Federal Interagency Traumatic Brain Injury Research (FITBIR)

National Trauma Research Repository (NTRR)

Data Access Request

Contents

Informatics System Data Access Request

From here on, the Federal Interagency Traumatic Brain Injury Research (FITBIR) and the National Trauma Research Repository (NTRR) will collectively be referred to as "the Informatics System." The Data Access Committee (DAC) approves access to data and/or images from the Informatics System for research purposes. The DAC will review the Informatics System Data Access Request (DAR) of each applicant requesting data and provide access based on the expectations outlined in the Informatics System policy.

These expectations include the protection of data privacy, confidentiality, and security. In the event that requests raise concerns related to privacy and confidentiality, risks to populations or groups, or other concerns, the DAC will consult with other experts as appropriate.

Recipients seeking access to data or images from the Informatics System are expected to submit their DAR, signed by the Data Access Requester and the Institutional Signing Official. Completing this DAR is a necessary step to access data or images from the Informatics System.

Steps to Request Query Access to the Informatics System

1. Read the Data Use Agreement for the Informatics System below.

2. Identify individuals from your institution to serve as:
   - Data Access Requester
   - Institutional Signing Official (SO)

   Note: ***The Institutional Signing Official CANNOT also serve as the Data Access Requester***
   Both the Data Access Requester and Institutional Signing Official must provide an email address affiliated with their same self-identified institution or corporation (NO personal email addresses will be accepted, e.g., Gmail).
   Any request submitted with a public-domain email address will be rejected.

3. Complete the Recipient Information and Certifications page and digitally sign it using a digital certificate. The signed document should be uploaded when requesting an account.

4. Request an account by using the Research Auth Service (RAS) for single-sign on. Detailed instructions are available here: FITBIR: https://fitbir.nih.gov/access-with-ras or NTRR: https://ntrr.nih.gov/access-with-ras. When creating an account, request privileges to access data (with Query and Study privileges) at FITBIR: https://fitbir.nih.gov/ or NTRR: https://ntrr.nih.gov/.

5. Access Request Review: The DAC will review requests to access the Informatics System. Such reviews are generally completed within 15-20 business days.

6. The DAC will notify the Operations staff if the access request has been approved. Users will receive an automated notification confirming their account access has been granted or updated.

7. Optional: Informatics System Training (if request is approved): Contact Operations through FITBIR: FITBIR-ops@mail.nih.gov or NTRR: NTRR-ops@list.nih.gov to discuss specific training needs the user may have and schedule the training.

Data Use Agreement for the Informatics System

Introduction

The Department of Defense (DoD), the Department of Veteran Affairs (VA), and the National Institutes of Health (NIH) have developed an informatics system to store the collection of data from participants in traumatic brain injury (TBI) and general trauma research studies, regardless of the source of funding. The extensive information collected by these studies, and subsequently stored in the Informatics System, provides a rare and valuable scientific resource. Promoting optimal use on a national scale of this resource will require a large and concerted effort, which may exceed the research capacity of current investigators. The DoD, VA, and NIH have a responsibility to the public in general, and to the scientific community in particular, to encourage the use of these resources to achieve rapid scientific progress. In order to take full advantage of such resources and maximize their research value, it is important that data be made available, on appropriate terms and conditions, to the largest possible number of qualified investigators in a timely manner.

Data collected by the Submitters have been stripped of all individual identifiers, but the unique and intrinsically personal nature of DNA, derivative data of which are included in the Informatics System, combined with the recent increase in the accessibility of conducting genotype and other sequence analyses (in terms of technological capacity and cost), has altered the framework through which "identify-ability" can be defined. To protect and assure the confidentiality and privacy of all participants, the Recipient who is granted access to these data is expected to adhere to the specifications of this DUC. Failure to do so could result in the denial of further access to data and subject the Recipient to any other applicable penalties and actions.

Submitters have significantly contributed to the Informatics System by consistently providing valuable data over the long term. The DoD, VA, and NIH seek to encourage appropriate data use and collaborative relationships by outside investigators with the Submitters and to ensure that the contribution of the Submitters is appropriately acknowledged.

