Requested Information	*Guidance on how to provide the requested information*	*Boxes shaded in green are locations for commenters to place information*
Commenter's Name (first name, last name)	*Please provide your first name and last name. Do not provide prefix, suffix or title (e.g., "Jane Smith" rather than "Ms. Jane Smith, CEO")*	Mark Savage
Commenter's Organization Name (full name)	*Please provide the full organization name and not abbreviations. For example, "Association of Community Organizations" rather than "ACO"*	Savage & Savage LLC
Date That Comments Were Prepared	*Please provide the date that you finalized your comments for submission to CalHHS/CDII.*	09/18/2023
Comment File Name	*Please provide the title of this file using the following convention: [Your Org Name]_[Your Last Name]_[Date Prepared]. For Example: Association of Community Organizations_Smith_Jan 20, 2023.xlxs*	Savage & Savage LLC_Savage_Sep 18, 2023_revised

Do not edit the below table - for CalHHS staff use only

Documents (i.e., Applicable Worksheets) That You Have Provided Comments On	
Document Name	**Status: "Yes" = comments in Worksheet**
1. P&P-Requirement to Exchange HSSI (amended)	*Yes*
2. P&P-Privacy Standards and Security Safeguards (amended)	*Yes*

General Instructions: Please use a single row for each individual comment; feel free to add new rows as needed.

Comment #	Applicable Text from Draft "P&P - Requirement to Exchange HSSI" Document	Applicable Page Number(s)	A Brief Title or Summary of Your Comment	Full Text of Your Comment
Please provide sequential numbering for your individual comments	*If applicable, please copy and paste the relevant text from draft DxF document in this field*	*Please input applicable page numbers in this field (e.g., "3" for a single page; "3-9" for a range of pages)*	*Please input a brief title or a high-level summary of your specific comment in this field.*	*Please input the full text of your comment in this field. Feel free to include any rationale or explanation for your comment.*
1	"The purpose of this policy is to set forth the responsibilities of Participants to respond to requests for Health and Social Services Information pursuant to the Data Exchange Framework."	1	Everyday exchange is both push and pull, but the policy limits its scope to "the responsibilities of Participants to respond to requests" and fails to cover the everyday exchanges where Participants initiate exchanges without a pending request or order. Section 130290 covers and mandates all "exchange," not just responses to order. The Policy must be revised to incorporate and cover push exchange as well, not just pull exchange.	The policy focuses on responses to requests (pull or query), but omits to cover initiation of exchange (push), which likewise occurs in so many important use cases under the Data Exchange Framework. The policy should be revised to incorporate both push and pull. The statute, sec. 130290(b)(1) and the Data Sharing Agreement govern "exchange" broadly and cover disclosure and transmission of health information with or without a request. Exchange is both push and pull. Providers, plans, and patients, for example, initiate exchanges as well as respond to requests. A referral to a specialist, a lab order, and public health reporting, for example, are initiated by providers, not responses to a request or order. A member of the shared care team, or an accountable care organization, may initiate exchange of new information to all members of the care team. A community-based organization or social services organization might initiate an exchange of information or initiate a referral, not just respond to a referral or request. Likewise, patients might initiate the submission of patient-generated health data or SDOH data without any pending order or request. A patient might initiate and direct the provider to transmit health information to a third party or the patient's third-party health app, as Congress provided in the HITECH Act, 42 USC § 17935. By its terms covering only responding to requests (pull or query exchange), the policy fails to cover a significant portion of exchanges within the mandate of AB 133. The draft policy should be reframed around exchange generally, and multi-directional exchange at that, not just responses to requests. I have been repeating this comment for some time (e.g. May 5, 2022 written comments; June 23, 2022 meeting; December 15, 2022 meeting; February 10, 2023 written comments). Each time I raise it, there seems to be recognition and agreement that exchange includes initiating exchange, not just responses to requests or queries. I urge CHHS to correct both this Policy and OPP-9 (Technical Requirements for Exchange) for all the reasons and use cases stated above.
2	"All Participants shall respond to requests for Health and Social Services Information made by other Participants and shall share Health and Social Services Information when required under the Permitted, Required and Prohibited Purposes Policy and Procedure. A Participant shall fulfill its duty to respond by either providing the requested Health and Social Services Information in accordance with the Data Sharing Agreement (the "DSA") and Applicable Law; or in the following circumstances, providing an appropriate error message or null response as specified by the technical standard in use and in accordance with the Technical Requirements for Exchange Policy and Procedure:"	1-2	This policy is ambiguous regarding whether Participants shall exchange generally and respond to certain requests--particularly Social Service Activities--as if they are Required Purposes requiring exchange, or Permitted Purposes permitting but not requiring exchange. The policy should clearly state that Social Service Activities for purposes of Treatment or Health Care Operations are a Required Purpose.	The policy provides that all "Participants shall respond to requests for Health and Social Services Information made by other Participants and shall share Health and Social Services Information when required under the Permitted, Required and Prohibited Purposes Policy and Procedure." The Permitted, Required and Prohibited Purposes Policy and Procedure, in turn, provides that "Treatment, Payment, Health Care Operations and Public Health Activities" are Required Purposes; and that Permitted Purposes "include but are not limited to Social Services Activities and Research activities." However, as federal policymakers and regulations have discussed, there are times and settings where Social Services Activities occur for purposes of Treatment or Health Care Operations, and in those contexts are Required Purposes, not Permitted Purposes. The policy is thus amiguous and fails to comport with federal standards in this respect. The policy should be amended to clearly state that Social Service Activities for purposes of Treatment or Health Care Operations are a Required Purpose and that Health and Social Services Information for such Social Services Activities and purposes shall be exchanged as Required Purposes. In proposed rulemaking in 2021, the Office for Civil Rights of the U.S. Department of Health and Human Services explained that the existing Privacy Rule permits covered health care providers and plans to disclose PHI, without prior consent, to third parties (public or private-sector entities) that provide health-related social and community-based services as part of the disclosing provider's treatment activities or health care operations or the disclosing plan's health care operations, e.g. coordination or management of treatment. OCR explained that this could include disclosures for Treatment or Health Care Operations to social services agencies, community based organizations, home and community-based services (HCBS) providers, and other similar third parties that provide health-related services to specific individuals for individual-level care coordination and case management, either as a covered provider's treatment activity or a covered provider's or health plan's health care operations activity. Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 86 Federal Register 6446, 6475 (Jan. 21, 2021). In such situations, this is a Required Purpose under the DSA and P&Ps, not a Permitted Purpose. This policy should be amended to state this clearly so there is no ambiguity about its being a Required Purpose, not a Permitted Purpose.

