TERMS OF ACCESS AGREEMENT FOR DATA

This Terms of Access Agreement ("Agreement") is by and between The Trustees of the University of Pennsylvania (“Covered Entity”) and (Institution/Organization) on behalf of (School/Department/Unit&PI) and the additional authorized parties listed in Appendix 1 (“Data Recipient”). This Agreement is effective as of the date of the last signature below (“Effective Date”).

WHEREAS, Covered Entity maintains certain protected health information that Data Recipient wishes to use and/or disclose for research purposes;

WHEREAS, Covered Entity and Data Recipient are committed to protecting the privacy and security of confidential patient information in accordance with HIPAA Privacy Regulations, other federal and state laws, and contractual obligations;

WHEREAS, the Data Recipient plays a crucial role in ensuring the privacy and security of this confidential information;

NOW, THEREFORE, the Data Recipient and steward of Covered Entity’s confidential patient information, before receiving access to confidential patient information for the purposes of research, acknowledges and agrees to the following:

1. Data Recipient agrees to abide by the terms of this Agreement as well as applicable federal and state laws, and contractual obligations.
2. Data Recipient agrees that all terms used in this document will have the same definition as those set forth in the HIPAA Privacy Regulations.
3. The Data Set referred to in this agreement is defined in Appendix 1.
4. Data Recipient may be granted access to proprietary or confidential patient information. Data Recipient agrees that privacy and security of this information is their personal duty and responsibility.
5. Data Recipient hereby certifies that anyone given access to the Data Set under the terms of the agreement herein has completed all applicable privacy, human subjects, and security training and has read and signed this Agreement.
6. Data Recipient understands that, for the purposes of this study, they will be receiving a de-identified Data Set. Data Recipient understands that they must utilize the same level of protection for this de-identified Data Set as s/he would any other confidential, non-public information.
7. Data Recipient agrees not to use any data contained in the Data Set except as minimally necessary to perform research.
8. The Data Recipient agrees to abide by the conditions of the Data Use Certification Agreement, submitted as part of the application to NIAGADS Data Sharing Service (DSS) to obtain permission to access the Data, a copy of which is attached as Appendix 2 to this Agreement.
9. Data Recipient understands that only the Principal Investigator and the persons listed in Appendix 1 who have also read and acknowledged the terms of this Agreement (collectively "Authorized Parties"), are authorized to use the Data Set or any part of it on behalf of Data Recipient. All Authorized Parties agree to abide by the terms of this Agreement. Secondary data sharing is not permitted and the Data Set cannot be provided to non- Authorized Parties, except as described in Secondary Data Sharing described

in Schedule 1.

10. Data Recipient agrees not to use these Data for any purpose other than the study identified in Appendix 1 attached to this Agreement.
11. If at any time an additional Investigator or staff member from the same institution will gain access to the data requested, the Principal Investigator will need to amend this Agreement with their signature, the institutional signing official's signature, and the additional personnel's signature acknowledging that they have read and agree to the terms of this agreement.
12. Data Recipient agrees to use all reasonable means to protect the privacy and security of data in their control and prevent it from being inappropriately accessed or disclosed including but not limited to encrypting the data when in storage and in transit.
13. Data Recipient agrees not to attempt to re-identify the subjects that provided DNA for the study or to contact the individuals whose information is contained within the Data Set.
14. Data Recipient understands that, for the purposes of this agreement Covered Entity means the entity who provides the data they are receiving.
15. Data Recipient understands that the data provided may be aggregated with the data of other Covered Entities for this project.
16. Data Recipient will not use or disclose the data in the Data Set for marketing or fundraising purposes.
17. Data Recipient agrees that when their employment, affiliation, privileges, or assignment and this study ends, they will not take any data with them.
18. Data Recipient agrees to report to Covered Entity any use or disclosure of the data or any part of the data if not provided for by this Agreement of which Data Recipient or any Authorized Party becomes aware.
19. Any notice permitted or required by this Agreement shall be provided in writing and sent to the contact address as noted below.
20. Data Recipient understands that if they do not maintain the privacy and security of the Data Set they are in breach of this agreement and the agreement may be immediately terminated.
21. If this agreement is terminated, the Data Set must be immediately returned and/or destroyed as appropriate with confirmation from a University signing official or the equivalent.
22. Data Recipient understands that unauthorized use or disclosure of Personal Health Information (PHI) (including re-identification of a de-identified Data Set) may violate federal or state law and could result in criminal or civil penalties.
23. Further, Data Recipient agrees to indemnify, defend, and hold Covered Entity harmless from all costs and expenses (including attorney fees) that relate to a breach of Data Recipient's obligations hereunder.
24. Data Recipient understands that, in any publication about the study, Covered Entity will be acknowledged for its participation. Other than acknowledgment, Covered Entity will not be specifically mentioned in the publication without the written permission of Covered Entity.

