

NCATS National Clinical Cohort Collaborative (N3C) Enclave DATA USE AGREEMENT

This Institutional Data Use Agreement ("Agreement") is between the National Center for Advancing Translational Sciences (NCATS), a component of the National Institutes of Health, _____ ("Institutional Requester") and _____ ("Data Access Requester") (each a "Party" and collectively, the "Parties") which will become effective on the date ("Effective Date") of the last signature below.

WHEREAS the NCATS mission is to turn research observations into health solutions through translational science.

WHEREAS the N3C Enclave ("N3C Enclave") facilitates information dissemination and research through data sharing. The N3C Enclave contains clinical data sets including, but not limited to, data derived from a Limited Data Set originating from records of individuals who have received longitudinal care from Data Contributors and/or, when available, synthetic data product(s) derived from the Limited Data Set.

WHEREAS the N3C Enclave is built upon a state-of-the-art analytics platform that emphasizes data security, confidentiality of records, and recognizes investigator contributions, it will facilitate Approved User(s) investigators' collaborative research efforts on an array of innovative technologies and novel analyses.

WHEREAS the N3C Enclave will support research by enabling the rapid collection and analysis of data such as clinical, laboratory, and diagnostic data from Data Contributors that have transferred Data via a Data Transfer Agreement to the N3C Enclave. Within the N3C Enclave, disease agnostic clinical data will be aggregated and harmonized on a recurring basis from participating Data Contributors to facilitate Approved User(s) research.

WHEREAS Institutional Requester(s) whose Data Access Requester wishes to access and use the Data for public health purposes and health-related/biomedical research will need to submit a Data Access Request (DAR) for every proposed project. A DAR will outline patient selection criteria which will be used to provide a unique dataset for each approved DAR. This Data Use Agreement establishes the only permitted uses of the Data by the Approved User(s) as assured by the Institutional Signing Official.

I. Definitions

1. **Approved User(s)** is a user approved by the relevant NIH Data Access Committee to access one or more datasets for a specified period, only for the purposes outlined in the Data Access Requester's approved Research Use Statement, and consistent with this Agreement and applicable rules. Any person under the direct supervision and control of the Data Access Requester are also Approved User(s) and must abide by the terms laid out in the Data Use Agreement and that of their home institution.
2. **Collaborator:** An individual whose identity has been validated and who is a permanent employee of their institution at a level equivalent to a tenure-track professor or senior scientist equivalent, but who is not under the direct supervision and control of the Data Access Requester submitting the Access Request, who assists with the research project involving controlled-access data. Internal Collaborators are employees of the Institutional Requester and work at the same institution as the Data Access Requester. External Collaborators are not employees of the Institutional Requester and/or do not work at the same location as the Data Access Requester and consequently must be independently approved to access controlled-access data.
3. **Data (also referred to as controlled-access data)** collectively means source Data Sets including clinical data to support comparative studies, provided or received herein:

- a. **Limited Data Set:** As defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and in accordance with 45 CFR § 164.514(e)(2) of the HIPAA Privacy Rule,
 - b. **De-identified Data:** Consists of patient data from the Limited Data Set with the following changes:
 - i. Dates of service are algorithmically shifted to protect patient identity.
 - ii. Patient ZIP codes are truncated to the first three digits or removed entirely if the ZIP code represents fewer than 20,000 individuals.
 - c. **Synthetic Data Set:** Consists of data that are computationally derived from a Limited Data Set and that resemble patient information statistically but are not actual patient data.
4. **Data Access Committee (DAC), referred to as the N3C DAC,** NIH Data Access Committees (DACs) review and evaluate (e.g., approve, table, or disapprove) requests from researchers for proposed secondary research uses of controlled-access datasets. NIH DACs are formed based on topic expertise and are not necessarily specific to an Institute, Center, or Office (ICO).
5. **Data Management Incident (DMI)** is defined to include any access to or use of N3C Enclave outside the bounds of an NCATS N3C DAC approved Data Access Request. The term is also inclusive of any violation of the terms and conditions of this Agreement or violations of responsible data use expectations defined within the N3C Enclave’s User Code of Conduct found here: <https://zenodo.org/search?q=n3c&l=list&p=1&s=10&sort=bestmatch>.
6. **Data Contributor** is any Institution that has elected to have their Data included within the N3C Enclave.
7. **Data Security Incident** is a specific kind of Data Management Incident defined to include any access to or use of N3C Data outside the bounds of a DAC-approved Data Access Request. A Data Security Incident may include, but is not limited to, any unauthorized data sharing (e.g. sharing with unapproved users), breach of data security, or inadvertent data releases that may compromise data confidentiality.
8. **Data Access Request (DAR),** previously called a Data Use Request (DUR), is a request submitted to a NIH Data Access Committee for a specific research use specifying the data to which access is sought, the planned research use, and the names of the Approved User(s) and any Collaborators. The Access Request will be signed by the Data Access Requester and their Institutional Signing Official.
9. **Data Access Requester** refers to the individual who prepares Data Access Requests (DARs), Project Renewals, and Project close-outs. To be able to submit a DAR, a Data Access Requester must be a permanent employee of their institution at a level equivalent to, but not limited to, a tenure-track professor or senior researcher; have oversight responsibility for others named on the Data Access Request who will be granted access to the Data; and can be accountable for ensuring that all aspects of data usage align with the terms of the Agreement and institutional policy. Data Access Requesters cannot be post-doctoral fellows, trainees, or lab techs. The Data Access Requester is an individual party to this Agreement with obligations that apply to Approved User conduct, DAR submissions, certifications, and compliance with approved research uses. The Data Access Requester is not responsible for institutional infrastructure, administrative safeguards, or other obligations assigned to the Institutional Requester.
10. **Data Transfer Agreement (DTA)** is a document that permits the transfer of Data from Contributor to the Enclave.
11. **HIPAA Privacy Rule** refers to the Health Insurance Portability and Accountability Act (HIPAA) of 2000, the Health Information Technology for Economic and Clinical Health Act, and all implementing regulations, as may be amended from time to time.