Definitions

For purposes of this agreement:

Approved Data User/Recipient (Recipient): A user approved by the relevant Data Access Committee to access one or more datasets for a specified period and only for the purposes outlined in the Data Access Requester's approved Research Use Statement. Any staff members and trainees under the direct supervision of the Data Access Requester are also Approved Data Users/Recipients and must abide by the terms laid out in the Data Use Agreement.

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 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 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. If the Data Access Requester plans to collaborate with investigators outside of their Requesting institution, then **each external collaborator must submit a separate DAR with the exact title and wording as the Data Access Requester** and be approved by the DAC.

Data: Refers to the information that has been collected and recorded from participants in TBI and/or trauma studies, regardless of the source of funding. Data from study participants were collected through the periodic examinations and follow-up contacts conducted pursuant to the Submitters' Cooperative Agreement grants, other grants, contracts, and other TBI or trauma studies conducted independent of the DoD, VA, or NIH.

Data Access Committee (DAC): Data Access Committee (DAC) review and approve, or disapprove, requests from extramural and intramural researchers for proposed secondary research uses of controlled-access datasets. The DAC is formed based on topic expertise and is not necessarily specific to an Institute, Center, or Office (ICO).

Data Access Request (DAR): A request submitted to the Data Access Committee for a specific research use specifying the data repository to which access is sought, the planned research use, and the names of collaborators. The DAR also constitutes an agreement between the Approved Data User/Recipient, the Institutional Requester, and NIH regarding the terms associated with access to controlled-access datasets and the expectations for use of these datasets. The DAR is digitally signed by the Data Access Requester requesting the data and their Institutional Signing Official.

Data Access Requester: 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. **Data Access Requesters cannot be post-doctoral fellows, trainees, or lab technicians.**
- Have oversight responsibility for others named on the data access request who will be granted access to the data.
- Can be accountable for ensuring that all aspects of data usage align with the terms of the DAR and institutional policy.
- Have an institutional email (no public emails will be accepted, e.g., Gmail).

Institutional Requester: The home institution or organization of the Approved Data User/Recipient that applies to the NIH controlled-access repository for access to controlled-access data.

Institutional Signing Official (SO): The label, “Signing Official,” refers to the individual who 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 Institutional Signing Official for the Institutional Requester reviews Access Request, Project Renewal, and Project Close-out applications submitted by investigators and legally binds the Institutional 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 the Data Use Agreement and signs on behalf of the Data Recipients. The label "Signing Official" is used in conjunction with the eRA Commons. If you are unable to identify your SO, contact the NIH eRA Commons Service Desk.

Note: SO’s MUST provide an email from the same institution as the Data Access Requester

Progress Update: Information included with the annual Access Requests renewal or Closeout summarizing the analysis of controlled-access datasets obtained through the Access Request, any publications and presentations derived from the work.

Project Close-out: Termination of a research project that used controlled-access data from an NIH controlled-access repository and confirmation of data destruction when the research is completed and/or discontinued.

Project Renewal: Renewal of a Data Access Requester’s access to controlled-access datasets for a previously approved project.

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**.**

Submitter: Defined as a researcher who has submitted data to the Informatics System, according to the policies laid out in the Informatics System Submission Agreement. The Submitter may have had a past or current/active grant, contract, or consulting agreement with the DoD, VA, or NIH, one of its contractors, or any other funding source.

Terms of Agreement

Data from active and completed studies are eligible for restricted "Controlled Access" by qualified researchers pursuant to the terms set forth in this agreement.

I request approval to access these data and/or images from the Informatics System for research purposes. I agree to the following terms:

Research Project: Received data will be used solely in connection with the "Project Summary/Abstract." If the Project does involve Submitter(s), their names and the work they will perform are also included in the Recipient Information and Certifications section.

This DAR covers only the Research Project contemplated in the Project Summary/Abstract section. The approved data recipient(s) agree that data will not be used in any research not disclosed and approved as part of the Research Project. The Data Access Requester will submit a completed DAR (this document) for each research project for which data are requested. This applies to all versions of the Informatics System data.

Non-identification: Approved Data Recipients agree not to use controlled access data sets obtained through the DAR, either alone or in concert with any other information, to identify or contact individual participants from whom data and/or samples were collected.

Recipient agrees to notify Operations as soon as possible if, upon use of the Informatics System data, the Recipient discovers identifying information in those data.

