UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

OFFICE OF THE VICE PRESIDENT – RESEARCH AND INNOVATION

OFFICE OF THE PRESIDENT
1111 Franklin Street, 11th Floor
Oakland, California 94607-5200

October 31, 2024

Dr. Darci Delgado, PsyD
Interim Chair, Committee for the Protection of Human Subjects
Assistant Secretary, California Health and Human Services Agency
1215 O Street, 11th Floor
Sacramento, CA 95814

RE: Public Comment on Suggested Framework for Additional IPA Review Criteria

Dear Interim Chair Delgado:

I write on behalf of the University of California (UC) system regarding the suggested framework for additional Information Practices Act (IPA) review criteria developed by the Committee for Protection of Human Subjects (CPHS) Subcommittee.

The UC system is comprised of ten research-intensive campuses, six medical schools, and three affiliated U.S. Department of Energy national laboratories. As California's research arm, UC conducts a wide array of research utilizing state-managed data to inform many critical issues important to the state, including housing, homelessness, education, public health, public safety, and much more. These research efforts often involve close collaborations with state agencies that hold the data.

This letter serves to 1) express concerns on the suggested framework for additional IPA review criteria, and 2) recommend other actions CPHS can take to safeguard data in accordance with the IPA. The comments below are informed by discussions with the IRB Directors across the UC system.

I. Concerns on Suggested Framework for Additional IPA Review Criteria

UC understands and shares in the commitment to protect research participants' privacy. However, moving forward with the suggested IPA review criteria would preclude the ability to conduct vital research. The suggested framework muddles the role of CPHS as the body who reviews requests for state-held personal information pursuant to Civil Code section 1798.24(t) versus the entity serving as the IRB for the California Health and Human Services Agency (CalHHS). Many elements provided in the framework extend beyond requirements in the IPA, as explained in the table in Appendix A, and in some cases even beyond 45 CFR 46 (Common Rule). Muddling CPHS's role is especially concerning in instances when researchers already seek IRB review from their own

institutions and comply with the regulations of the Common Rule and many other regulatory requirements. Having expanded IPA review creates unnecessary confusion, burdens, and opens the very real possibility of incongruent reviews between CPHS and institutional IRBs.

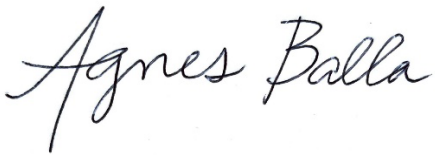
In addition, the proposed framework suggests that certain research would be approved only if researchers obtain individual consent retroactively. In some cases, researchers simply have no ability to obtain individual consent from everyone who may have information in a state database. Consequently, this requirement would effectively eliminate the ability of researchers to use state-held personal information for research aimed at advancing the health and safety of Californians. Legislative statutes already strike a careful balance between privacy concerns and the value of such data for research and hence to society, and the proposed CPHS regulations would undermine these carefully considered frameworks.

II. Recommended Actions CPHS Can Take to Safeguard Data in Accordance with the IPA

Rather than moving forward with the suggested framework, UC strongly advises that CPHS develop a checklist that guides researchers' understanding of appropriate technical safeguards in accordance with the IPA. See our recommended checklist in Appendix B.

UC would gladly assist CPHS in creating resources that shepherd understanding of IPA review while balancing the ability to move research forward. Thank you for your consideration on this important issue. If there is further information UC can provide on this matter that would be of help to CPHS, please do not hesitate to reach out to me at Agnes.Balla@ucop.edu.

Sincerely,



Agnes Balla
Director
Research Policy Analysis and Coordination
University of California, Office of the President

Cc: Agnieszka Rykaczewska, PhD

Appendix A.