3	"A Participant shall fulfill its duty to respond by either providing the requested Health and Social Services Information in accordance with the Data Sharing Agreement (the "DSA") and Applicable Law; or in the following circumstances, providing an appropriate error message or null response as specified by the technical standard in use and in accordance with the Technical Requirements for Exchange Policy and Procedure: . . . 2) determines that an exception in the California Information Blocking Prohibitions Policy and Procedure applies;"	1-2	The policy directs Participants to provide "an appropriate error message or null response" whenever the Participant "determines that an exception in the California Information Blocking Prohibitions and Procedure applies." As written, this provision is both ambiguous and overbroad, and should be clarified. Firstly, with respect to the second scenario, following or using an exception to information blocking is voluntary, not mandatory, and the Participant may still choose to exchange the information even if it falls within an exception. Thus, the exception may "apply", but the Participant might *not* want to provide an error message or null response and might instead choose to exchange the information. Secondly, with respect to all four scenarios, the provision as written appears to direct the Participant to provide "an appropriate error message or null response" in response to the entire request, not just that part of the request that might fall within one of the four scenarios, and thus the provision is overbroad in this respect. The policy might instead provide for "an appropriate error message or null response	The policy directs Participants to provide "an appropriate error message or null response" whenever the Participant "determines that an exception in the California Information Blocking Prohibitions and Procedure applies." As written, this provision is both ambiguous and overbroad, and should be clarified. Firstly, with respect to the second scenario, following or using an exception to information blocking is voluntary, not mandatory, and the Participant may still choose to exchange the information even if it falls within an exception. (See https://www.healthit.gov/buzz-blog/information-blocking/to-share-or-not-to-share-whats-an-exception-to-information-blocking.) Thus, the exception may "apply", but the Participant might *not* want to provide an error message or null response and might instead choose to exchange the information. Secondly, with respect to all four scenarios, the provision as written appears to direct the Participant to provide "an appropriate error message or null response" in response to the entire request, not just that part of the request that might fall within one of the four scenarios, and thus the provision is overbroad in this respect. The policy might instead provide for "an appropriate error message or null response only to the extent that, and limited to that portion of the request, that" falls within one or more of the four exceptions. This second point applies to both "Required Purposes" and "Permitted Purposes."
4	"This policy does not override or supersede a restriction placed by an Individual or their Personal Representative on Access, Use, or Disclosure of their Health and Social Services Information by a Participant pursuant to Applicable Law."	3	Consistent with the HIPAA Privacy Rule, the provision should be corrected to track the individual's right to *request* a restriction, not a right to *place* a restriction (with one exception).	Under the Privacy Rule, 45 CFR § 164.522, the individual generally has the "right . . . to request restriction of uses and disclosures", but not a right to require that restriction be placed. With one exception, a covered entity is not required to agree to a requested restriction, and the decision is left to the covered entity. Indeed, FAQ number 26 iterates this point. This is the general standard. Special state and federal statutes may impose additional requirements for especially sensitive categories of health information, such as requiring the individual's consent before disclosure. To avoid confusion or ambiguity, I recommend that the draft provision be revised to address explicitly both the general rule and the special exceptions: "This policy does not override or supersede AN INDIVIDUAL'S RIGHT TO REQUEST THAT a restriction BE placed ~~by an Individual or their Personal Representative~~ on Access, Use, or Disclosure of their Health and Social Services Information by a Participant pursuant to 45 C.F.R. § 164.522, NOR DOES IT OVERRIDE OR SUPERSEDE A RESTRICTION PLACED BY AN INDIVIDUAL OR PERSONAL REPRESENTATIVE ON ACCESS, USE, OR DISCLOSURE OF THEIR HEALTH AND SOCIAL SERVICES INFORMATION BY A PARTICIPANT PURSUANT TO ANY OTHER Applicable Law."
5				
6				
7				
8				
9				
10				