These provisions do not apply to original data submitters 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 Data Recipients conducting "human subjects research" within the scope of 45 CFR 46 must comply with the requirements contained therein.

Certificate of Confidentiality: 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 are protected by a Certificate. Therefore, Approved Data Recipients(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.

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 following applicable Federal regulations governing the protection of human subjects in research.

For more information, see: *Certificates of Confidentiality (CoC) | Grants & Funding*.

GUID and Access to Submitted Data: The Global Unique Identifier (GUID) is a computer-generated alphanumeric code that is unique to each research participant. GUID allows the Informatics System to link together all submitted information on a single participant, giving researchers access to information even if the data were collected at different locations or through different studies. If Recipients request access to data on individuals for whom they themselves have previously submitted data to the Informatics System, they may gain access to more data about an individual participant than they themselves collected. Consequently, these research activities may be considered “human subjects research” and may require that they obtain institutional IRB approval of their Research Project.

Non-Transferability: The Institutional Requester and Approved Data Users/Recipients agree to retain control of NIH controlled-access datasets accessed through the request and further agree not to distribute controlled-access data to any entity or individual not identified in the submitted request. If the Approved Data Users/Recipients are provided access to controlled-access datasets for inter-institutional collaborative research described in the Research Use Statement of the Data Access Request, and all members of the collaboration are also Approved Data Users/Recipients through their home institution(s), data obtained through the Data Access Request may be securely transmitted within the collaborative group. Each Approved Data User/Recipient will follow all data security practices and other terms of use defined in this Agreement and the Institutional Requester’s IT security requirements and policies.

The Institutional Requester and Approved Data Users/Recipients acknowledge responsibility for ensuring the review and agreement to the terms within this Agreement and the appropriate research use of controlled-access data obtained through the Data Access Request, subject to applicable laws and regulations. Institutional Requester and Approved Data Users/Recipients 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.

Institutional Requester must have policies and procedures to ensure that Approved Data Users/Recipients complete the Project Close-out process (See Termination and Data Destruction Provision) before moving to a new institution. If an Approved Data User/Recipient moves to a new institution without completing the Project Close-out process, Institutional Requester must immediately notify the relevant DAC. A new Data Access Request, in which the new Institutional Requester agrees to the Data Use Agreement, must be approved by the relevant DAC before controlled-access data may be re-accessed.

The Institutional Requester and Approved Data Users/Recipients agree that any substantive changes made to the Research Project require execution and approval of a new DAR, in which the new Research Project is described. If the Recipient appoints another Principal Investigator to complete the Research Project, a new DAR in which the new Recipient is designated is necessary.

Data Security and Unauthorized Data Release: Recipient acknowledges the expectations set forth by the attached "Information Security Best Practices" for the use and security of data.

The Institutional Requester agrees that the Institutional Requester's IT security requirements and policies are sufficient to protect the confidentiality and integrity of the NIH controlled-access data entrusted to the Institutional Requester.

The Institutional Requester and Approved Data User/Recipient agree to notify the NIH Incident Response Team, DAC on the project request, and NIH Office of Extramural Research Data Sharing Policy Implementation (OER/DSPI) Team 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. For the NIH Incident Response Team, notifications can be made by phone (301) 496-HELP (4357); Toll Free Number: (866) 319-4357or TTY: (301) 496-8294, and can also be sent by email to NIHInfoSec@nih.gov or via the Report an Incident Link: https://irtportal.ocio.nih.gov/. For OER/DSPI Team, notifications can be sent to DMI_OER@mail.nih.gov.

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 notification, the Institutional Requester agrees to submit to the DAC on the project request and the OER/DSPI Team 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 Data User/ Recipient(s).

NIH, or another entity designated by NIH may, as permitted by law, also investigate any data security incident or policy violation. Approved Data Users/Recipients 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 Data Users/Recipients 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.

Terms of Access Violations: The Institutional Requester and Approved Data Users/Recipients acknowledge that NIH may terminate the Data Access Request, including this Agreement and immediately revoke or suspend access to all controlled-access datasets at any time if the Institutional Requester and/or Approved Data User/Recipient is found to be no longer in agreement with the terms described in this Agreement, the policies, principles, and procedures of NIH.

