange Framework

**3. CA Data Exchange Landscape\_Draft\_5.12.22**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| California Initiatives to Advance Data Exchange, Data Exchange in California Today | N/A | Missing state data sharing activities | We recommend that CalHHS include in both sections references to other state data sharing efforts, including the ePOLST registry included in AB 133; the DHCS Population Health Management Service; California Cancer Case Registry; California Parkinson’s Disease Registry; the Controlled Substance Utilization Review and Evaluation System (independent from Cal-HOP) and the California all-payer claims database. Including these efforts in the landscape assessment ensures that these initiatives are rightfully acknowledged as efforts to improve data sharing, including data sharing among organizations and the state. Moreover, CalHHS should outline in the landscape assessment how it envisions the DxF and DSA advancing these and the other state data sharing efforts enumerated in the document. This would importantly communicate to stakeholders how CalHHS and its subagencies envision the DxF and DSA reinforcing its data sharing efforts. |

**5. CalHHS\_DxF\_Governance\_Draft\_05-12-2022**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| Governance Legal and Contractual Framework | “Data Exchange Framework Governance decision-making authority will rest with the California Health and Human Services Agency, supported by CalHHS’ Center for Data Insights and Innovation (CDII) and an HIE Policy Board. 6 CDII will oversee initial implementation of the Data Sharing Agreement and ongoing development and maintenance of its Policies and Procedures and requirements for entities subject to AB133’s data sharing mandate. The HIE Policy Board should be established through legislation and, once established, will assume responsibility for a specified set of oversight functions.” | Need for enabling legislation | We recommend that CalHHS seek to establish legal authority for the governance model presented via Trailer Bill Language this legislative session. We support the model outlined and the opportunity for public input; however, given that the mandate to sign the DSA goes into effect for most providers and health plans on January 1, 2023, CalHHS should look to put its governance model in place as soon as possible to ensure that enabling legislation is in place that allows for the governance model to be in place, and for the Policy Board to enforce the mandate. |