[Signatures on Next Page]

Data Recipient has had the opportunity to read and understand this Terms of Access Agreement and agree to its terms and obligations as indicated by signing below:

COVERED ENTITY

THE TRUSTEES OF THE UNIVERSITY

OF PENNSYLVANIA

AUTHORIZED SIGNATURE

x _____

Printed Name: _____

Title: _____

_____

Date: _____

READ AND ACKNOWLEDGED

PRINCIPAL INVESTIGATOR

x _____

Printed Name: _____

Title: _____

_____

Date: _____

RECIPIENT

INSTITUTION

AUTHORIZED SIGNATURE

x _____

Printed Name: _____

Title: _____

_____

Date: _____

READ AND ACKNOWLEDGED

PRINCIPAL INVESTIGATOR

x _____

Printed Name: _____

Title: _____

_____

Date: _____

RECIPIENT INSTITUTION AUTHORIZED PARTIES READ AND ACKNOWLEDGED:

x _____

Printed Name:

Date:

x _____

Printed Name:

Date:

x _____

Printed Name:

Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

x _____
Printed Name:
Date:

Schedule 1.

Secondary data sharing – item 9 above: Signatories of this document are allowed to exchange the Data Set and data derived (secondary analysis data) from the Data Set with the PIs listed as collaborators and with approved Data Access Requests from the NIAGADS DSS. Sharing with other parties outside those specified as above are prohibited except with explicit approval by NADAC.

APPENDIX 1

1. Description of the Data Set the Recipient is requesting.

All primary and secondary/derived data provided by the NIAGADS DSS as approved by NADAC regarding your active Data Access Request(s). Primary data includes raw sequencing data (BAM, CRAM, FASTQ or gVCF format), subject phenotypes, and pedigree structures. Secondary/derived data are any data generated through reprocessing or analyses of the primary data.

2. Description of the project the data will be used for.

Insert DAR ID and Research Use Statement from NIAGADS DSS application for access to requested data here.

Insert name of Institution PI and all Authorized Parties here.

NIAGADS

DATA USE CERTIFICATION AGREEMENT

Last revised 4/05/2023

This Data Use Certification Agreement outlines the terms of use for requested controlled-access datasets maintained in NIH-designated data repositories under the NIH Genomic Data Sharing Policy (e.g., the NIA Genetics of Alzheimer's Disease Data Storage Site (NIAGADS)). The Addendum to this Agreement outlines additional terms and information which are specific to each requested dataset or study such as:

- NIAGADS Contact Information
- Data Use Limitation(s)
- Sponsoring NIH Institute or Center
- Responsible Data Access Committee
- Required Acknowledgement Statement

INTRODUCTION AND STATEMENT OF POLICY

The National Institute on Aging (NIA) has established the NIA Genetics of Alzheimer's Disease Data Storage Site (NIAGADS) as a resource to serve as a repository for many types of data generated by NIA supported grants and cooperative agreements and/or NIA funded biological samples. NIAGADS operates under the NIH Genomics Data Sharing Policy (GDS) and the NIA Genetics of Alzheimer's Disease Data Sharing Policy. Because the human genomic and phenotypic data contained in NIAGADS is, in some instances, potentially sensitive information, e.g., data related to the presence or risk of developing Alzheimer's Disease and related neurodegenerative disorders, and information regarding family relationships or ancestry, data must be shared in a manner consistent with the research participants' informed consent, and the confidentiality of the data and the privacy of participants must be protected.

Access to human genomic data will be provided to research investigators who, along with their institutions, have certified their agreement with the expectations and terms of access detailed below. It is the intent of NIH and the National Institute on Aging (NIA) that approved users of datasets obtained through this NIAGADS Data Access Request (DAR) recognize any restrictions on data use established by the submitting institution through the Institutional Certification and stated on the NIAGADS website https://www.niagads.org/.

Definitions of terminology in this document are found in section 14.