The Institutional Requester and Approved Data User/Recipient(s) agree to notify the OER/DSPI Team, and the DAC indicated in the project request to this Agreement, of any terms of access violations, hereinafter referred to as data management incidents (DMIs), within 24 hours of when the incident is identified. For OER/DSPI Team, notifications can be sent to DMI_OER@mail.nih.gov. 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 notification(s), the Institutional Requester agrees to submit to the DAC indicated on the project request and the OER/DSPI Team 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 Data Users/Recipients.

As outlined in Term # (Data Security and Unauthorized Data Release), all notifications of unauthorized data sharing, breaches of data security, or inadvertent data releases should also be sent to the NIH Incident Response Team. For the NIH Incident Response Team, notifications can be made by phone (301) 496-HELP (4357); Toll Free Number: (866) 319-4357or TTY: (301) 496-8294, and can also be sent by email to NIHInfoSec@nih.gov or via the Report an Incident Link: https://irtportal.ocio.nih.gov/.

NIH, or another entity designated by NIH, may, as permitted by law, also investigate any DMI. Approved Data Users/Recipients 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 Data Users/Recipients 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.

Recipient's Compliance with Institutional Requirements: Recipient acknowledges that access, if provided, is for research that is approved by the Institution, which must be operating under an Office of Human Research Protections (OHRP)-approved Assurance. Furthermore, Recipient agrees to comply with all applicable DoD, VA, and NIH rules for the protection of human subjects, and other federal and state laws for the use of these data. The recipient agrees to report promptly to the Informatics System any proposed change in the research project and any unanticipated problems involving risks to subjects or others. This DAR is made in addition to, and does not supersede, any of Recipient's institutional policies or any local, State, and/or Federal laws and regulations that provide additional protections for human subjects.

One-Year Term and Access Period: Accounts with active projects are valid for one year and will be renewed annually following review and approval by the DAC, but only after the annual updates by the account holders (recipients) as discussed below. Data access will terminate 180 days following project/ grant end date. Accounts that remain inactive for 12 consecutive months may be closed at the discretion of the DoD, VA, and NIH.

Annual Update: The recipient will upload an annual summary of research accomplishments derived from the use of the Informatics System, along with an updated biographical sketch http://grants.nih.gov/grants/funding/2590/biosketchsample.pdf or CV, and a progress report, to their Informatics System account. Future access to the Informatics System will be contingent upon receiving the annual update.

Termination and Data Destruction: Upon Project Close-out, the Institutional Requester and Approved Data Users/Recipients agree to destroy all copies and versions of the dataset(s) retrieved from NIH controlled-access databases, regardless of the storage medium or format. However, the Data Access Requester may retain this data as necessary to comply with law, regulation, and government policy. A Data Access 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 Institutional Requester IT security requirements and policies.

The data may not be used to answer any additional research questions, even if they are within the scope of the approved DAR, unless the Data Access Requester submits a new DAR and is approved by NIH to conduct the additional research. If a Data Access Requester retains data for any of these purposes, the relevant portions of terms for Non-Identification, Certificate of Confidentiality, Non-transferability, Data Security and Unauthorized Data Release, Terms of Access Violations, and Termination and Data Destruction remain in effect after termination of this Agreement. These terms remain in effect until the data is destroyed.

Notification of Publication: Prompt publication or other public disclosure of the results of the Research Project is required. Recipient agrees to notify the Operations team via email FITBIR: FITBIR-ops@mail.nih.gov or NTRR: NTRR-ops@list.nih.gov as to when and where a publication (or other public disclosure) of a report from the Research Project will appear. Notification of such publications can occur by sending to the Operations team an updated biographical sketch http://grants.nih.gov/grants/funding/2590/ biosketchsample.pdf or CV of the publishing author.