12. **Human Research Protection Program (HRPP)** is defined as the overarching program at the Institutional Requester charged with the responsible oversight of human subject's research and compliance with federal regulations (e.g., the Federal Policy for the Protection of Human Subjects (45 CFR 46)) by Approved User(s) from that Institutional Requester.
13. **Institutional Requester**, previously defined as the Accessing Institution, is the home institution or organization of the Approved User(s) that applies to the NIH controlled-access repository for access to controlled-access data.
14. **Institutional Signing Official**: The label, "Signing Official," refers to the individual that has institutional authority to legally bind the institution in 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 Institutional Signing Official for the Institutional Requester reviews the Data Access Request, Project Renewal, and Project Close-Out applications submitted by the Data Access Requester and legally binds the Institutional Requester to agree to adhere to the terms described in this Agreement.
15. **NCATS National Clinical Cohort Collaborative Enclave "N3C Enclave or Enclave"** is a secure, controlled environment for storage, management, and analysis of data. The underlying architecture, compute resources, and infrastructure used to support the environment may evolve over time to meet future operational and research needs while still preserving the highest standards of data protection and patient privacy.
16. **Progress Update**: Information included with the annual Access Requests renewal or Closeout that summarizes the analysis of controlled-access Data Sets obtained through the Data Access Request, including any publications and presentations derived from the work.
17. **Project Close-out**: Termination of a research project that used Data and confirmation of data destruction when the research is completed and/or discontinued.
18. **Project Renewal**: Renewal of a Data Access Requester's access to Data for a previously approved project.
19. **Research Use Statement** A brief description of the proposed research submitted by the Data Access Requester and reviewed by Data Access Committees to ensure that the research is consistent with the use limitations of the requested dataset.

II. Data Use Terms and Conditions

1. **Research Use**
 - a. For each proposed Research Use Statement, Data Access Requester agree(s) to submit a Data Access Request (DAR) to the NCATS N3C DAC for review and consideration of approval, permitting the Data Access Requester to access the Data.
 - b. DARs must be submitted by a Data Access Requester with certification from the Institutional Signing Official that the Data Access Requester is affiliated with the Institutional Requester and they are permitted to submit a Data Access Request.
 - c. Any changes to the DAR must be approved in writing by the DAC prior to changing access to the Enclave. Minimal changes may be afforded an expedited review. Substantial changes will require submission of a new DAR and will undergo a new review by the Data Contributors and final approval by the DAC. Substantial changes may include, but are not limited to, an update in Phenotype or Research Use Statement.
 - d. Access to Data that is a Limited Dataset is restricted to United States domestic institutions.