Table Outlining How CPHS Framework Extends beyond IPA

Proposed Framework	Applicable IPA Clause	Comment
# 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	---	These elements are not within the scope of Civil Code section 1798.24(t) and should not be included in the suggested framework if researchers provide sufficient plans to protect the confidentiality of the personal information.
# 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.	---	We are unclear how future proposals can be evaluated under this consideration. This element should not be included in the suggested framework if researchers provide sufficient plans to protect the confidentiality of the personal information.
# 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.	1798.24(t)(1)(B)	This criterion is inconsistent with the statutory text at1798.24(t)(1)(B), which permit the researcher to demonstrate an ongoing need for the personal information and have a long-term plan sufficient to protect the confidentiality of that information.
# 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.	---	This criterion is in opposition to the IPA because it suggests that the data in question is deidentified data. However, the IPA applies only to “personal information,” defined as information “that identifies or describes an individual.”
# The researchers plan to retain, for an extended time, identifiers that they propose to remove and store separately.	1798.24(t)(1)(B)	This criterion is inconsistent with the statutory text at1798.24(t)(1)(B), which permit the researcher to demonstrate an ongoing need for

		the personal information and have a long-term plan sufficient to protect the confidentiality of that information.
# 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.	1798.24(t)(1)(C)	This criterion is inconsistent with the statutory text at 1798.24(t)(1)(C), which permit the researcher to provide 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.
# The researchers plan to disclose de-identified data that may allow re-identification, even if the data conform 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.	1798.24(t)(1)(C)	This criterion is inconsistent with the statutory text at 1798.24(t)(1)(C), which permit the researcher to provide 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.
# When the data were originally collected, the individuals were not told that their information would be used for research.	---	This element is not within the scope of the Civil Code section 1798.24(t), and would undermine the research exception in the IPA.
# When the data were originally collected, the individuals were not told that their information would be linked to data from other sources.	---	This element is not within the scope of the Civil Code section 1798.24(t), and would undermine the research exception in the IPA.
# The research and its privacy procedures would be unacceptable to the individuals whose information will be used if they were aware of it.	---	This element is not within the scope of the Civil Code section 1798.24(t).
# The researchers investigated what the individuals whose information will be used were told, when the data were originally collected, about using their information for research, and whether that was sufficient to serve as an informed consent.	---	This element is not within the scope of the Civil Code section 1798.24(t), and would undermine the research exception in the IPA as well as the ability of the IRB to grant a waiver of informed consent.
# The proposed use of data does not exceed any authorization given, at the time the data were originally collected, by the individuals whose information will be used, or would be eligible for a waiver of informed consent.	---	This element is not within the scope of the Civil Code section 1798.24(t), and would undermine the research exception in the IPA as well as the ability of the IRB to grant a waiver of informed consent.
# The research does not include obtaining especially sensitive identifiers or information which have undue risks associated with using them.	---	This element is not within the scope of the Civil Code section 1798.24(t) and should not be included in the suggested framework if justifying the information needed to perform

		the research as required under 1798.24(t)(3)(B).
# The research does not include obtaining especially sensitive identifiers or information unnecessary to perform the research.	1798.24(t)(3)(A-C)	This criterion contradicts with the requirement that researchers clearly justify that the information is needed to perform the research.

Appendix B.
UC Proposed Reviewer Checklist for IPA Compliance

In reviewing plans or written assurances for sufficiency, a reviewer will ensure the following is addressed:

- The system containing personal information must have sufficient administrative, physical, and technical controls in place to protect that personal information.
- Personal information must be encrypted during transfer, using Secure File Transfer Protocol (SFTP) or similar.
- Personal information must be encrypted at rest using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher, or similar.
- Access to personal information must use a role-based access control, and a list of authorized users must be maintained. Users must be issued a unique username, for their access only. Passwords must be based on information security best practices for password length, complexity, and reuse.
- The system hosting the personal information must automatically timeout, requiring re-authentication of the user session, after no more than fifteen (15) minutes of inactivity.
- The system must maintain an automated audit trail which must be archived for at least one (1) year. There must be a process for routinely storing and reviewing system logs for unauthorized access.
- To correct known security vulnerabilities, the researcher must install security patches and updates in a timely manner on all devices storing personal information.
- Researchers must have a plan for securely destroying the data upon termination of the project.