## Data Sharing Agreement and Policies and Procedures

1. **DxF Single Data Sharing Agreement\_Draft\_5.12.22**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| Definitions | “Breach” shall mean the unauthorized acquisition, access, disclosure, or use of Health and Social Services Information as set forth in the Policies and Procedures. | Alignment with HIPAA | We recommend CalHHS cite the federal definition of “Breach” at 45 CFR § 164.402. |
| Definitions | ““Qualified Health Information Organization” or “Qualified HIO” shall mean a state-designated data exchange intermediary that facilitates the exchange of Health and Social Services Information between Participants.” | Detail of qualification process for HIOs | We recommend CalHHS create a process for qualifying HIO in the DSA and/or P&Ps. In particular, we recommend CalHHS utilize the process DHCS created for the Cal-HOP program for qualifying HIOS, with elements including:   * Status as a non-profit organization or local government agency based in California; * Openness to participation by any provider or health plan in their service region * Technical capacity to facilitate data exchange between Participants for all Required Purposes * Signatory to the DSA as a Participant (in place of signatory to the CalDURSA and CTEN participant).   CalHHS should also require HIOs allow any DSA Participant in their service region to participate in their organizations. |
| Definitions | “Health and Social Services Information” shall mean any and all information received, stored, processed, generated, used, transferred, disclosed, made accessible, or shared pursuant to this Agreement, including but not limited to: (a) Data Elements as set forth in the applicable Policy and Procedure; (b) information related to the provision of health care services, including but not limited to PHI; and (c) information related to the provision of social services. Health and Social Services Information may include PHI, PII, deidentified data (as defined in the HIPAA Regulations at 45 C.F.R. §164.514), pseudonymized data, metadata, digital identities, and schema.  …Personally Identifiable Information or PII shall have the same meaning as “Personal Information” set forth in Section 1798.140(o) of the California Civil Code.” | Reference to California Consumer Privacy Act; Alignment with federal and state law | We recommend removing the reference to the California Consumer Privacy Act definition of “personal information” in the definition of “Personally Identifiable Information or PII.” Most DSA Participants are unlikely to be subject to the CCPA. We instead recommend CalHHS cite to the definitions of “personal information” under California’s Civil Code, § § 1798.3 and 1798.80.Additionally, we recommend removing the references in the “Health and Social Services Information” to deidentified data and metadata. Under both federal and state law, de-identified data and metadata that doesn’t identify an individual are not considered health information or medical information, and therefore the use of such by DSA Participants should not be restricted.Lastly, we recommend CalHHS decouple the definition of “Health Information” from “Social Services Information.” We are concerned that subjecting social services organizations to the same privacy and security standards as health organizations may not be a workable solution, given that HIPAA and California law largely rely on treatment, health care operations and payment use cases that do not fit neatly for most social services organizations unless they are a Business Associate. Moreover, meeting the HIPAA Security Rule, while a worthy goal, may not be appropriate for social services organizations. CalHHS should instead pursue a stakeholder advisory process with social services organizations to understand their particular needs in a DSA that also includes health care organizations. |
| Minimum necessary | “ Any use or disclosure of PHI or PII pursuant to this Agreement will be limited to the minimum PHI or PII necessary to achieve the purpose for which the information is shared, except where limiting such use or disclosure to the minimum necessary (i) is not feasible, (ii) is not required under the HIPAA Regulations (such as for Treatment) or any other Applicable Law, (iii) is a disclosure to an Individual User or Individual User’s Personal Representative, (iv) is a disclosure pursuant to an Individual User’s Authorization, or (v) is a disclosure required by Applicable Law.” | Alignment with HIPAA | We recommend CalHHS cite the federal definition of “minimum necessary” at 45 CFR **§§** 164.502(b), 164.514(d).  Additionally, the current language would expand the minimum necessary standard to apply to all PII/PI, and it is not clear for what reason CalHHS has extended. Additionally, the DSA adds an exception for “feasibility,” which is vague and undefined. |
| Legal Requirements | (a) Monitoring and Auditing. The Governance Entity, acting through its agents and independent contractors, shall have the right, but not the obligation, to monitor and audit Participants’ compliance with their obligations under this Agreement. Unless prohibited by Applicable Law, Participants shall cooperate with the Governance Entity in these monitoring and auditing activities and shall provide, upon the reasonable request of the Governance Entity, complete and accurate information in the furtherance of its monitoring and auditing activities. To the extent that any information provided by Participants to the Governance Entity in connection with such monitoring and auditing activities constitutes Confidential Participant Information, the Governance Entity shall hold such information in confidence and shall not redisclose such information to any person or entity except as required by Applicable Law. | Request for more specificity | This section gives extremely broad auditing and monitoring powers to a “Governance Entity.” As mentioned above in our comments on the Data Exchange Framework, we recommend CalHHS create Trailer Bill Language that sets out CalHHS and the delegated Policy Board’s authority to lay out more specific parameters around what authority the Governance Entity has or doesn’t have.  We also recommend that the DSA explicitly contemplate inclusion in the Governance Entity of a broad stakeholder base to ensure transparency and accountability into the process by which the Governance Entity provides oversight, sets priorities, and crafts policies, particularly if/when CalHHS disbands the current Stakeholder Advisory Group. |

1. **Policy and Procedure: Process for Amending the DSA\_Draft\_5.12.22**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| Consideration of Proposed Amendments to the DSA | “Following the task force’s approval of the amendment to the DSA, the Participants shall be given at least forty-five (45) calendar days to review the approved amendment and register an objection if a Participant believes the amendment will have a significant adverse operational or financial impact on the Participant. Such objection shall be submitted to the Governance Entity and contain a summary of the Participant’s reasons for the objection…  …If the task group’s recommendation is to amend the DSA and the Governance Entity approves such a recommendation, the Governance Entity will circulate the amendment to all of the Participants for signature at least forty-five (45) calendar days prior to the effective date of the amendment, except in the event that a shorter time period is necessary in order to comply with Applicable Law.” | Lengthening timelines for comment and implementation of DSA amendments | We recommend that CalHHS adopt a 90-day period at a minimum for both comment periods and for implementation of new DSA amendments. While we understand that AB 133 exempts the DSA and DxF from the California Administrative Procedures Act, we believe that a 90-day requirement is more suitable to allow for adequate time for stakeholders to provide input on proposed amendments, and to implement approved amendments. A 45-day standard is too short to allow for both adequate stakeholder input, and time for Participants to make the necessary legal, technical and human resources changes to comply with amendments. |

