NATIONAL TRAUMA RESEARCH REPOSITORY (NTRR) POLICIES

This work was sponsored by the Department of the Army, Prime award #W81XWH-15.2.0089. The U.S. Army Medical Research Acquisition Activity, 820 Chandler Street, Fort Detrick MD21702-5014 is the awarding and administering acquisition office. The opinions or assertions contained herein are the private views of the authors and are not to be construed as official or as reflecting the view of the Department of the Army or the Department of Defense.

Overview

Previous analyses of research data have shown that many trauma studies cannot be replicated or validated due to a variety of factors including lack of access to study data, lack of access to protocol information, and inability to replicate procedures used in the study. New data sharing rules for federally funded studies have been put in place to address factors associated with this issue. In order to address data sharing requirements, investigators conducting research on trauma and critical care can maximize the utility of the data they produce with the launch of the National Trauma Research Repository (NTRR).

The NTRR was developed as a resource to support new and emerging data sharing needs within the trauma research community and is envisioned to be a key piece of the national trauma research infrastructure (http://www.ntrr-nti.org/). It is funded by the Department of Defense (DoD) (http://www.usamma.amedd.army.mil/) and developed by the National Trauma Institute (NTI) (https://www.nattrauma.org/) to promote collaboration, accelerate research, and advance knowledge on the treatment of trauma. When fully functional, the NTRR will be a comprehensive repository offering thousands of data points from hundreds of studies, enabling investigators to query across studies for their own research objectives.

The NTRR was developed by trauma researchers for trauma researchers. A national committee of civilian and military trauma researchers and stakeholder organizations defined the functional requirements of the repository that would best serve investigators.(1) The NTRR allows users to peruse available data elements, study datasets, and supporting documentation (e.g., protocols, consent forms, data dictionaries). Investigators contributing data to the NTRR can upload completed datasets and supporting documents at the completion of a study or as the study is being conducted. All studies will submit core data elements and study metadata (information about the study). Use of common data elements (CDEs) is encouraged to improve data harmonization and opportunities for comparison and combination of data from multiple studies. The system also allows researchers to use unique data elements, or UDEs, if a CDE for that variable is not available. When the dataset is complete and validated, it receives a digital object identifier (DOI) to allow contributing researchers to be acknowledged in publications resulting from secondary analyses.

The NTRR is organized in four modules representing the entire patient care trajectory: pre-hospital care, inpatient care, rehabilitation, and long-term outcomes/quality of life issues. Access to the system is through a web-based interface developed by the National Institutes of Health – Center for Information Technology (NIH/CIT) (https://www.cit.nih.gov/) and enhanced by NTI. Hosted in a secure Amazon Web Services (AWS) cloud environment, the repository conforms to standards set forth in the Federal Information Security Management Act (FISMA), which provides a standardized approach for assessing, monitoring, securing, and authorizing cloud computing products. Specific security controls in place for NTRR include firewalls, application monitoring software and integrated cloud tools for operating system scanning, SSL (Secure Sockets Layer), Anti-Virus and Password encryption technology, and security audits and inspections.

Oversight and Governance

The National Trauma Institute developed a governance structure for NTRR to provide oversight. The NTRR is directed by the NTRR Executive Committee. The NTRR Data Use Committee oversees the NTRR data sharing policies and procedures.

The NTRR Data Use Committee is also responsible for overseeing data access to promote consistent and robust participant protections in NTRR.

The NTRR operating and data sharing policies address: 1) data sharing procedures, 2) data access principles, and 3) issues regarding the protection of research participants during the submission of, storage of, and access to data within the NTRR. The goal of the policies is to advance science for the benefit of the public through the creation of a centralized Federal data repository for trauma research data. The principles contained in this policy were developed by the NTRR Policy Subcommittee and are consistent with existing NTI and DoD policies on data sharing. The NTI recognizes that scientific, ethical, and societal issues relevant to this policy are evolving. The NTI Policy Subcommittee will revisit and revise the policy and related practices as appropriate. NTI has also adopted data use guidance, definitions, tools, and use agreement templates developed by the Data Stewardship Subcommittee of the Federal Demonstration Partnership (http://sites.nationalacademies.org/PGA/fdp/index.htm). The Data Stewardship Subcommittee advises government and research partners on administrative requirements imposed across federal agencies related to data security, retention, sharing, and integrity.(2)

Applicability

The NTRR General Operating Policy applies to data collected during DoD and other federal (e.g., Department of Health and Human Services (DHHS)) extramural research projects, projects funded by other sources, and projects without funding that include trauma studies, defined as:

- Patient-oriented research. Research conducted with human subjects (or on material of human origin such as tissues, specimens, and cognitive phenomena) for which an investigator (or colleague) directly interacts with human subjects. Excluded from this definition are *in vitro* studies that utilize human tissues that cannot be linked to a living individual. It includes:
    - mechanisms of human disease;
    - therapeutic interventions;
    - clinical trials;
    - development of new technologies;
- Epidemiological and behavioral studies;
- Outcomes research and health services research;
- Prospective, observational studies;
- Case studies;
- Meta-analysis studies

Contributing and Recipient Investigators

For purposes of these policies:

A **contributing investigator** is an investigator who has submitted/or plans to submit data to the NTRR, according to the policies laid out in the NTRR Data Submission Request. The contributing investigator may have had a past or current/active grant, contract, or consulting agreement with DoD or NTI, one of its contractors, or any other funding source. For more information on contributing investigators' responsibilities, see the NTRR Data Contribution Policy.

