

FaceBase Data Use Certification Agreement

Agreement pertaining to FaceBase datasets containing data from human subjects

INTRODUCTION AND STATEMENT OF POLICY

FaceBase is a central repository for data generated by the FaceBase Consortium as well as data offered for inclusion by other investigators working on similar projects. Both the FaceBase database and the Consortium are funded by the National Institute of Dental and Craniofacial Research (NIDCR) of the National Institutes of Health (NIH). Implicit in the establishment of the FaceBase data repository is the idea that scientific progress in understanding craniofacial development and disorders of that process will be greatly enhanced if the data produced by the Consortium's studies are readily available to investigators in the wider research community.

Because the volume of human genomic and phenotypic data contained in this repository is substantial and, in some instances, potentially sensitive (e.g., data related to the presence or risk of developing particular diseases or conditions 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 and/or phenotypic 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 expectation of the NIH, the NIDCR and the FaceBase Consortium that approved users of FaceBase-provided datasets adhere to any restrictions on data use delineated within the original informed consent agreements of the contributing studies, as established by the institution that contributed the dataset and as stated on the FaceBase website.

Definitions of terminology used in this document are found in the Appendix.

The parties to this agreement include: the Principal Investigator (PI) granted access to the FaceBase dataset (an "Approved User"), the PI's home institution as represented by its Institutional Signing Official (the "Requester"), the FaceBase Consortium as represented by its Data Access Committee (the FaceBase DAC), and the NIDCR/NIH. The effective date of this agreement shall be the Project Approval Date, as specified on the Data Access Committee (DAC) approval notification.

TERMS OF ACCESS

1. Research Use

The Requester agrees that if access is approved, the following personnel shall become Approved Users of the requested dataset(s):

- (1) the Principal Investigator named in the Data Access Request (DAR) and

(2) those named as Collaborators in the DAR, including the Information Technology Director and any trainee, employee, or contractor¹ working on the proposed research project under the direct oversight of these individuals. Research use will occur solely in connection with the approved research project described in the DAR, which includes a description of the research objectives and design. 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. 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). The applicant will be required to demonstrate institutional approval for the modified project. Access to the requested dataset(s) is granted for a period of 1 year as defined below. Access to the dataset beyond the end of this one-year period can be obtained through resubmission of the DAR.

Each FaceBase dataset has specific use limitations, which can be found at www.facebase.org. The research project described in the DAR must be consistent with these limitations.

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

Through submission of the DAR, the PI agrees to submit either a request for renewal of access to the dataset(s) (section 10, below) or a final report (section 11, below) to the FaceBase Data Access Committee (DAC) two weeks prior to the expiration date of the 1-year data access period. Failure to submit a renewal or to complete the close-out process, including confirmation of data destruction by the Institutional Signing Official, may result in termination of all current data access and/or suspension of the PI and all associated

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 appropriate terms in any contract agreement to ensure that any of the contractor's employees who have access to the data adhere to the NIH 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.

personnel and collaborators from submitting new DARs for a period to be determined by NIH. Repeated violations or unresponsiveness to NIH requests may result in further compliance measures affecting the Requester.

Some FaceBase datasets contain information that could potentially be linked to the research participants (e.g. 3D mesh images derived from facial photographs). Any dataset which could lead to identification of the participant is considered to be human subjects research. Access to any FaceBase dataset requires prior review and approval of the project by the Requester's IRB. By approving and submitting the attached DAR, the Institutional Signing Official provides assurance that relevant institutional policies and national, tribal, and state laws and regulations, as applicable, have been followed, including IRB approval. The Institutional Signing Official also assures through approval of the DAR that other institutional departments with relevant authorities (e.g., those overseeing human subjects research, information technology, or technology transfer) have reviewed the relevant sections of the NIH GDS Policy and the associated procedures and are in agreement with the principles defined.

In some cases, NIH anticipates that FaceBase datasets will be updated with 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 if he or she becomes an Approved User, information about the PI and the approved research use will be posted publicly on the FaceBase website, as well as a public, U.S. government website that describes approved research projects. The information may include the Approved User's name and institution, project name, and Specific Aims as described in the DAR. Citations of publications resulting from the use of FaceBase datasets obtained through this DAR may also be posted on the FaceBase and relevant NIDCR websites.