Acknowledgments: Recipient agrees to acknowledge the contribution of the bioinformatics platform, the relevant Informatics System dataset identifier(s) (a serial number), and the Submitter(s) in any and all oral and written presentations, disclosures, and publications resulting from any and all analyses of data using the Informatics System tools, whether or not Recipient is collaborating with Submitter(s). The manuscript should include the following acknowledgement or other similar language:

> *Data and/or research tools used in the preparation of this manuscript were obtained and analyzed from the controlled access datasets distributed from the DoD, VA, and NIH-supported Informatics Systems. The Informatics System, created by the Department of Defense, the Department of Veteran Affairs, and the National Institutes of Health, is a national resource to support and accelerate research in TBI and trauma.*
>
> *Dataset identifier(s): [provide]. This manuscript reflects the views of the authors and may not reflect the opinions or views of the DoD, VA, NIH, or of the Submitters submitting original data to the Informatics System.*

If the Research Project involves collaboration with Submitters or Operations staff, then Recipient will acknowledge Submitters as co-authors, if appropriate, on any publication. In addition, Recipients agree to include a reference to Informatics System datasets analyzed and to cite the Informatics System and the federal funding sources in abstracts, as space allows.

Non-Endorsement, Indemnification: The Institutional Requester and the Approved Data User/Recipient acknowledge that all reasonable efforts have been taken to ensure the accuracy and reliability of controlled-access data accessed through the request, the NIH and Submitting Investigator(s) do not and cannot warrant the results that may be obtained by using any data included

therein. NIH and all contributors to these datasets disclaim all warranties as to performance or fitness of the data for any particular purpose.

Recipient agrees not to claim, infer, or imply endorsement by the United States Government, the Department of Defense, the Department of Veteran Affairs, the Department of Health & Human Services, or the National Institutes of Health of the Research Project, the entity, or personnel conducting the Research Project or any resulting commercial product(s).

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.

Data Access for Research: Recipients of Controlled Access data acknowledge that other authorized researchers have access to the data and that downloading, utilization, and duplication of research are distinct possibilities.

Recipient's Permission to Post Information Publicly: Recipient agrees to permit the DoD, VA, and the NIH to summarize on the Informatics System website the Recipient's research use of the Informatics System, along with the Recipient's name and organizational/institutional affiliation.

Privacy Act Notification: In order to access the Informatics system, the Recipient agrees to provide the information requested below.

The Recipient agrees that information collected from the Recipient, as part of the Data Access Request, may be made public in part or in whole for tracking and reporting purposes. This Privacy Act Notification is provided pursuant to Public Law 93-579, Privacy Act of 1974, 5 U.S.C. Section 552a. Authority for the collection of the information requested below from the recipient comes from the authorities regarding the establishment of the NIH, its general authority to conduct and fund research and to provide training assistance, and its general authority to maintain records in connection with these and its other functions (42 U.S.C. 203, 241, 289l-1 and 44 U.S.C. 3101), and Section 301 and 493 of the Public Health Service Act. These records will be maintained in accordance with the Privacy Act System of Record Notice 09-25-0156 covering "Records of Participants in Programs and Respondents in Surveys Used to Evaluate Programs of the Public Health Service, HHS/PHS/NIH/OD." The primary uses of this information are to document, track, and monitor and evaluate the use of the Informatics System datasets, as well as to notify interested recipients of updates, corrections, or other changes to the database.

The Federal Privacy Act protects the confidentiality of the Recipient's DoD, VA, and NIH records. The DoD, VA, and NIH, and any sites that are provided access to the datasets will have access to the data collected from the Recipient for the purposes described above. In addition, the Act allows the release of some information in the Recipient's records without his/her permission; for example, if it is required by members of Congress or other authorized individuals. The information requested is voluntary, but necessary for obtaining access to data.

Amendments: Amendments to this DAR must be made in writing and signed by authorized representatives of all parties.

Accurate Representations: The Recipient expressly certifies that the contents of any statements made or reflected in this document are truthful and accurate.

Information Security Best Practices

The purpose of these Security Best Practices, which are subject to applicable law, is to provide minimum security standards and best practices for individuals who use the Informatics System to submit, access, and analyze data. Keeping the Informatics System information secure through these best practices is important. Subject to applicable law, Recipients agree to immediately report breaches of data confidentiality to the DAC.

Best Practices

- Do not attempt to override technical or management controls to access data for which you have not been expressly authorized.
- Do not use your trusted position and access rights to exploit system controls or access data for any reason other than in the performance of the proposed research.
- Ensure that anyone directed to use the system has access to, and is aware of, Information Security Best Practices and all existing policies and procedures relevant to the use of the Informatics System, including but not limited to, the Informatics System policy at FITBIR: https://fitbir.nih.gov/ or NTRR: https://ntrr.nih.gov/.
- Notify Operations staff, as permitted by law, at either FITBIR: FITBIR-ops@mail.nih.gov or NTRR: NTRR-ops@list.nih.gov of security incidents, or any incidents of suspected fraud, waste, or misuse of the Informatics System, or when access to the Informatics System is no longer required.