The parties to this agreement include: the Principal Investigator (PI) requesting access to the genomic study dataset (an "Approved User"), the PI's home institution as represented by the Institutional Signing Official (the "Requester"), and NIAGADS. The effective date of this agreement shall be the Project Approval Date, as specified on the NIAGADS approval notification.

TERMS OF ACCESS

1. Research Use

The Requester agrees that if access is approved, (1) the PI named in the Data Access Request (DAR) and (2) those named in the "Senior/Key Person Profile" section of the DAR, including the Information

Technology Director and any trainee, employee, or contractor[1] working on the proposed research project under the direct oversight of these individuals, shall become Approved Users of the requested dataset(s). Research use will occur solely in connection with the approved research project described in the DAR, which includes a 1-2 paragraph description of the research objectives and design. Investigators interested in using cloud computing for data storage and analysis must indicate in their Data Access Request (DAR) that they are requesting permission to use cloud computing and identify the cloud service provider (CSP) or providers and/or Private Cloud System (PCS) that they propose to use. They must also submit a Cloud Computing Use Statement as part of the DAR that describes the type of service and how it will be used to carry out the proposed research described in the Research Use Statement of the DAR. If investigators plan to collaborate with investigators outside their own institution, the investigators at each external site must submit an independent DAR using the same project title and Research Use Statement, and if using the cloud, Cloud Computing Use Statement. New uses of these data outside those described in the DAR will require submission of a new DAR; modifications to the research project will require submission of an amendment to this application (e.g., adding or deleting collaborators from the same institution, adding datasets to an approved project). Access to the requested dataset(s) is granted for a period of 1 year as defined below, with the option to renew access or close-out a project at the end of that year.

Submitting Investigator(s), or their collaborators, who provided the data or samples used to generate controlled-access datasets subject to the NIH GDS Policy and who have Institutional Review Board (IRB) approval and who meet any other study specific terms of access, are exempt from the limitation on the scope of the research use as defined in the DAR.

2. Requester and Approved User Responsibilities

The Requester agrees through the submission of the DAR that the PI named has reviewed and understands the principles for responsible research use and data management of the genomic datasets as defined in the NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy. The Requester and Approved Users further acknowledge that they are responsible for ensuring that all uses of the data are consistent with national, tribal, and state laws and regulations, as appropriate, as well as relevant institutional policies and procedures for managing sensitive genomic and phenotypic data. The Requester certifies that the PI is in good standing (i.e., no known sanctions) with the institution, relevant funding agencies, and regulatory agencies and is eligible to conduct independent research (i.e., is not a postdoctoral fellow, student, or trainee). The Requester and all Approved Users may use the dataset(s) only in accordance with the parameters described on the study page and in the Addendum to

[1] If contractor services are to be utilized, the principal investigator (PI) requesting the data must provide a brief description of the services that the contractor will perform for the PI (e.g., data cleaning services) in the research use statement of the DAR. Additionally, the Key Personnel section of the DAR must include the name of the contractor's employee(s) who will conduct the work. These requirements apply whether the contractor carries out the work at the PI's facility or at the contractor's facility. In addition, the PI is expected to include in any contract agreement requirements to ensure that any of the contractor's employees who have access to the data adhere to the GDS Policy, this Data Use Certification Agreement, and the NIH Security Best Practices for Controlled-Access Data Subject to the GDS Policy. Note that any scientific collaborators, including contractors, who are not at the same institution as the PI must submit their own DAR.

this Agreement for the appropriate research use, as well as any limitations on such use, of the dataset(s) and as described in the DAR and as required by law.

Through the submission of this DAR, the PI acknowledges receiving and reviewing a copy of the Addendum which includes Data Use Limitation(s) for each dataset requested. The PI agrees to comply with the terms listed in the Addendum.

Through submission of the DAR, the PI and Requester agree to submit either a project renewal or close-out request prior to the expiration date of the 1-year data access period. The PI also agrees to submit an annual progress update or a final progress report prior to the 1-year anniversary of the DAR, as described under *Research Use Reporting* below.

By approving and submitting the attached DAR, the Institutional Signing Official provides assurance that relevant institutional policies and related local, state, tribal, and federal laws and regulations, as applicable, have been followed, including IRB approval, if required. The PI may be required to have IRB approval if they have access to personal identifying information for research participants in the original study at their institution, or through their collaborators. The Institutional Signing Official also assures, through the approval of the DAR, that other institutional departments with relevant authorities (e.g., those overseeing human subjects research, information technology, technology transfer) have reviewed the relevant sections of the NIH GDS Policy and the associated procedures and are in agreement with the principles defined.