- e. A Progress Update will be required for Project Renewals and Project Closeouts and will include the reporting of any publications, presentations and/or intellectual property produced since the last renewal, or if none, since the last Data Access Request.
- f. Approved User(s) are not authorized to download or remove the Data from the Enclave in any form, including screenshots. Research results may be downloaded with the written approval of the NCATS N3C DAC or an N3C download committee. Research results containing reference to <20 participants will not be allowed.
- g. Approved User(s) agree(s) to use the Data exclusively for public health purposes and health-related/biomedical research and consistent with the N3C DAC approved Data Access Request. Any other use of the Data is prohibited.
- h. For projects that involve Approved User(s) from more than one Institutional Requester, each Institutional Requester will be required to have an Agreement in place prior to their Data Access Requester(s) submitting a DAR.
- i. Approved User(s) agree(s) to use the Data in compliance with all applicable federal, state, local, and tribal laws, regulations, and policies. The Approved User(s) agree(s) to adhere to the Institutional Requester's HRPP policies regarding oversight expectations for research with the Data.
- j. Approved User(s) agree(s) to use the Data in compliance with all Enclave policies and guidelines (such as the User Code of Conduct).
- k. Institutional Requester confirms that its Approved User(s) will have completed training in human subject's research protection prior to the approval of a DAR and will remain compliant with training recertification for the duration of a DAR.
- l. If an Approved User(s) leaves the Institutional Requester, the Data Access Requester must notify the N3C DAC. The Approved User's new Institutional Requester must have an active Agreement and be affiliated with the current DAR before the Approved User(s) may continue work on the approved DAR within the Enclave.

2. **Confidentiality**

- a. Approved User(s) of the Enclave will have their identity authenticated, and their research activities shall be regularly audited and tracked for data security.
- b. Approved User(s) agree(s) not to photograph, create screen shots, and/or download the Data viewed on the Enclave.
- c. Approved User(s) agree(s) to not combine Data from separate/different DARs unless permitted by the NCATS N3C DAC.
- d. NCATS encourages the development of new analytical tools, models, diagnostics, therapeutics, or other interventions building on basic discoveries enabled through Data obtained from the Enclave. The Institutional Requester and its Approved User(s) are free to pursue patent protection on any inventions or discoveries developed through their approved use of Enclave.

3. **Dissemination of Research Descriptions, Results and Acknowledgements**

- a. Institutional Requester and Approved User(s) agree(s) to allow the following information in the approved DAR to be made publicly available: non-confidential research statement of the Research Project, Project Title, Approved User(s) names and Institutional Requester.
- b. The workspace and contents, including all research results, subsequent to the DAR's approval will be archived by NCATS. Archival will occur after a Project Closeout or the termination/expiration of this Agreement.

- c. In recognition of the effort that Data Contributor(s) made in collecting and providing the Data, Approved User(s) who post their results, or otherwise publicly present findings, agree(s) to acknowledge the Enclave and Data Contributors as the source of these Data.
- d. In recognition of the Enclave as an NIH-supported research resource, the outputs of any research conducted within the Enclave must be publicly disseminated as outlined in the Enclave's guidelines. For example, as found in the Code of Conduct: "Publicly disseminate findings or new insights into disease etiology, progression, pathobiology, risk or resilience factors, treatment, or prevention based on research conducted using the Enclave, ideally through open access formats. And, as applicable, enable development of new preventive, diagnostic, therapeutic, or other interventions to benefit public health."
- e. In keeping with the NIH's stated commitment to improving the reproducibility and reliability of research findings through effective data sharing, Approved User(s) are expected to share research results, supporting documentation, code, and other knowledge objects generated in the course of conducting the research and irrespective of publication status. Failure to comply may result in termination of DAR(s), Agreement(s), and/or prohibition of access to the Enclave.

4. **Non-Identification**

- a. Approved User(s) agree not to use Data from a DAR, either alone or in concert with any other information, to re-identify or contact individuals from whom data were collected. These provisions do not apply to Data Contributors operating with specific Institutional Review Board (IRB) or equivalent body 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 Approved User(s) conducting "human subjects research" within the scope of 45 CFR 46 must comply with the requirements contained therein.
- b. Approved User(s) agree not to attempt to use the Data to identify or contact any Data Contributors or healthcare providers unless such identification is needed for data preparation and management purposes and only at the request of NCATS or required by law to maintain public health and safety.

5. **Non-Transferability**

- a. The Institutional Requester and Approved User(s) agree to retain control of Enclave Data accessed through the approved DAR and further agree not to distribute this controlled-access data to any entity or individual not identified in the submitted request.
- b. The Institutional Requester and Data Access Requester acknowledge responsibility for ensuring review of and compliance with the terms of this Agreement that apply to them and acknowledge responsibility for the appropriate research use of controlled-access data obtained through the Data Access Request, subject to applicable laws and regulations. Institutional Requester and Data Access Requester agree that controlled-access data obtained through the Data Access Request, in whole or in part, may not be sold to any individual at any point in time for any purpose.
- c. Institutional Requester must have policies and procedures to ensure that Data Access Requester(s) complete the Project Close-out process (See Termination and Data Destruction Provision) before moving to a new institution. If a Data Access Requester(s) moves to a new institution without completing the Project Close-out process, Institutional Requester must immediately notify the N3C DAC. A new Data Access Request, in which the new Institutional

Requester and Data Access Requester agree to the Data Use Agreement, must be approved by the N3C DAC before controlled-access data may be re-accessed by Approved User(s).