1. **Policy and Procedure: Modifications to Policies and Procedures\_Draft\_5.12.22**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| Submission of Proposed, New, Amended, Repealed or Replaced Policies and Procedures | “Following the Governance Entity’s approval of the new, amended, repealed or replaced Policy, the Participants shall be given at least forty-five (45) calendar days to review the approved Policy and provide written comments to the Governance Entity, except in the event that a shorter time period is necessary in order to comply with Applicable Law. “ | Lengthening timelines for comment and implementation of P&Ps | We recommend that CalHHS adopt a 90-day comment period regarding proposed modifications to P&Ps, for the same reasons as listed above regarding amendments to the DSA. |

1. **Policy and Procedure: Data Elements to be Exchanged\_Draft\_5.12.22**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| Data to be Exchanged | “Participants shall make available or exchange, at a minimum, data as defined in the  subparagraphs below.  i. Health Care Providers, including but not limited to physician practices, organizations, and medical groups, general acute care hospitals, critical access hospitals, long term acute care hospitals, acute psychiatric hospitals, rehabilitation hospitals, skilled nursing facilities, and clinical laboratories, shall provide access to or exchange at a minimum:  a. Until October 6, 2022, data elements in the United States Core Data for Interoperability (USCDI) Version 1 and held by the entity.  b. After October 6, 2022, all Electronic Health Information (EHI) as defined under federal regulation in Section 171.102 of Title 45 of the Code of Federal Regulations and held by the entity.  ii. County health facilities that are Participants shall provide access to or exchange, at a minimum, the same data required of Health Care Providers in Section II.A Paragraph 1a as permitted under Applicable Law.  iii. Health Plans, including but not limited to health care service plans and disability insurers that provide hospital, medical, or surgical coverage that are regulated by the Department of Managed Health Care or the Department of Insurance, Medi-Cal managed care plans, shall provide access to or exchange, at a minimum, the data required to be shared under the Centers for Medicare and Medicaid Services Interoperability and Patient Access regulations  for public programs as contained in United States Department of Health and Human Services final rule CMS-9115-F, 85 FR 25510.  iv. Public health agencies that are Participants shall provide access to or exchange, at a minimum, the same data required of Health Care Providers in Section II.A Paragraph 1a as permitted by Applicable Law.  2 v. Intermediaries, including but not limited to health information exchange networks and health information organizations, that are Participants shall provide access to or exchange, at a minimum, all of the following that apply:  a. Data defined in Section II.A Paragraph 1a if providing exchange services to one or more Health Care Provider or county health facilities.  b. Data defined in Section II.A Paragraph 1c if providing exchange services to one or more Health Plan.  c. Data defined in Section II.A Paragraph 1d if providing exchange services to one or more public health agency.  b. Participants not listed in Paragraph 1, including but not limited to Social Services Organizations, shall provide access to or exchange Health and Social Services Information as defined broadly in the Data Exchange Framework Data Sharing Agreement. Data to be exchanged by other Participants, including Social Services Organization, may be the subject of a future revision to this policy…” | Citations to federal law | We recommend CalHHS cite to the Applicable Law related to the data that Health care providers and health plans are required to share. While we recognize that the latest draft of these requirements reflects the language of AB 133, we believe that citing the law will keep these requirements evergreen as laws change, and still be within the spirit of AB 133. |