The **recipient investigator** is an investigator who seeks access to data from the NTRR. The recipient investigator and his/her organization may be a researcher at a non-profit or for-profit organization or corporation with or without an approved assurance from the Department of Health and Human Services Office for Human Research Protections (OHRP) or the DoD. The recipient requests access to study data at his/her sole risk and at no expense to the study, DoD, and NTI. For more information on recipient investigators' responsibilities, see the NTRR Data Sharing Policy.

Data Quality

The NTI has implemented a two-tiered data control procedure for information submitted to the NTRR to ensure that the information submitted has undergone reviews for accuracy, completeness, and availability. The first level of quality control is performed by the researcher who is expected to certify the accuracy of the information prior to submission. The second level of quality control occurs when data are submitted to the NTRR (validation process). NTRR will provide a period of three months to allow the contributing investigator to undertake activities to review the completeness of the submission. Such efforts include verifying that the information received by NTRR is complete (i.e., not missing records intended for submission), contains no identifying information, and displays correctly. Should the investigator determine that additional time is necessary to ensure the quality of the submitted information (e.g., time necessary to remedy concerns), the NTI may opt to extend the quality control period, as necessary. After quality control measures are satisfied, the submitted information will be certified as accurate by the submitting researcher.

Data Security

The NTRR has several layers of security patterned after the controls in place for other Biomedical Research Information Computer System (BRICS) projects developed by the National Institutes of Health – Center for Information Technology. The following is a list of the specific controls in place:

- Firewall – NTRR has implemented a dual-layer firewall policy, which includes both AWS security groups and directly on the Linux/Windows servers. The policy only allows the necessary ports for both web and sftp traffic. In addition, the logs are checked periodically for any suspicious activity.
- Anti-Virus – The NTRR Linux servers have ClamAV installed and daily scans are performed.
- Patching – All NTRR servers are a mix of Redhat Enterprise Linux, CentOS Linux, and Windows Server 2016, and patches are installed on a regular schedule. In addition, critical and high vulnerabilities will be mitigated immediately.
- Scanning – NTRR will utilize both its own scanning tools (including IBM Appscan and AWS) and will also implement any security fixes mandated by NIH/BRICS.
- Monitoring – The NTRR project will employ the integrated AWS monitoring to track resource activity and other miscellaneous monitoring.

Protecting Research Participants

The potential for public benefit to be achieved through sharing trauma research data is significant. However, the broad data distribution goals of NTRR highlight the importance of protecting the privacy of research participants and the confidentiality of their data. The NTRR Data Sharing Policy includes steps to protect the interests and privacy concerns of individuals, families, and identifiable groups who participate in trauma research. The informed consent process is a critical step, and subject consent forms in prospective clinical studies should include language similar to the following:

> "All links with your identity will be removed from the data before they are shared. Only de-identified data that do not include anything that might directly identify you will be shared with National Trauma Research Repository (NTRR) users and the general scientific community for research purposes."

For studies conducted before the development of NTRR, there is considerable variation in the extent to which data sharing and future research have been addressed within the informed consent documents. The submitting institution will determine whether a study is appropriate for submission to the NTRR (including an Institutional Review Board (IRB) and/or Privacy Board review of specific study elements, such as participant consent). Some studies may require additional consent of the research participants. To ensure the security of the data held in the NTRR, NTI will employ multiple tiers of data security based on the content and level of risk associated with the data. NTRR will maintain

operating policies and procedures to address the privacy and confidentiality of research participants, the interests of individuals and groups, data access procedures, and data security mechanisms. These will be reviewed periodically by the NTRR oversight bodies as appropriate.

Non-Research Use of Data

As agencies of the Federal Government, the DoD and NTI are required to release government records in response to a request under the Freedom of Information Act (FOIA), unless they are exempt from release under one of the FOIA exemptions. Although the NTRR-held data will be de-identified, and neither the DoD nor NTI will hold direct identifiers to individuals within the NTRR, the agencies recognize the personal and potentially sensitive nature of the genotype-phenotype data. The NTI maintains that release of un-redacted NTRR datasets in response to a FOIA request would constitute an unreasonable invasion of personal privacy under FOIA Exemption 6, 5 U.S.C. § 552 (b)(6). Therefore, among the safeguards that the agencies foresee using to preserve the privacy of research participants and confidentiality of genetic data are the redaction of individual-level genotype, phenotype, and other clinical data from disclosures made in response to FOIA requests and the denial of requests for un-redacted datasets.