Security Standards

All users in possession of NIH controlled-access data must protect this data in accordance with National Institute of Standards and Technology (NIST) SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations". Additional security standards are provided below based on workspace location for the data analysis. Non-U.S. users of controlled access data that are unable to align with the NIST SP 800-171 are permitted to use the ISO/IEC 27001/27002 "Information security, cybersecurity and privacy protection – Information security management systems – Requirements" and "Information security, cybersecurity and privacy protection – Information security controls" as a comparable standard.

All users must attest that their institution is compliant with the NIST SP 800-17. Users choosing a third-party IT system and/or Cloud Service Provider (CSP) for data analysis and/or storage for their project should provide the Informatics System with an attestation that the third-party system is compliant with NIST SP 800-171.

- Protect the data, providing access solely to authorized researchers permitted access to such data by your institution or to others as required by law.
- When downloading data from the Informatics System, ensure it is saved to a secure computer or server with strong password protection.
- For the computers hosting data from the Informatics System, ensure it has the latest security patches and are running virus protection software.
- Make sure the data are not exposed to the Internet or posted to a website that may be discovered by Internet search engines such as Google or MSN.
- If you leave your office, close out of data files or lock your computer. Consider the installation of a timed screen saver with password protection.
- Avoid storing data on a laptop or other portable medium. If storing data on such a device, encrypt the data. Most operating systems have the ability to natively run an encrypted file system or encrypt portions of the file system. (Windows = EFS or Pointsec and Mac OSX = File Vault)
- When finished using the data, destroy the data or otherwise dispose of it properly, as permitted by law.

Recipient Information and Certifications

NOTE: Upload the document as a PDF. E-signatures with a digital certificate are required.

Date: _____

Select one: ◯ FITBIR ◯ NTRR

Type of Application: ◯ New ◯ Renewal

Data Access Requester Information (Click Link for more information)

Are you the Project Director/Principal Investigator? ◯ Yes ◯ No

First Name:_____ Last Name: _____

Degree:_____Academic Position (or Title): _____

Institution:_____Department: _____

Street Address:_____

City:_____State/Province:_____

Zip/Postal Code:_____Country: _____

Telephone:_____ FAX: _____

E-mail Address_____

Note: public emails will be automatically rejected- please use your institutional email

Research Project (brief description of research objectives, study design, and analysis plan):

_____

_____

_____

Project Start Date:_____

Project End Date:_____

Note: All approved users will be granted access to all Shared Data within the Informatics System.

IRB Requirement

Access to data within the Informatics System requires an active and valid IRB approval.

Other Project Information:

1. Are Human Subjects Involved? ◯ Yes ◯ No

   If yes to Human Subjects

   Is the Project Exempt from Federal regulations? ◯ Yes ◯ No

   If yes, check the appropriate exemption number. ◯1 ◯2 ◯3 ◯4 ◯5 ◯6 ◯7 ◯8

   If no, is the IRB review pending? ◯ Yes ◯ No IRB

   Approval Date:_____

2. Project Summary/Abstract or Research Goal:

By signing and dating this DAR as part of requesting access to data in the Informatics System, I certify that I will comply with the terms and conditions of the DAR and with applicable DoD, VA, and NIH principles, policies, and procedures governing the use of the Informatics System. I attest that the data will be secured in accordance with the NIST SP 800-171, NIH Security Best Practices for Users of Controlled-Access Data. I further attest that if a third-party IT system and/or Cloud Service Provider (CSP) is used for data analysis and/or storage for this project, I will provide the Informatics System with an attestation that the third-party system is compliant with NIST SP 800-171, NIH Security Best Practices for Users of Controlled-Access Data. I also acknowledge that I have shared this document and the DoD, VA, and NIH policies and procedures with all research staff who will participate in the use of the Informatics System.

Signature:_____ Date: _____

IRB Approval #:_____ Expiration Date:_____

Recipient's Authorized Institutional Signing Official (SO) information: (Click link for more information)

Name: _____

Title: _____

Email:_____

Note: The SO email needs to be associated with the same institution as the Data Access Requester.
The SO CANNOT also serve as the Data Access Requester.