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 (including facial images) and/or samples were collected. All investigators conducting "human subjects research" within the scope of 45 CFR 46 must comply with the requirements contained therein.

5. Non-transferability

The Requester and Approved Users agree to retain control of FaceBase datasets obtained through the attached DAR and any derivatives² of FaceBase datasets and further agree not to distribute FaceBase datasets and derivatives of FaceBase datasets to any entity or individual not identified in the submitted DAR. If Approved Users are provided access to FaceBase datasets subject to the GDS Policy for inter-institutional collaborative research described in the Specific Aims and Analysis Plan sections of the DAR, and all members of

² Any data containing individual-level information that are generated or inferred from controlled-access datasets (e.g. imputed or annotated data) obtained from NIH-designated data repositories (e.g., dbGaP).

the collaboration are also Approved Users through their home institution(s), data obtained through the attached 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 GDS Policy](#) and the Requester's IT security requirements and policies, for raw data as well as derived data, including any transmission of the data.

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

PIs agree 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 FaceBase DAC before FaceBase data may be re-accessed. As part of the close-out process, all copies and versions of the datasets retrieved from NIH-designated controlled-access databases as well as any derivatives of FaceBase datasets stored at the institution must be destroyed and destruction confirmed by the Institutional Signing Official, as described below. However, a written request may be submitted to the FaceBase Data Access Committee to transfer responsibility for the approved research project to another Approved User within the original institution. The FaceBase DAC will make a determination on a case-by-case basis (see section 12).

6. Data Security and Data Release Reporting

FaceBase has adopted the data security and data release reporting procedures developed by the NIH for dbGaP. The Requester and Approved Users, including the institutional IT Director, acknowledge NIH's expectation that they have reviewed and agree to manage the requested FaceBase dataset(s) and any derivatives of FaceBase datasets 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 FaceBase data entrusted to the Requester. These include, but are not limited to:

- all Approved Users have completed all required computer security training required by their institution, for example, the <https://irtsectraining.nih.gov/publicUser.aspx>, or the equivalent;
- the data will always be physically secured (for example, through camera surveillance, locks on doors/computers, security guard);
- servers must not be accessible directly from the internet (for example, they must be behind a firewall or not connected to a larger network), and unnecessary services should be disabled;
- use of portable media, e.g., on a CD, flash drive or laptop, is discouraged, but if necessary then they should be encrypted consistent with applicable law;
- use of up to date anti-virus/anti-spyware software;

- security auditing/intrusion detection software, detection and regular scans of potential data intrusions;
- use of strong password policies for file access; and
- all copies of the dataset should be destroyed, as permitted by law, whenever any of the following occurs:
 - the DUC expires, and renewal is not sought;
 - access renewal is not granted;
 - the FaceBase Consortium, the NIDCR or the NIH requests destruction of the dataset; or
 - the continued use of the data would no longer be consistent with the DUC.

In addition, the Requester and Approved Users agree to keep the data secure and confidential at all times and to adhere to information technology best practices in all aspects of data management to assure that only authorized individuals can gain access to FaceBase datasets. This agreement includes the maintenance of appropriate control over any copies or derivatives of the data obtained through the Data Access Request.

Requesters and PIs agree to notify the FaceBase 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 FaceBase DAC notification, the Requester, through the PI and the Institutional Signing Official, agree to submit to the FaceBase 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:
 FaceBase Data Access Committee
 URGENT email: nidcrufacedac@mail.nih.gov

NIDCR, 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, in the case of a breach of data security or unintended data release, Requesters and Approved Users agree to work with the NIDCR and NIH to assure that plans and procedures that are developed to address identified problems are mutually acceptable and consistent with applicable law.

7. Intellectual Property

The FaceBase Consortium follows the intellectual property principles developed by the NIH. By requesting access to FaceBase 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 FaceBase data repository. Following the NIH principles, the FaceBase Consortium encourages broad use of NIH-supported genotype and 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 FaceBase Consortium considers these data as pre-competitive and urges Approved Users to avoid making IP claims derived directly from the FaceBase dataset(s). These FaceBase-provided data, and conclusions derived therefrom, will remain freely available, without requirement for licensing. However, the FaceBase Consortium 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.