The Requester acknowledges that controlled-access datasets subject to the NIH GDS Policy may be updated to exclude or include additional information. Unless otherwise indicated, all statements herein are presumed to be true and applicable to the access and use of all versions of these datasets.

3. Public Posting of Approved Users' Research Use Statement

The PI agrees that information about themselves and their approved research use will be posted publicly on the NIAGADS website. The information includes the Approved User's name and institution, project name, research use statement, and a non-technical summary of the research use statement. In addition, and if applicable, this information may include the Cloud Computing Use Statement and name of the Cloud Service Provider (CSP) or Private Cloud System (PCS). Citations of publications resulting from the use of datasets obtained through this DAR may also be posted on the NIAGADS website.

4. Non-Identification

Approved Users agree not to use the requested datasets, either alone or in concert with any other information, to identify or contact individual participants from whom data and/or DNA samples were collected. Approved Users also agree not to generate information (e.g., facial images or comparable representations) that could allow the identities of research participants to be readily ascertained. These provisions do not apply to research investigators operating with specific IRB approval, pursuant to 45 CFR 46, to contact individuals within datasets or to obtain and use identifying information under an IRB

approved research protocol. All investigators conducting "human subjects research" within the scope of 45 CFR 46 must comply with the requirements contained therein.

5. Certificate of Confidentiality

Effective March 15, 2017 the Certificate of Confidentiality (Certificate) issued for the NIA Genetics of Alzheimer's Disease Data Storage Site (NIAGADS) is subject to the requirements of section 301(d) of the Public Health Service Act (42 U.S.C. 241(d)). Moreover, as of October 1, 2017 NIAGADS is required to adhere to the *NIH Policy for Issuing Certificates of Confidentiality* (NOT-OD-17-109). Therefore, Approved Users of NIAGADS, whether or not funded by the NIH, who access a copy of information protected by a Certificate held by NIAGADS, are also subject to the requirements of the Certificate of Confidentiality and subsection 301(d) of the Public Health Service Act.

Under Section 301(d) of the Public Health Service Act and the *NIH Policy for Issuing Certificates of Confidentiality*, recipients of a Certificate of Confidentiality shall not:

- Disclose or provide, in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding, the name of such individual or any such information, document, or biospecimen that contains identifiable, sensitive information about the individual and that was created or compiled for purposes of the research, unless such disclosure or use is made with the consent of the individual whom the information, document, or biospecimen pertains; or
- Disclose or provide to any other person not connected with the research the name of such an individual or any information, document, or biospecimen that contains identifiable, sensitive information about such an individual and that was created or compiled for purposes of the research.

Disclosure is permitted only when:

- Required by Federal, State, or local laws (e.g., as required by the Federal Food, Drug, and Cosmetic Act, or state laws requiring the reporting of communicable diseases to State and local health departments), excluding instances of disclosure in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding;
- Necessary for the medical treatment of the individual to whom the information, document, or biospecimen pertains and made with the consent of such individual;
- Made with the consent of the individual to whom the information, document, or biospecimen pertains; or
- Made for the purposes of other scientific research that is in compliance with applicable Federal regulations governing the protection of human subjects in research.

6. Non-Transferability

The Requester and Approved Users agree to retain control of the data obtained through the attached DAR, and any Data Derivatives of controlled-access datasets, and further agree not to distribute controlled-access datasets and Data Derivatives of controlled-access datasets to any entity or individual

not identified in the submitted DAR. If Approved Users are provided access to controlled-access datasets subject to the GDS Policy for inter-institutional collaborative research described in the research use statement of the DAR, and all members of the collaboration are also Approved Users through their home institution(s), data obtained through this DAR may be securely transmitted within the collaborative group. Approved Users are expected to follow all data security practices and other terms of use defined in this agreement, the NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy, and the Requester's IT security requirements and policies.

The Requester and Approved Users acknowledge responsibility for ensuring the review and agreement to the terms within this Data Use Certification Agreement and the appropriate research use of controlled-access data obtained through the attached DAR and any Data Derivatives of controlled-access datasets by research staff associated with any approved project, subject to applicable laws and regulations. Controlled-access datasets obtained through this DAR and any Data Derivatives, in whole or in part, may not be sold to any individual at any point in time for any purpose.