6. **Certificate of Confidentiality**

- a. Certificates of Confidentiality (Certificate) protect the privacy of research participants by prohibiting disclosure of protected information for non-research purposes to anyone not connected with the research except in specific situations. Data that are stored in and shared through the NIH data repositories accessed under this agreement are protected by a Certificate. Therefore, Institutional Requester and Approved User(s), whether or not funded by the NIH, who are approved to access a copy of information protected by a Certificate, are also subject to the requirements of the Certificate of Confidentiality and subsection 301(d) of the Public Health Service Act (<https://www.govinfo.gov/content/pkg/COMPS-8773/pdf/COMPS-8773.pdf>).
- b. 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:
 - i. 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
 - ii. 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.
- c. Disclosure is permitted only when:
 - i. 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.
 - ii. Necessary for the medical treatment of the individual to whom the information, document, or biospecimen pertains and made with the consent of such individual.
 - iii. Made with the consent of the individual to whom the information, document, or biospecimen pertains; or
 - iv. Made for the purposes of other scientific research that is following applicable Federal regulations governing the protection of human subjects in research.
- d. For more information see: *Certificates of Confidentiality (CoC) | Grants & Funding* (<https://grants.nih.gov/policy-and-compliance/policy-topics/human-subjects/coc>).

7. **Data Security and Access Violations**

- a. The Institutional Requester and Approved Users agree to manage the Data according to the “NIH Security Best Practices for Users of Controlled-Access Data” and acknowledge that when Data are maintained in the Enclave, the data are secured according to NIH’s expectation.
- b. Approved User(s) will not share their Enclave log-in credentials with others at any time and must keep all log-in information credentials protected from unauthorized access
- c. Institutional Requester and Approved User(s) agree to establish appropriate administrative, technical, and physical safeguards to prevent unauthorized use of or access to the Data and

- comply with any other special requirements. The Institutional Requester and Approved User(s) must complete appropriate required NIH IT training, relating to safeguarding of the Data as may be set forth in the NIH website <https://irtsectraining.nih.gov/public.aspx>. Note that NCATS may request evidence of completion of the NIH IT training from Approved User(s) (*i.e.*, a copy of the Certificate of Completion provided at the end of the course).
- d. Failure to comply with the Enclave's User Code of Conduct by Institutional Requester and/or Approved User(s) may result in a suspension of access to the Data for **ALL** Approved User(s) until NCATS completes an investigation into the specific Data Management Incidents. After this time, NCATS, at its sole discretion, may either reinstate or terminate, in whole or in part, Approved User(s)'s access to the Data.
 - e. The Institutional Requester and Approved User(s) acknowledge that NIH may terminate the Data Access Request, including this Agreement, and immediately revoke or suspend access to the Enclave and/or all Data at any time if the Institutional Requester and/or Approved User(s) is found to be no longer in compliance with the terms described in this Agreement, or the policies, principles, and procedures of NIH.
 - f. The Institutional Requester and Approved User(s) agree(s) to notify the, NIH DAC(s) on the project request, and NIH Data Management Incident Notification inbox of any terms of access violations or unauthorized data sharing, breaches of data security, or inadvertent data releases that may compromise data confidentiality within twenty-four (24) hours of when the incident is identified. NIH Incident Response Team must be included in notifications relating to Data Security Incidents. For the NIH Incident Response Team, notifications can be made by phone (301) 496-HELP (4357); Toll Free Number: (866) 319-4357 or TTY: (301) 496-8294 and can also be sent by email to NIHInfoSec@nih.gov. For the NIH Data Management Incident Notification inbox, email DMI_OER@mail.nih.gov. For notifications to the NIH DAC which approved the project request and the NCATS N3C team, please use ncatsn3cdac@mail.nih.gov and NCATSDataAccessIncidents@nih.gov
 - g. Unless prohibited 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 three (3) business days of the notification, the Institutional Requester agrees to submit to the NIH DAC(s) on the project request and the NIH Data Management Incident Notification inbox 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 future incidents, including specific information on timelines anticipated for action. The Institutional Requester agrees to provide documentation verifying that the remediation plans have been implemented. Repeated violations or unresponsiveness to NIH requests may result in further compliance measures affecting the Institutional Requester and the Approved User(s).
 - h. NIH, or another entity designated by NIH may, as permitted by law, also investigate any data security incident or policy violation. The Institutional Requester and Approved User(s) and their associates agree to support such investigations and provide information, within the limits of applicable local, state, Tribal, and federal laws and regulations. In addition, Institutional Requester and Approved User(s) agree to work with NIH to assure that plans and procedures that are developed to address identified problems are mutually acceptable and consistent with applicable law.
 - i. NIH may apply for injunctive or other equitable relief before courts of competent jurisdiction as remedy for breach of the Agreement, in addition to all other remedies available at law or in equity.