1. **Policy and Procedure: Breach Notification\_Draft\_5.12.22**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| Policy | “Breaches are very serious events with potential for serious impact on Participants and the individuals whose Health and Social Services Information is breached. Thus, each Participant has the obligation to identify, notify, investigate and mitigate any known Breach or potential Breach and, when detection of a potential Breach has occurred, to notify the Governance Entity and any affected Participants of the potential Breach in accordance with the procedures herein. | Alignment with federal and state breach notification laws | The use of the term “potential Breach,” suggests that Participants need to report even potential, not just actual breaches, which neither federal nor state law require. We recommend CalHHS remove references to “potential” breaches. |
| Obligations of Participant | “a. As soon as reasonably practicable, but no later than seventy-two (72) hours after discovering a Breach has occurred, a Participant shall notify the Governance Entity and all affected Participants.  b. As soon as reasonably practicable, but no later than ten (10) calendar days after discovering a Breach has occurred, a Participant shall provide a written report of the Breach to the Governance Entity and all affected Participants....  c. Notwithstanding the above, Participants agree that within twenty-four (24) hours following the discovery of a Breach that may involve a Governmental Participant, Participants shall provide notification to all Governmental Participants that are likely impacted by the Breach in accordance with the procedures and contacts provided by such Governmental  Participant. ” | Timeframes for breach notification should mirror state and federal law; clarification | We recommend CalHHS incorporate state and federal law by reference and not create new breach notification timeframes via the DSA. For example, licensed health care facilities in California have up to 15 days (22 Health and Safety Code §§ 79902) to report a breach to the Department of Public Health, and Business Associates under HIPAA have 60 days to report a breach to Covered Entities (45 CFR §§ 164.400-414). The 72-hour and 10-day standards are burdensome and impracticable for organizations. Moreover, both HIPAA and California law do not require reporting of a breach notification if a risk analysis concludes that there is al ow probability that data has been comprised; this P&P does not include such an exception to the breach notification rule. Without the ability to conduct a risk analysis, the reporting obligation will be overwhelming for Participants.  We also recommend CalHHS remove the requirements to notify “affected Participants” and/or “likely impacted” Government Participants. In the alternative, we recommend that such terms be clarified to ensure consistency with federal and state law breach notification requirements. It is unclear how Participants will determine who the “affected Participants” are in the event of a breach, and to whom they must provide notice. Along those same lines, the terms “likely impacted” are vague and have unclear implications for purposes of needing to notify Governmental Participants.  Additionally, there is no current requirement under either federal or state law to notify affected parties other than the individual whose information is breached, the California Department of Public Health, and the California Office of Attorney General. |

1. **Policy and Procedure: Permitted Required and Prohibited Purposes\_Draft\_5.12.22**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| Definitions | “Health Care Operations” for purposes of this policy, shall consist of the following activities:  1. Quality Assessment and Improvement activities as described in subsection (1) of the definition of health care operations set forth at 45 C.F.R. § 164.501.  2. Population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives as set forth at 45 C.F.R. § 164.501…” | Health care operations definition should mirror HIPAA | We recommend CalHHS include all health care operations activities listed in 45 C.F.R. § 164.501. AB 133 specifies that CalHHS shall develop a data sharing agreement for treatment, payment, or health care operations.” Absent a compelling reason for excluding certain activities, CalHHS should include all activities in the definition in the P&P to ensure that all health care operations activities are “Required Purposes.” |
| Prohibited Purposes | “Unless otherwise permitted by Applicable Law, Participants shall not, for their own indirect or direct financial benefit, re-use, re-disclose, aggregate, de-identify, re-identify or engage in the Sale of Health and Social Services Information received through the DSA without explicit written authority to do so from the appropriate party. A Participant shall not be considered to be acting for its own benefit if:  (i) The Participant is a Business Associate and has a legally enforceable written agreement authorizing the re-use, re-disclosure, aggregation, de-identification or re-identification of such Health and Social Services Information. This shall not include the Sale of Health and Social Services Information;  (ii) The Participant is performing Individual Access Services at the direction of an Individual User or an Individual User’s Personal Representative; or  (iii) The Participant is a Social Services Organization and has a legally enforceable written agreement authorizing the re-use, re disclosure, aggregation, de-identification or re-identification of such Health and Social Services Information with a government entity, Government Participant or other Social Services Organization. This shall not include the Sale of Health and Social Services Information.” | Financial interest provisions should be removed | We recommend CalHHS remove entirely this section for several reasons. We note that while the prohibition on financial interests is a worthy goal, this will functionally require Participants to tag information received through the DSA unless there is a written agreement authorizing such re-use in place, which is a heavy burden for Participants, especially those with few IT and legal resources. This restriction may also have unintended consequences; for example, a provider may use data received under the auspices of the DSA for treatment to claim payment for services rendered, which would be considered a re-use of the data under the DSA.  We also recommend that CalHHS allow Participant to reuse, aggregate, de-identify information for any purpose permitted by Applicable Law.  Additionally, it is not clear why, if the policy intent is to prohibit the sale or other financial benefits of reusing data, Business Associates would still be allowed to do so under the DSA so long as there is a written agreement with the other party. |
| Prohibited Purposes | “Unless permitted by Applicable Law, Participants shall not, under the DSA, be required to exchange or provide access to any information subject to 42 C.F.R. Part 2.” | Unnecessary need for prohibition on requirement to share 42 C.F.R. Part 2 data | We recommend that CalHHS remove this provision. 42 C.F.R. Part 2 cannot be shared unless permitted by Applicable Law, making this provision irrelevant. Given that that SAMHSA is currently contemplating amendments to 42 C.F.R. Part 2, this provision is likely to require future, unnecessary modification to the P&Ps.  In the alternative, we recommend that CalHHS set out language that Participants shall not be required to exchange or provide access to any sensitive PHI or PI subject to any heightened requirements under Applicable Law except as permitted by such Applicable Law - rather than just focusing on Part 2, since there are other laws that deal with sensitive PHI (e.g., the Lanterman-Petris-Short Act protects mental health records and has stricter requirements than HIPAA). Leaving a more general reference to “Applicable Law” will obviate the need to make future modification to the P&Ps in the event Part 2 or other laws/regs are amended. |