The PI agrees that if they change institutions during the access period they will complete the DAR close-out process before moving to their new institution. A new DAR and Data Use Certification, in which the new Requester agrees to the GDS Policy, must be approved by the NIAGADS Data Use Committee (NIAGADS DUC) and the NIAGADS AD/RD Data Access Committee (NADAC) before controlled-access data obtained through this NIAGADS DAR may be re-accessed. As part of the close-out process, any versions of the data stored at the institution and/or CSP must be destroyed and destruction confirmed by the Signing Official, as described below.

7. Data Security and Unauthorized Data Release

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

If approved by NIAGADS 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 NIH Genomic Data Sharing (GDS) Policy.

Requesters and PIs agree to notify NIAGADS 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 NIAGADS notification, the Requester, through the PI and the Institutional Signing Official, agree to submit to NIAGADS 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. The Requester agrees to provide documentation verifying that the remediation plans have been implemented. Repeated violations or unresponsiveness to NIAGADS requests may result in further compliance measures affecting the Requester.

All notifications and written reports of data security incidents and policy compliance violations should be sent to NIAGADS as indicated in the Addendum to this Agreement.

NIA, NIH, or another entity designated by NIH may, as permitted by law, also investigate any data security incident or policy violation. 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 NIAGADS DUC and NADAC and NIH to assure that plans and procedures that are developed to address identified problems are mutually acceptable and consistent with applicable law.

8. Policy Compliance Violations

The Requester and Approved Users acknowledge that the NADAC may terminate the DAR, including this Agreement and immediately revoke or suspend access to all controlled-access datasets subject to the NIH GDS Policy at any time if the Requester is found to be no longer in agreement with the principles outlined in the NIH GDS Policy, the terms described in this Agreement, or the Genomic Data User Code of Conduct. The Requester and PI agree to notify NIAGADS of any violations of the NIH GDS Policy, this Agreement, or the Genomic Data User Code of Conduct data within 24 hours of when the incident is identified. Repeated violations or unresponsiveness to NIH requests may result in further compliance measures affecting the Requester.

Requesters and PIs agree to notify NIAGADS 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 NIAGADS notification, the Requester, through the PI and the Institutional Signing Official, agree to submit to NIAGADS 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. The Requester agrees to provide documentation verifying that the remediation plans have been implemented. Repeated violations or unresponsiveness to NIAGADS requests may result in further compliance measures affecting the Requester.

All notifications and written reports of data security incidents and policy compliance violations should be sent to NIAGADS as indicated in the Addendum to this Agreement.

NIA, NIH, or another entity designated by NIH may, as permitted by law, also investigate any data security incident or policy violation. 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 NIAGADS DUC and

NADAC and NIH to assure that plans and procedures that are developed to address identified problems are mutually acceptable and consistent with applicable law.

9. Intellectual Property

By requesting access to genomic dataset(s), the Requester and Approved Users acknowledge the intent of the NIH that anyone authorized for research access through the attached DAR follow the intellectual property (IP) principles in the NIH GDS Policy as summarized below:

Achieving maximum public benefit is the ultimate goal of data distribution through the NIH- designated data repositories. The NIH encourages broad use of NIH-supported genotype- phenotype data that is consistent with a responsible approach to management of intellectual property derived from downstream discoveries, as outlined in the NIH Best Practices for the Licensing of Genomic Inventions and its Research Tools Policy.

The NIH considers these data as pre-competitive and urges Approved Users to avoid making IP claims derived directly from the genomic dataset(s). It is expected that these data, and conclusions derived therefrom, will remain freely available, without requirement for licensing. However, the NIH also recognizes the importance of the subsequent development of IP on downstream discoveries, especially in therapeutics, which will be necessary to support full investment in products to benefit the public.

10. Dissemination of Research Findings and Acknowledgement of Controlled-Access Datasets Subject to the NIH GDS Policy

It is NIH's intent to promote the dissemination of research findings from controlled-access dataset(s) subject to the GDS Policy as widely as possible through scientific publication or other appropriate public dissemination mechanisms. Approved Users are strongly encouraged to publish their results in peer-reviewed journals and to present research findings at scientific meetings.