By signing and dating this DAR as part of requesting access to data in the Informatics System, I certify that I will comply with all the terms and conditions of the DAR and with applicable DoD, VA, and NIH principles, policies, and procedures governing the use of the Informatics System. I attest that the data will be secured in accordance with the NIH Security Best Practices for Users of Controlled-Access Data. I further attest that if a third-party IT system and/or Cloud Service Provider (CSP) is used for data analysis and/or storage for this project, I will provide the Informatics System with an attestation that the third-party system is compliant with NIST SP 800-171, NIH Security Best Practices for Users of Controlled-Access Data. As the SO, I confirm that the listed Data Access Requester is affiliated with their listed institution and meets the minimum requirements to qualify as a Data Access Requester. I also confirm that each listed Collaborator is affiliated with their indicated institution.

Signature:_____ Date: _____

Information on Other Key Personnel Requiring Repository Data Access:

Please list ALL individuals on the project that will need access to the repository data, including graduate students, post-doctoral fellows, technicians, internal collaborators, etc.

Note: Collaborators MUST be from the same institution as the Data Access Requester and SO. List each Collaborator below. External Collaborators are required to submit a separate DAR. (Click link for more information)

Data User Profile (Must be from the same institution as the Data Access Requester and SO):

First Name:_____ Last Name: _____

Degree:_____Academic Position (or Title): _____

Institution:_____Department: _____

Street Address: _____

City:_____State/Province: _____

Zip/Postal Code:_____Country: _____

Telephone:_____FAX: _____

E-mail Address: _____(institutional emails only, no Gmail etc)

Project Role:_____Other Project Role Category: _____

Data User Profile (Must be from the same institution as the Data Access Requester and SO):

First Name:_____ Last Name: _____

Degree:_____Academic Position (or Title): _____

Institution:_____Department: _____

Street Address: _____

City:_____State/Province: _____

Zip/Postal Code:_____Country: _____

Telephone:_____FAX: _____

E-mail Address: _____(institutional emails only, no Gmail etc)

Project Role:_____ Other Project Role Category: _____

Data User Profile (Must be from the same institution as the Data Access Requester and SO):

First Name:_____ Last Name: _____

Degree:_____Academic Position (or Title): _____

Institution:_____Department: _____

Street Address: _____

City:_____State/Province: _____

Zip/Postal Code:_____Country: _____

Telephone:_____FAX: _____

E-mail Address: _____(institutional emails only, no Gmail etc)

Project Role:_____Other Project Role Category: _____

Data User Profile (Must be from the same institution as the Data Access Requester and SO):

First Name:________________________________ Last Name: ____________________________

Degree:_________________Academic Position (or Title): __________________________________

Institution:__________________________________Department: ____________________________

Street Address: ____

City:___________________________________State/Province: ______________________________

Zip/Postal Code:____________________Country: ________________________________

Telephone:______________________________FAX: _____________________________

E-mail Address: ______________________________________(institutional emails only, no Gmail etc)

Project Role:________________________________Other Project Role Category: _______________________

Data User Profile (Must be from the same institution as the Data Access Requester and SO):

First Name:________________________________ Last Name: ____________________________

Degree:_________________Academic Position (or Title): __________________________________

Institution:__________________________________Department: ____________________________

Street Address: ____

City:___________________________________State/Province: ______________________________

Zip/Postal Code:____________________Country: ________________________________

Telephone:______________________________FAX: _____________________________

E-mail Address: ______________________________________(institutional emails only, no Gmail etc)

Project Role:________________________________Other Project Role Category: _______________________

Data User Profile (Must be from the same institution as the Data Access Requester and SO):

First Name:________________________________ Last Name: ____________________________

Degree:_________________Academic Position (or Title): __________________________________

Institution:__________________________________Department: ____________________________

Street Address: ____

City:___________________________________State/Province: ______________________________

Zip/Postal Code:____________________Country: ________________________________

Telephone:______________________________FAX: _____________________________

E-mail Address: ______________________________________(institutional emails only, no Gmail etc)

Project Role:________________________________Other Project Role Category: _______________________

Use additional sheets for additional profiles as needed.