1. **Policy and Procedure: Requirement to Exchange Health and Social Services Information\_Draft\_5.12.22**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| Duty to Respond | “All Participants that request Health and Social Services Information for Permitted Purposes or Required Purposes shall have a corresponding reciprocal duty to respond to requests for Health and Social Services Information for these purposes. A Participant shall fulfill its duty to respond by either (i) providing the requested Health and Social Services Information, or (ii) responding with a standardized response that indicates the Health and Social Services Information is not available or cannot be exchanged. All responses to requests for Health and Social Services Information shall comply with Specifications, the Data Sharing Agreement (the “DSA”), any other data exchange agreements, and Applicable Law.” | Timeframes to respond | We recommend CalHHS include timeframes for responses to “Required Purposes” in that respective Policy and Procedure. Without timeframes, the DxF will not get the state closer to realizing AB 133’s vision of “real-time data sharing.” While we recognize that there is no industry standard for sharing in a framework like this one, we recommend the DxF start with a “reasonableness” standard and develop more concrete timeframes through the P&P amendment process over time. |
| Duty to Respond | “All Participants that request Health and Social Services Information for Permitted Purposes or Required Purposes shall have a corresponding reciprocal duty to respond to requests for Health and Social Services Information for these purposes. A Participant shall fulfill its duty to respond by either (i) providing the requested Health and Social Services Information, or (ii) responding with a standardized response that indicates the Health and Social Services Information is not available or cannot be exchanged. All responses to requests for Health and Social Services Information shall comply with Specifications, the Data Sharing Agreement (the “DSA”), any other data exchange agreements, and Applicable Law.” | Proactive data sharing | We recommend CalHHS consider key use cases where proactive data sharing should occur and include those in this P&P. For example, under the CMS Interoperability and Patient Access Rule (24 CFR § 482.24), CMS already requires hospitals as a condition of participation in the Medicare program to share ADT notifications with the patient’s established primary care practitioner. Additionally, for example, state law requires persons including health care providers, public health professionals and laboratories to report cases or suspected cases of dangerous diseases or conditions, among other items, to the local health officer (17 Cal. Code Regs. §§2500, 2504, 2505, 2508). CalHHS should strongly consider requiring proactive sharing of data via the DSA where there are already existing reporting mandates. |
| Duty to Respond | N/A | Lack of enforcement provisions | We recommend that CalHHS flesh out the purposes and powers of the Governance Entity here, and also outline consequences for noncompliance with the Duty to Respond, and to noncompliance with the mandate to sign the DSA. While we realize that enforcement authority may require statutory authority, CalHHS should ensure that it proposes enforcement standards this legislative session, since the data sharing mandate goes into effect on January 1, 2023 for some health care organizations. Enforcement provisions would ensure the success of the DxF.  Any enforcement language should also address due process of Participants (e.g., notice, appeal rights, etc.). |
| N/A | N/A | Directory for Participant API endpoints | We recommend that CalHHS include in this P&P a requirement that the Agency maintain a directory of Participant API endpoints. Due to the fact that the data sharing mandate takes effect for most health care organization on January 1, 2023, CalHHS should ensure that it begins to build out a directory by which Participants can determine the endpoints to which they are to share data. |