Approved Users agree to acknowledge the Contributing Investigator(s) who submitted data from the original study to NIAGADS, the primary funding organization that supported the Contributing Investigators, and the NIAGADS in all oral and written presentations, disclosures, and publications resulting from any analyses of controlled-access data obtained through this DAR. Approved Users further agree that the acknowledgment shall include the reference to NIAGADS accession number specific version of the dataset(s) analyzed. An acknowledgment statement is provided for each dataset in the Addendum to this Agreement.

Acknowledgment statement for use of data distributed by NIAGADS:
Data for this study were prepared, archived, and distributed by the National Institute on Aging Alzheimer's Disease Data Storage Site (NIAGADS) at the University of Pennsylvania (U24AG041689), funded by the National Institute on Aging.

11. Research Use Reporting

To assure adherence to NIH policies and procedures for genomic data, PIs agree to provide annual progress updates as part of the annual project renewal or project close-out processes, prior to the expiration of the 1-year data access period. PIs who are seeking renewal or close-out of a project agree to complete the appropriate online forms and provide specific information such as how the data have been used, including publications or presentations that resulted from the use of the requested dataset(s), a summary of any plans for future research use (if the requester is seeking renewal), any violations of the terms of access described within this Data Use Certification Agreement and the implemented remediation, and information on any downstream intellectual property generated from the data. PIs also may include general comments regarding suggestions for improving the data access process in general. Information provided in the progress updates helps NIH evaluate program activities and may be considered by the NIH GDS governance committees as part of NIH's effort to provide ongoing oversight and management of data sharing activities subject to the GDS Policy.

12. Non-Endorsement, Indemnification

The Requester and Approved Users acknowledge that although all reasonable efforts have been taken to ensure the accuracy and reliability of controlled-access data obtained through this DAR, the NIH, the NIAGADS Data Use Committee, and Contributing Investigators do not and cannot warrant the results that may be obtained by using any data included therein. NIH, NIA, NIAGADS, NADAC and all contributors to these datasets disclaim all warranties as to performance or fitness of the data for any particular purpose.

No indemnification for any loss, claim, damage, or liability is intended or provided by any party under this agreement. Each party shall be liable for any loss, claim, damage, or liability that said party incurs as a result of its activities under this agreement, except that NIH, as an agency of the United States, may be liable only to the extent provided under the Federal Tort Claims Act, 28 USC 2671 et seq.

13. Termination and Violations

Upon project close-out, all Approved Users agree to destroy all copies, versions, and Data Derivatives of the dataset(s) retrieved from NIAGADS, on both local servers and hardware, and if cloud computing was used, delete the data and cloud images from cloud computing provider storage, virtual and physical machines, databases, and random access archives, in accord with the NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy. However, the Requester may retain these data as necessary to comply with any institutional policies (e.g., scientific data retention policy), law, and scientific transparency expectations for disseminated research results, and/or journal policies. A Requester who retains data for any of these purposes continues to be a steward of the data and is responsible for the management of the retained data in accordance with the NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy, and any institutional policies. Any retained data may only be used by the PI and Requester to support the findings (e.g., validation) resulting from the research described in the DAR that was submitted by the Requester

and approved by NADAC. The data may not be used to answer any additional research questions, even if they are within the scope of the approved Data Access Request, unless the Requester submits a new DAR and is approved by the NADAC to conduct the additional research. If a Requester retains data for any of these purposes, the relevant portions of Terms 4, 5, 6, 7, and 11 remain in effect after termination of this Data Use Certification Agreement. These terms remain in effect until the data is destroyed.

14. Definitions

Approved User: A user approved by the relevant Data Access Committee(s) to access one or more datasets for a specified period of time and only for the purposes outlined in the Principal Investigator (PI)'s approved Research Use Statement. The Information Technology (IT) Director indicated on the Data Access Request, as well as any staff members and trainees under the direct supervision of the PI are also Approved Users and must abide by the terms laid out in the Data Use Certificate Agreement.

Collaborator: An individual who is not under the direct supervision of the PI (e.g., not a member of the PI's laboratory) who assists with the PI's research project involving controlled-access data subject to the GDS Policy. Internal collaborators are employees of the Requester and work at the same location/campus as the PI. External collaborators are not employees of the Requester and/or do not work at the same location as the PI, and consequently must be independently approved to access controlled-access data subject to the GDS Policy.

Contributing Investigator: An investigator who submitted a genomic dataset to an NIH-designated data repository (e.g., NIAGADS).