8. Research Dissemination and Acknowledgement of Controlled-Access Datasets Subject to the GDS Policy

It is the intent of the FaceBase Consortium and NIDCR to promote the dissemination of research findings from FaceBase 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.

Images of individuals derived from 3D facial photography (e.g., 3D or 2.5D mesh images) are comparable to a full facial photograph and are therefore considered an individual identifier under the HIPAA rules (45 CFR 164.514). Therefore, derived images from any individual included in a dataset obtained from FaceBase must not be used in publications or presentations. The publication of composite (e.g., averaged) facial images is permitted.

Publications, written and oral presentations, and disclosures describing the results of research conducted using FaceBase datasets should cite the FaceBase dataset accession number and must acknowledge the individual FaceBase project(s) that generated the data, the FaceBase Data Management Hub, and the FaceBase Consortium. They should also acknowledge any relevant FaceBase Consortium publications describing the creation of the dataset, which will be posted on the FaceBase website (www.facebase.org) when they are available. Public acknowledgements should also credit the NIDCR as the source of FaceBase funding.

Sample statements for the acknowledgement of FaceBase datasets follow:

Morphometric data from normal faces (FB00000491, FB00000892, FB00000667) were obtained from FaceBase (www.facebase.org) and were generated by projects U01DE020078 and U01DE020054. The FaceBase Data Management Hub (U01DE024449) and the FaceBase Consortium are funded by the National Institute of Dental and Craniofacial Research.

Genomic data for individuals with cleft lip and/or cleft palate (FB00000345) were obtained from FaceBase (www.facebase.org) and were generated by project

U01DE020073. The FaceBase Data Management Hub (U01DE024449) and the FaceBase Consortium are funded by the National Institute of Dental and Craniofacial Research.

9. Departures from the Previously Approved Research Plan

To assure that FaceBase and NIH policies and procedures for human subjects data use are adhered to, any departure from the project described in the original DAR must be reported to the FaceBase DAC prior to implementation. Such reports must demonstrate that appropriate institutional approvals for the revisions have been obtained by the Approved Users, and that the project's aims remain consistent with any data use limitations for the approved datasets. This includes changes in the project's Collaborators.

10. Renewal of Dataset Access

Approval of access to FaceBase datasets will be for one year at a time. Principal Investigators, through their Institutional Signing Official, can request continued access to FaceBase datasets by submitting a renewal request to the FaceBase DAC at least two weeks prior to the anniversary of the Project Approval Date specified on the Data Access Committee approval notification (<https://www.facebase.org/odocs/human-data-access-request-renewal>). The renewal application will describe how these data have been used during the previous year, any results that have been generated as a result of access to the data, including patents and publications, and any proposed departures from the originally proposed research plan. Renewal requests should also provide evidence of review of the renewal request by the IRB at the Approved User's institution.

This information will be used by the FaceBase Data Access Committee and NIDCR staff for program evaluation activities and may be considered by the NIDCR as part of the NIH effort to provide ongoing oversight and management of all NIH data sharing activities.

Renewal Requests should be submitted by e-mail to:

nidcrfacebasedac@mail.nih.gov

11. Final Reporting at Termination of Dataset Access

Principal Investigators not seeking renewal agree to provide the FaceBase DAC, through their Institutional Signing Official, a Final Report no later than one month after the end of the anniversary of the Project Approval Date (<https://www.facebase.org/odocs/human-data-access-final-report>). This report will provide information regarding potentially significant findings and publications or presentations that resulted from the use of the requested dataset(s), any violations of the terms of access described within this Data Use Certification and the implemented remediation, and information on any downstream intellectual property generated as a result of the data. This Final report should either confirm that the Approved Users' copies of the FaceBase dataset(s) have been destroyed in accordance with this document or explain why the conditions for retention of the dataset(s) described in Section 12 (below) pertain. If the conditions for retention described in Section 12 do pertain, the Final Report should address when the dataset(s) will be destroyed and arrangements for secure storage of the dataset(s) during the interim period.

This information will be used by the FaceBase Data Access Committee and NIDCR staff for program evaluation activities and may be considered by the NIDCR as part of the NIH effort to provide ongoing oversight and management of all NIH data sharing activities.