1. **Policy and Procedure: Privacy and Security Safeguards\_Draft\_5.12.22**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| Privacy Standards and Safeguards | “To support the privacy, confidentiality and security of PHI or PII, each Participant hereby represents and warrants: i. If the Participant is a Covered Entity or a covered component of a Hybrid Entity, the Participant does, and at all times shall, comply with the HIPAA Regulations to the extent applicable and with Applicable Law. ii. If the Participant is a Business Associate, the Participant does, and at all times shall, comply with the provisions of its Business Associate Agreements (or for governmental entities relying upon 45 C.F.R. section 164.504(e)(3)(i)(A), its Memoranda of Understanding) and Applicable Law.” | Alignment with federal law | We recommend that any references to “at all times” be removed. It is not reasonable to expect that Participants can truthfully represent and warrant that they are in compliance with HIPAA and other laws *at all times.* |
| Privacy Standards and Safeguards | “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, as a contractual standard, at all times, at a minimum, comply with the provisions of the HIPAA Regulations at 45 C.F.R. part 164, subparts C and E, as if it were acting in the capacity of a Business Associate.” | Ensuring Social Service Organizations can meaningfully participate on exchange. | We recommend that CalHHS consider whether there are alternative means by which Social Service Organizations may be accommodated to ensure access to Health and Social Services Information- for example read-only access through a Qualified HIO to ease some of the security burdens on such organizations. The DSA defines “Participant(s)” to mean Social Services Organizations, which are not covered by HIPAA or the CMIA. This P&P provision, however, requires such organizations comply with the provisions of the HIPAA Regulations at 45 C.F.R. part 164, subparts C and E, as if it were acting in the capacity of a Business Associate. While Social Service Organizations that participate in the exchange should be subject to meaningful data security standards, many may struggle to comply with all of the HIPAA requirements applicable to Business Associates. |
| Privacy Standards and Safeguards | Each Participant, regardless of whether it, pursuant to federal law, is subject to the HIPAA Regulations, shall use appropriate safeguards to prevent unauthorized use or disclosure of PHI or PII in a manner consistent with HIPAA Regulations, including implementing appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of PHI or PII. | Alignment with federal and state laws | We recommend CalHHS remove the references to PII. This provision would impose the same safeguards required under HIPAA to prevent unauthorized use or disclosure of PHI to *PII*, which is not legally required of Participants not practical in many if not most circumstances. |

1. **Policy and Procedure: Individual Access Services\_Draft\_5.12.22**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Text** | **Summary of Comment** | **Full Text of Comment** |
| Policy; No Fees for Individual Access Services | “Participants shall provide an Individual User or the Individual User’s Personal Representative access to the Individual User’s PHI or PII in accordance with this policy.”  “A Participant may not charge another Participant any fees for PHI or PII exchanged in furtherance of this section.” | Alignment with state law | We recommend CalHHS clarify the requirements Participants have to respond to individual requests to access data, and ensure consistency with the language around an individual’s right to access to conform with patients’ rights under both federal and state law. This individual right to access will add a substantial additional burden for Participants if the expectation is that they are required to provide PHI or PII that it does not maintain, but that it may obtain from another Participant on the exchange (which appears to be the case, since Participants may not change other Participants “for PHI or PII exchanged in furtherance of this section.” Under HIPAA, a provider may deny requests by patients in such cases, “though if it knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.” 45 CFR 164.124(d).  We further recommend that CalHHS propose amendments to California state law through Trailer Bill Language to ensure that the proposed policy change regarding fees charged to patients is reflected in state law. Currently, Cal. Health and Safety Code § 123110(j)(1) states that a “health care provider may impose a reasonable, cost-based fee for providing a paper or electronic copy or summary of patient records…”  We also recommend, should CalHHS keep the prohibition on Participant fees, that QHIOs are able to charge their respective participants fees, some of whom may be DSA Participants. Most HIO business models charge health plans and large health systems fees for participation, and for this reason, should be given an exception.  Finally, we recommend CalHHS align with the federal information blocking rules and allow in specific circumstances where it may be burdensome for a Participant to respond to a request, for that Participant to charge fees on a requesting Participant. For example, the exceptions to the federal information blocking rules permit actors to charge fees as long as they are: based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests; reasonably related to the actor’s costs of providing the type of access, exchange, or use of EHI; and not based on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the actor. The exception does not apply to: a fee based in any part on the electronic access by an individual, their personal representative, or another person or entity designated by the individual to access the individual’s EHI; or a fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10). 45 CFR § 171.302. |