General Instructions: Please use a single row for each individual comment; feel free to add new rows as needed.				
Comment #	**Applicable Text from Draft "P&P - Privacy Standards & Security Safeguards" Document**	**Applicable Page Number(s)**	**A Brief Title or Summary of Your Comment**	**Full Text of Your Comment**
Please provide sequential numbering for your individual comments	*If applicable, please copy and paste the relevant text from draft DxF document in this field*	*Please input applicable page numbers in this field (e.g., "3" for a single page; "3-9" for a range of pages)*	*Please input a brief title or a high-level summary of your specific comment in this field.*	*Please input the full text of your comment in this field.* *Feel free to include any rationale or explanation for your comment.*
1	"b. Participants who are Covered Entities or Business Associates under the HIPAA Regulations. . . . . ii. If the Participant is a Business Associate, the Participant shall comply with the privacy and security provisions of its Business Associate Agreements (or for governmental entities relying upon 45 C.F.R.§ 164.504(e)(3)(i)(A), its memoranda of understanding) and all other Applicable Law. iii. If the Participant is a Covered Entity or Business Associate, the Participant shall comply with the Policies and Procedures and shall update its Business Associate Agreements or memoranda of understanding if they conflict with the Policies and Procedures."	2	The new amendment requiring Participants to comply with the privacy and security requirements of their BAAs, but to update their BAAs if hey conflict with the Policies and Procedures, is a significant improvement, but the amendment should go further to provide that any conflicting provision of a BAA is void and unenforcable, no matter how long it might take the Participant to update its BAA. This recommendation borrows from ONC's regulations that conflicting provisions in contracts and agreements are void and unenforceable.	The previous version of this policy provided: "If the Participant is a Business Associate, the Participant shall comply with the provisions of its Business Associate Agreements . . . ." In my prior comments dated June 21, 2023, I explained that, under this previous version, Participants could readily use conflicting provisions in their Business Associate Agreements (BAA) to trump and not comply with requirements of the Data Sharing Agreement and Policies & Procedures. In response, the revised draft policy provides that the Participant shall comply with "the privacy and security provisions of its Business Associate Agreements," not the entire BAA; and it adds: "If the Participant is a Covered Entity or Business Associate, the Participant shall comply with the Policies and Procedures and shall update its Business Associate Agreements or memoranda of understanding if they conflict with the Policies and Procedures." This is a significant improvement. However, as amended, the policy is amiguous about whether and how long a Participant can comply with or require compliance with a conflicting provision in a BAA. The Participant still "shall comply" with the privacy and security provisions of its BAA. This would arguably include provisions currently in many BAAs that prohibit the BA from providing an individual with access to their health information under 45 CFR § 164.524 of the Privacy Rule. Adding the provision that the Participant shall update its BAAs if they conflict with the Policies and Procedures begs the question and does not resolve the ambiguity of what the Participant may continue to do under the conflicting provisions of the BAA until that update is complete (which could take a considerable amount of time). Thus, while I greatly appreciate the significant improvement, I repeat my prior additional recommendation: "The best solution is not just to delete or change this language of the Draft Privacy and Security P&P, but also to amend the DSA and include a broad provision that Participants shall not include terms in BAAs that conflict with the DSA and P&Ps as amended, and that any such term is void and unenforceable; that Participants shall notify all business associates that any provision in existing BAAs that violates the DSA and P&Ps, as amended, is void and will not be enforced; and that Participants shall then amend the BAAs to remove or void any and all such inconsistent provisions when the BAAs are next modified. At the very least, the state should make this change to the Privacy
2				
3				
4				
5				
6				
7				
8				
9				
10				