

## Suggested Framework for Additional IPA Review Criteria (Fourth Draft)

California's Information Practices Act (IPA) specifies certain minimum criteria that CPHS must consider when reviewing research applications under provisions of the IPA. In addition, CPHS may elect to consider additional factors related to data privacy and security. All research applications are currently required by the IPA to include:

- “a plan sufficient to protect personal information from improper use and disclosures, including sufficient administrative, physical, and technical safeguards to protect personal information from reasonable anticipated threats to the security or confidentiality of the information.” (Cal. Civ. Code § 1798.24(t)(1)(A).)
- “a sufficient plan to destroy or return all personal information as soon as it is no longer needed for the research project, unless the researcher has demonstrated an ongoing need for the personal information for the research project and has provided a long-term plan sufficient to protect the confidentiality of that information.” Cal. Civ. Code § 1798.24(t)(1)(B).)
- “sufficient written assurances that the personal information will not be reused or disclosed to any other person or entity, or used in any manner, not approved in the research protocol, except as required by law or for authorized oversight of the research project.” Cal. Civ. Code § 1798.24(t)(1)(C).)

In reviewing the sufficiency of such plans or written assurances, a reviewer will take the following risks into consideration:

- The requested data includes especially sensitive information about physical health, including but not limited to variables related to abortion, gender-affirming care, genetic testing, or HIV/AIDS testing.
- The requested data includes especially sensitive information about psychological health, including but not limited to variables related to clinical psychological tests, drug or alcohol abuse, sexual behavior, or suicide.
- The requested data includes especially sensitive social, economic, or legal information, including but not limited to variables related to immigration status, law enforcement or court records, income, or credit history.
- The requested data is for vulnerable populations described in the 2018 Common Rule (45 CFR 46), including but not limited to children, prisoners, individuals with impaired decision-making capacity, or economically or educationally disadvantaged persons.
- The researchers propose, or will later propose, to link the requested data to information from other sources, especially including those that fall within any of the previous descriptions.
- The researchers plan to add additional years of data in the future, either to provide longitudinal information about individuals already in the data or to add information about new individuals.

- The number or nature of variables that will be available in the data to be analyzed makes re- identification of individuals a possible risk despite researcher efforts to remove identifiers or mask the data.
- If the researchers propose to remove identifiers and store them separately, the length of time the identifiers will be retained.
- The researchers plan to disclose some or all of the data in a database that will be made available to other individuals not listed on the CPHS application.
- The researchers plan to disclose de-identified data that may allow re-identification, even if conforming to HIPAA safe harbor standards, taking into consideration any expert risk assessment provided by the researchers assessing the probability that individuals could be re-identified.
- When the data were originally collected, the individuals were not told that their information would be used for research.
- [Jared Goldman deleted an earlier version of this] Individuals whose information will be used would not expect that the data collected about them might be used for research.
- [Jared Goldman deleted an earlier version of this] Individuals whose information will be used would object to having their information used if they were aware of the research and its privacy procedures.

The approval of a research proposal shall include a review and determination that all the following additional criteria have been satisfied:

- If consent to use the information for research was obtained when the requested data were originally collected, the consent sufficiently describes the purposes of the proposed research.
- [Jared Goldman deleted an earlier version of this] The research does not include obtaining especially sensitive identifiers or information that should not be approved considering the risks associated with using them.
- The research does not include obtaining especially sensitive identifiers or information unnecessary to perform the research.