DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

National Institutes of Health
Bethesda, Maryland 20892

DATE: 01/10/2025

TO: NIH OMB Desk Officer
Office of Management and Budget (OMB)
Reports Clearance Officer, DHHS

FROM: Mikia P. Currie
Chief, Project Clearance Branch

SUBJECT: Modification of Original dbGaP Authorized Access Forms, OMB Control Number: 0925-0670; Expiration Date: March 31, 2026

This is a request for OMB to approve a modification of "Original dbGaP Authorized Access Forms" to add an attestation of adherence to the NIH Security Best Practices for Users of Controlled-Access data and to update the language in the "Cloud Use Statement" and "Agreement to Adhere to Data Security Expectations". These changes implement NIH's *Update for Data Management and Access Practices Under the Genomic Data Sharing Policy* (NOT-OD-24-157), which updates security expectations for the management and access of controlled-access data subject to the GDS Policy. NIH requires this information to ensure that contemporary security standards commensurate with the sensitivity of controlled-access data are being met. Changes were last approved on 03/13/2023. OER intends to add the language in **Figure-1** and make the updates in **Figure-2** and **Figure-3** to the "Requesting Investigator: Access Web Form" section of dbGaP's online "Data Access Request" system. These changes are shown in slides 6-8 of the accompanying ppt**.** OER also intends to make the update in **Figure-4** for the "Institutional Signing Official: Access Web Form" section of dbGaP's online "Data Access Request" form. The same language in Figure 4 will be added to the "Institutional Signing Official: Access Web Form" for renewals. These changes are shown in slides 10 and 13 of the accompanying ppt**.**

Figure-1: "Attestation of NIH Security Best Practices for Users of Controlled-Access Data"

NIH expects that Approved Users of NIH controlled-access data under the GDS Policy systems comply with NIH Security Best Practices for Users of Controlled-Access Data and maintain such data on institutional IT systems, cloud service providers, and/or third-party IT systems with security standards that meet or exceed NIST SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" or the equivalent ISO/IEC 27001/27002 standards.

- ☐ By checking this box, I, as the PI requesting access to this data, attest that data will be secured, at a minimum, in accordance with NIST SP 800-171 or the equivalent ISO/IEC 27001/27002 standards as stipulated by the NIH Security Best Practices for Users of Controlled-Access Data.

Figure-2: Update to Clouse Use Checkbox

Original:

☐ I am requesting permission to use cloud computing to carry out the research described in my Research Use Statement.

Updated:

☐ By checking this box, I am requesting permission to use cloud computing to carry out the research as described in my Research Use Statement and attest that the cloud service provider and/or third-party IT system used for data analysis and/or storage will secure data, at a minimum, in accordance with NIST SP 800-171 or the equivalent ISO/IEC 27001/27002 standards as stipulated by the NIH Security Best Practices for Users of Controlled-Access Data.

Figure-3: Update to Cloud Use Statement

Original:
Describe the type(s) of cloud computing service(s) you wish to obtain (e.g., PaaS, SaaS, IaaS, DaaS) and how you plan to use it (them) to carry out the work described in your research use statement (e.g., datasets to be included, process for data transfer, analysis, and storage, and tools and/or software to be used). Also describe the role of any collaborators. Please limit your statement to 2000 characters.
Updated:
State the name of the cloud service provider and/or third-party IT system, their security standard, and how they will be used to carry out the work described in your Research Use Statement. Also, if applicable, describe the role of any collaborators. Please limit your statement to 2000 characters.

Figure-4: Update to "Agreement to Adhere to Data Security Expectations"

Original:
By signing below, I certify on behalf of this institution that the Information Technology Director, the Principle Investigator and other approved users under the DAR, and I have reviewed NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy and that we agree to manage and protect the requested dataset(s) by following those Best Practices as well as our own institutional IT security requirements and policies. I also certify that this institution's IT security requirements and policies are sufficient to protect the confidentiality and integrity of the requested dataset(s) entrusted to this institution.

☐ I agree

Updated:

☐ By checking this box, I attest on behalf of this institution that all institutional IT systems, cloud service providers, and/or third-party IT systems used for data analysis and/or storage will secure the requested data, at a minimum, in accordance with NIST SP 800-171 or the equivalent ISO/IEC 27001/27002 standards as stipulated by the NIH Security Best Practices for Users of Controlled-Access Data.

Your full consideration is appreciated.

NIH Office of Extramural Research (OER)
Website: https://grants.nih.gov/aboutoer
Email: oer@od.nih.gov