



Office of the Vice Provost for Research

To: NIH
From: University of Pennsylvania, Vice Provost for Research
Date: 08 January 2013
Subject: Submission to NIH Database of Genotypes and Phenotypes (dbGaP)

I am the responsible Institutional Official for the University of Pennsylvania. By way of this letter, I certify that I have approved the submission of data from the following research project to be submitted to the NIH Database of Genotypes and Phenotypes (dbGaP):

Protocol # 816980
Title: Genetic Variability in Taste Perception of Kaletra
Principal Investigator: Julie Mennella, PhD

This approval assures that:

- The data submission is consistent with all applicable laws and regulations, as well as institutional policies;
- All uses of these data that are deemed acceptable and approved per NIH policy and that follow the dbGAP procedures for access are allowable,
- The identities of research participants will not be disclosed to dbGAP; and
- The University of Pennsylvania IRB reviewed this application and verified that:

The submission of data to the NIH GWAS data repository and subsequent sharing for research purposes are consistent with the informed consent of study participants from whom the data were obtained;

The investigator's plan for de-identifying datasets is consistent with the standards outlined in the policy;

It has considered the risks to individuals, their families, and groups or populations associated with data submitted to the NIH GWAS data repository; and

The genotype and phenotype data to be submitted were collected in a manner consistent with 45 C.F.R. Part 46.

Sincerely,

A handwritten signature in black ink, appearing to read "Dawn A. Bonnell".

Dawn A. Bonnell, PhD
Vice Provost for Research
Henry Robinson Towne Professor of Engineering and Applied Science
Materials Science and Engineering

Addendum to the Data Use Certification Agreement Modification of Data Security Terms and Best Practices

Effective for all dbGaP Data Access Requests submitted on or after March 23, 2015, Section 6 of the Data Use Certification Agreement is replaced in its entirety by the following:

6. Data Security and Data Release Reporting

The Requester and Approved Users, including the institutional IT Director, acknowledge NIH's expectation that they have reviewed and agree to manage the requested dataset(s) according to the current NIH Security Best Practices for Controlled-Access Data Subject to the GDS Policy and the institutional IT security requirements and policies, and that the institution's IT security requirements and policies are sufficient to protect the confidentiality and integrity of the NIH controlled-access data entrusted to the Requester.

If approved by NIH to use cloud computing for the proposed research project, as outlined in the Research and Cloud Computing Use Statements of the Data Access Request, the Requester acknowledges that the IT Director has reviewed and understands the cloud computing guidelines in the NIH Security Best Practices for Controlled-Access Data Subject to the GDS Policy.

Requesters and PIs agree to notify the NIDCD DAC of any unauthorized data sharing, breaches of data security, or inadvertent data releases that may compromise data confidentiality within 24 hours of when the incident is identified. As permitted by law, notifications should include any known information regarding the incident and a general description of the activities or process in place to define and remediate the situation fully. Within 3 business days of the NIDCD DAC notification, the Requester, through the PI and the Institutional Signing Official, agree to submit to the NIDCD Data Access Committee a detailed written report including the date and nature of the event, actions taken or to be taken to remediate the issue(s), and plans or processes developed to prevent further problems, including specific information on timelines anticipated for action.

All notifications and written reports of data security incidents should be sent to:

NIDCD Data Access Committee URGENT: watsonb@nidcd.nih.gov

GDS mailbox: gds@mail.nih.gov

NIH, or another entity designated by NIH may, as permitted by law, also investigate any data security incident. Approved Users and their associates agree to support such investigations and provide information, within the limits of applicable local, state, and federal laws and regulations. In addition, Requesters and Approved Users agree to work with the NIDCD and NIH to assure that plans and procedures that are developed to address identified problems are mutually acceptable and consistent with applicable law.