8. Liability

- a. Approved User(s) will retain ownership rights in any derivative work developed through the use of the Data. Data Contributors shall retain ownership of any rights they may have to the Data.
- b. Approved User(s) creating an Enclave workspace(s) are expected to ensure that external data, files, or software that they import into the Enclave are conducted in accordance with all applicable national, tribal, and state laws and regulations as well as relevant institutional policies, procedures and agreements. NCATS assumes no responsibility and/or liability regarding any imported data, files, or software.
- c. NCATS must pre-approve all external data, files, and/or software that will be imported by the Approved User(s) into the Enclave. The Approved User(s) may only import external data, files, or software after NCATS provides written approval. Such data may be shared with other DARs as indicated by the Approved User(s) importing the data. NCATS has the right to remove all external data, files, or software from the Approved User(s)'s Enclave workspace at any time and without notice, even if approval was previously granted.
- d. The Institutional Requester and the Approved User(s) acknowledge that although all reasonable efforts have been made to ensure the accuracy and reliability of controlled-access data accessed through the request, the NIH and Data Contributors do not and cannot warrant the accuracy of results that may be obtained by using any Data included therein. NIH and all Data Contributors to these datasets disclaim all warranties as to performance or fitness of the Data for any particular purpose.
- e. 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 because 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.*

9. Termination and Data Destruction

- a. This Agreement may be immediately terminated by mutual written agreement between the Parties. Any Party can terminate this Agreement without cause by providing thirty (30) days written notice to the other Parties. Upon termination, all access for Approved User(s) from the Institutional Requester will be terminated.
- b. Upon Project Close-out, all Approved User(s)'s access to the DAR's workspace will be promptly removed. Workspaces will be retained and not destroyed for a period of 12 months from the Project close out. Extensions to the destruction timeline can be requested by a Data Access Requester or Institutional Signing Official. Access to DARs can be restored following appropriate N3C procedures.
- c. Approved Users agree to use research results downloaded from N3C consistent with the approved DAR, even after Project Close-out.
- d. This Agreement shall be effective as of the date on which it is signed by the last of the Parties. This Agreement shall remain in effect for as long as the DAR it supports is active. Each DAR will have a one (1) year term and be eligible for two (2) additional 1-year term renewals. All legal notices related to this Agreement will be sent to the below listed contact information.
- e. The following terms and conditions of the Agreement, 1g, 1i, 1l, 3, 4, 5, and 6 in their entirety, 7h, 7i, 8a, 8d, 8e, and 9c will survive expiration or termination of this Agreement.

AGREED AND ACCEPTED by the Parties

By signing below, the Institutional Signing Official represents that they are authorized to bind the Institutional Requester, and that the Institutional Requester agrees to the terms of this agreement and to all obligations assigned to it under this Agreement. Additionally, the Institutional Signing Official certifies that the Data Access Requester is affiliated with the institution.

Institutional Requester: _____

Institutional Signing Official Name: _____

Institutional Signing Official Title: _____

Institutional Requester Address: _____

Signature: _____ Date: _____

Legal Notice Contact (email): _____

Email of Institutional Signing Official: _____

By signing below, I acknowledge that I understand the obligations assigned to the role of Data Access Requester in this Agreement, as distinct from the obligations of the Institutional Requester, and I agree to comply with the Data Access Requester obligations in this Agreement. I do not sign on behalf of the Institutional Requester and do not assume obligations assigned to the Institutional Requester.

Data Access Requester Name: _____

Data Access Requester Title: _____

Data Access Requester Address: _____

Signature: _____ Date: _____

Email of Data Access Requester: _____

For: National Center for Advancing Translational Sciences (NCATS)

Name: Krishna Balakrishnan M.B.A. Ph.D.

Title: Director, Office of Strategic Alliances (OSA)

Signature: _____ Date: _____

Email for Legal Notices: NCATSPartnerships@mail.nih.gov