Cloud Computing: The National Institute for Standards and Technology defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. For more information see NIST Special Publication 800-145.

Cloud Service Provider (CSP): A company or institution that offers some component of cloud computing to other businesses or individual, typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS), as defined by the National Institute of Standards and Technology. For more information see NIST Special Publication 800-145.

Data Access Request (DAR): A request submitted to a Data Access Committee for a specific "consent group" specifying the data to which access is sought, the planned research use, and the names of collaborators and the IT Director. The DAR is signed by the PI requesting the data and her/his Institutional Signing Official. Collaborators and project team members on a request must be from the same institution or organization.

Data Derivative: any data including individual-level data or aggregate genomic data that stems from the original dataset deposited (e.g. imputed or annotated data) in NIH-designated data repositories (e.g.,

NIAGADS). Summary information that is expected to be shared through community publication practices in not included in this term.

Data Use Certification Agreement (DUC): An agreement between the Approved Users, the Requester, and University of Pennsylvania regarding the terms associated with access of controlled-access datasets subject to the GDS Policy and the expectations for use of these datasets.

Genomic Data User Code of Conduct: Key principles and practices agreed to by all research investigators requesting access to controlled-access data subject to the NIH GDS Policy. The elements within the Genomic Data User Code of Conduct reflect the terms of access in the Data Use Certification Agreement. Failure to abide by the Genomic Code of Conduct may result in revocation of an investigator's access to any and all approved datasets.

Information Technology (IT) Director: Generally, a senior IT official with the necessary expertise and authority to affirm the IT capacities at an academic institution, company, or other research entity. The IT Director is expected to have the authority and capacity to ensure that the NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy and the institution's IT security requirements and policies are followed by the Approved Users.

Institutional Certification: Certification by the Submitting Institution that delineates, among other items, the appropriate research uses of the data and the uses that are specifically excluded by the relevant informed consent documents. Further information may be found here.

Institutional Signing Official: The label, "Signing Official," is used in conjunction with the NIH eRA Commons and refers to the individual that has institutional authority to legally bind the institution in grants administration matters. The individual fulfilling this role may have any number of titles in the institution, but is typically located in its Office of Sponsored Research or equivalent. The Signing Official for the Requester reviews Data Access Request, Project Renewal, and Project Close-out applications submitted by Principal Investigators and legally binds the Requester to agree to adhere to the terms described in this Agreement if the application is submitted to NIH. The Institutional Signing Official for the Submitting Institution enters into the Institutional Certification and signs on behalf of the Submitting Investigator(s) who has submitted data.

NIAGADS Alzheimer's Disease and Related Dementias (ADRD) Data Access Committee (NADAC): A committee made up of NIH staff and University of Pennsylvania investigators that reviews Data Access Request applications made by Principal Investigators.

NIAGADS Data Use Committee (DUC): The Data Use Committee (DUC) is independently formed by NIA. The DUC reviews all plans to return derived/secondary data to NIAGADS.

Principal Investigator (PI): The investigator who prepares Data Access Requests (DARs), Project Renewals, and Project close-outs. The Principal Investigator plays a lead role in ensuring that management and use of controlled-access data remains consistent with the terms in the Data Use Certification Agreement. To be able to submit a DAR, a Principal Investigator must be designated as such by their institution in eRA Commons *and* be a permanent employee of their institution at a level

equivalent to a tenure-track professor or senior scientist with responsibilities that most likely include laboratory administration and oversight.

Private Cloud System (PCS): A cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Progress Update: Information included with the annual Data Access Request (DAR) renewal or close- out summarizing the analysis of controlled-access datasets obtained through the DAR and any publications and presentations derived from the work.

Project Close-out: Termination of a research project that used controlled-access data from an NIH-designated data repository (e.g., NIAGADS) and confirmation of data destruction when the research is completed and/or discontinued. The project close-out process is completed by NIAGADS.

Project Renewal: Renewal of a PI's access to controlled-access datasets for a prior-approved project.

Requester: The home institution or organization of the PI that applies to NIAGADS for access to controlled-access data subject to the GDS Policy.

Senior/Key Persons: Collaborators at the home institution of the data submitter or Requester, such as the Information Technology Director.

Submitting Institution: An organization who submitted a genomic dataset to an NIH-designated data repository (e.g., NIAGADS).

Submitting Investigator: An investigator who submitted a genomic dataset to an NIH designated data repository (e.g., NIAGADS).