NIH Controlled Access Data — Approved User Assurance

Data requestor: _____

SAGE reference # _____ (Award Modification # or eGC1 #)

In order to submit a Data Access Request for NIH Controlled Access Data, you need:

- A compliant IT Environment
- If using a cloud environment, a Cloud Computing IT Environment Statement
- Confirmation from IT Director that this environment meets NIST SP 800-171 requirements
    - If using an environment hosted by non-UW service provider, a Confirmation from IT Director that such environment is deemed compliant by the service owner, and any system administrator responsibilities delegated to the IT Director will be carried out consistent with NIST SP 800-171
- Sign this assurance as the Approved User
- To have completed required compliance training(s)

The Cloud Computing IT Environment Statement is uploaded by you into the DAR.

Submit a copy of your DAR, Confirmation from IT Director and this signed assurance to the SAGE item and route to OSP for next steps.

As an Approved User, you must follow the below:

General Information Security Requirements

• Make sure these files are never exposed to the Internet with the exception of such connections as are required to download data from source repositories.

- For cloud infrastructure, investigators must restrict external access to instances and storage under the investigator's control (see section on cloud computing for more details).

• Data must never be posted on servers in any fashion that will make them publicly accessible, such as an investigator's (or institution's) website, because the files can be "discovered" by Internet search engines.

• Institutions (and your research team, department or unit) must not set up web or other electronic services that host the data publicly, or that provide access to other individuals that are not listed on the Data Use Request even if those individuals have access to the same dbGaP data.

• Utilize strong authentication technology for access control. Two factor authentication technology (smart cards, hard or soft token, etc.) is required.

• Do not place controlled access data on mobile devices (e.g. laptops, smartphones, tablets, mp3 players) or removable media such as USB thumb drives (except where such media are used as backups and follow appropriate physical security controls).

- If data must be placed on mobile devices, it must be encrypted. NIH recommends the use of NIST validated encryption technologies.

• Keep all software patches up-to-date.

Physical Security Requirements

• Data that are in hard copy or reside on portable media, e.g., on a USB stick, CD, flash drive or laptop (if necessary) should be treated as though it were cash, with appropriate controls in place. Such media must be encrypted and stored in a secured and locked facility with access granted to the minimum number of individuals required to efficiently carry out research.

• Restrict physical access to all servers, network hardware, storage arrays, firewalls and backup media only to those that are required for efficient operations.

• Log access to secure facilities, ideally with electronic authentication.

Controls for Servers

• Secure controlled-access data on the systems you are authorized to use and do not allow access to other users (restrict directory permissions to only the owner and group)

• If accessing the secure systems remotely, use encrypted data access (such as Secure Shell (SSH) or Virtual PrivateNetwork (VPN)).

Source Data and Control of Copies of Data

• Approved users must ensure only the Data Custodian, as named in the IT Director confirmation, can download the original version of the encrypted data.

• Do not make copies or extracts, except as allowed for retention purposes, and ensure that the information is not divulged to anyone except authorized staff members at the institution.

As collaborating investigators from other institutions must submit an independent DAR and be approved by NIH to access to the data, therefore, do not allow outbound access from devices that host controlled access data.

• Data downloaded from NIH-designated data repositories must be destroyed if they are no longer needed or used, or if the project is to be terminated and closed-out in the dbGaP Authorized Access System. Delete all data for the project from storage, virtual and physical machines, databases, and random access archives (i.e., archival technology that allows for deletion of specified records within the context of media containing multiple records).

• Investigators and Institutions may retain only encrypted copies of the minimum data necessary at their institution to comply with institutional scientific data retention policy and any data stored on temporary backup media as are required to maintain the integrity of the institution’s data protection program.

The data should not exist on backup media that is used by other projects. If retaining the data on separate backup media is not possible, as will be the case with many users, the media may be retained for the standard media retention period but may not be recovered for any purpose without a new Data Access Request approved by the NIH.

Retained data should be deleted at the appropriate time, according to institutional policies.

NIH Controlled Access Data — Approved User Assurance

I have read and acknowledge my responsibilities as an Approved User. I understand that if the Data Access Request is approved by NIH, that only the Data Custodian named in the IT Director confirmation may download the dataset into the IT environment.

I confirm I have taken the necessary training related to handling of controlled-access data and use of a restricted IT environment, as required by the University of Washington.

Approved User Name:_____

Signature : _____ Date: _____

Title:_____

Additional Approved User Name (if applicable):_____

Signature _____ Date: _____

Title:_____

Additional Approved User Name (if applicable):_____

Signature _____ Date: _____

Title:_____

Additional Approved User Name (if applicable):_____

Signature _____ Date: _____

Title:_____

If the Data Access Request includes more approved users, please attach additional signatures.