Final Reports should be submitted by e-mail to:

nidcrfacebasedac@mail.nih.gov

12. Final Disposition of Dataset(s)

At the end of the approved access period, Approved Users agree to destroy all copies of the requested dataset(s), except as required by publication practices, institutional requirements, or law to retain them. The FaceBase DAC will inform the Approved Users' Institutional Signing Official of the expiration/termination of the Approved Users' access to the FaceBase dataset(s) and of the need to destroy all copies of the dataset(s) provided to the previously Approved Users.

Copies of FaceBase dataset(s) may not need to be destroyed if, with advance notice and approval by the FaceBase Data Access Committee, the project has been transferred to another Approved User at the same institution. In this case, documentation must be provided that other Approved Users are using the dataset(s) under an active FaceBase DAC approved research project.

13. Non-Endorsement, Indemnification

The Requester and Approved Users acknowledge that although all reasonable efforts have been taken to ensure the accuracy and reliability of the FaceBase data obtained through the attached DAR, FaceBase Consortium, the NIDCR, the NIH, the FaceBase Data Access Committee, and Contributing Investigators do not and cannot warrant the results that may be obtained by using any data included therein. The NIDCR, NIH, the FaceBase Data Access Committee 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.

14. Termination and Violations

Upon project close-out, all Approved Users agree to destroy all copies, versions, and derivations of the dataset(s) retrieved from NIH-designated controlled-access databases, on both local servers and hardware, virtual and physical machines, databases, and random-access archives, except as required by publication practices, institutional policies, or law to retain them.

The Requester and PI acknowledge that the NIH or the NIDCR, or the FaceBase Consortium may terminate this agreement and immediately revoke access to all FaceBase datasets subject to the GDS Policy at any time if the Requester is found to be no longer in

agreement with the policies, principles and procedures of the NIH, the NIDCR, and the FaceBase Consortium.

By submission of the attached Data Access Request, the Requester through the Institutional Signing Official attests to the Approved Users' qualifications for access to and use of FaceBase dataset(s) and certifies their agreement to the FaceBase and NIH principles, policies, and procedures for the use of the requested datasets as articulated in this document, including the potential termination of access should a violation of any of these agreement terms be identified.

Requesters and the Principal Investigator further acknowledge that they have shared this document and the FaceBase data sharing policies and procedures for access and use of FaceBase datasets with any Approved Users, appropriate research staff, and all other Collaborators identified in the DAR.

The Institutional Signing Official acknowledges that they have considered the relevant FaceBase policies and procedures, that they have shared this document and the relevant policies and procedures with appropriate institutional organizations and have assured compliance with local institutional policies related to technology transfer, information technology, privacy, and human subjects research.

Information Technology (IT) Director:

Printed Name

Position at Institution

Signature

Date

Principal Investigator:

Printed Name

Position at Institution

Signature

Date

Institutional Signing Official:

Printed Name

Position at Institution

Signature

Date

APPENDIX

DEFINITIONS

Approved User: A user approved by the FaceBase Data Access Committee 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 FaceBase data. 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 FaceBase data.

Contributing Investigator: An investigator who submitted a genomic dataset to FaceBase.

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 Use Certification Agreement (DUC): An agreement between the Approved Users, the Requester, and NIH regarding the terms associated with access of controlled-access datasets subject to the GDS Policy and the expectations for use of these 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 GDS Policy](#) and the institution's IT security requirements and policies are followed by the Approved Users.

Institutional Signing Official: The Signing Official has institutional authority to legally bind the institution in grants administration matters. The label, "Signing Official," is used in conjunction with the [NIH eRA Commons](#). An Institutional Signing Official in Commons is the equivalent of an Authorized Organizational Representative. The individual fulfilling this role may have any number of titles in the grantee organization but is typically located in its Office of Sponsored Research or equivalent. The Signing Official reviews Data Access Request, Renewal, and Close-out applications submitted by Principal Investigators and on behalf of the institution, agrees to adhere to the terms described in the Data Use Certification Agreement if the application is submitted to NIH.

Project Close-out: Termination of approved access to FaceBase data and confirmation of data destruction when the research is completed and/or discontinued.

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