In addition, the NTI acknowledges that legitimate requests for access to data made by law enforcement offices to the NTRR may be fulfilled. NTI will not possess direct identifiers within the NTRR, nor will the agencies have access to the link between any data code and the identifiable information that may reside with the contributing primary investigators or contributing institutions for particular studies. The release of identifiable information may be protected from compelled disclosure by the primary investigator's institution if a Certificate of Confidentiality is or was obtained for the original study. The NTI encourages investigators to consider the potential appropriateness of obtaining a Certificate of Confidentiality (https://humansubjects.nih.gov/coc/index) as an added measure of protection against future compelled disclosure of identities for studies planning to collect genome-wide association data. These confidentiality provisions may not apply to military subjects' chains of command.

Publications

The NTI strongly encourages collaboration; but at a minimum, all investigators who access NTRR data are expected to acknowledge the funding organization(s) that supported their work, the contributing investigator(s) who conducted the original study, the digital object identifier for the data (DOI), and the NTRR in all resulting presentations, disclosures, or publications of the analyses. Data recipients should submit manuscripts to the NTRR Steering Committee for administrative review at least four weeks prior to submission for publication to ensure that the terms of the user agreement have been met, the description of NTRR procedures are accurately described (if any), and the original researchers, DOI and NTRR are appropriately acknowledged. This administrative review will take no longer than two weeks.

Contributing Investigator

A contributing investigator is defined as a researcher who has submitted/or plans to submit data to the NTRR, according to the policies laid out in the NTRR Data Submission Request form. The contributing investigator may have had a past or current/active grant, contract, or consulting agreement with DoD or NTI, one of its contractors, or any other funding source.

User Accounts

Contributing investigators need an NTRR account to access the data submission modules. Investigators seeking a user account from NTRR will submit a Data Submission Request, a biographical sketch or CV, and study materials via the NTRR website. User accounts will be reviewed by the NTRR Data Use Committee. Membership of this committee includes researchers and staff with expertise in relevant scientific disciplines, research participant protection, and privacy. The NTRR Data Use Committee reviews the application of each investigator and grants access based on the professional experience of the researcher affiliation with a research institution, and the scientific merit of the request. It is anticipated that most requests will be appropriate and can be approved rapidly, and that only a few will require clarification. In the event that requests raise concerns related to privacy and confidentiality, risks to populations or groups, or other concerns, the Data Use Committee will consult with other experts and the NTRR Executive Committee, as appropriate.

Data Submission Process

Contributing investigators will submit study information as part of Data Submission Request form, receive notification about their account status, attend NTRR virtual training sessions (optional), set up their study within the system (including granting access to other team members), and review the NTRR data dictionary and form structures. The NTRR Operations team works with researchers to map their study variables to existing common data elements (CDEs) and new unique data elements (UDEs). In addition to CDE and UDE variables, NTRR will accept supporting documentation such as:

- study protocols;
- manual of operations;
- study data dictionary;
- Human subjects protection documents (e.g., Institutional Review Board application, consent forms, etc.);
- case report forms; and
- other relevant documents.

If the data submission request is approved, the investigator's institution must execute a Data Transfer and Use Agreement with the National Trauma Institute prior to submitting data. See user manuals and training videos on the NTRR website for details on creating a study and uploading study data.

Data submitted to the NTRR will be certified as de-identified or as a limited data set by the contributing investigator such that the identities of data subjects cannot be readily ascertained or otherwise associated with the data by the NTRR staff or secondary data users. Contributing investigators will certify that an appropriate IRB has considered such risks and that the data have been de-identified or conforms with limited data sets standards in accordance with other federal

regulations (e.g., HIPAA) before the data are submitted.

Submissions of data to NTRR will be accompanied by a certification signed by the contributing investigator to assure that:

- The data submission is consistent with all applicable laws and regulations, as well as institutional policies;
- The appropriate research uses of the data and the uses that are explicitly excluded by the informed consent documents are delineated;
- The identities of research participants will not be disclosed to the NTRR/NTI; and
- An IRB of the contributing institution and/or Privacy Board, as applicable, reviewed and verified that:
    - The submission of data to the NTRR and subsequent sharing for research purposes to recipient investigators are consistent with the informed consent of study participants from whom the data were obtained;
    - The investigator's plan for de-identifying or limiting datasets is consistent with the standards outlined above;
    - The risks to individuals, their families, and groups or populations associated with data submitted to the NTRR have been considered.

Recipient Investigator

The recipient investigator is an investigator who seeks access to data from the NTRR. The recipient investigator and his/her organization may be a researcher at a non-profit or for-profit organization or corporation with or without an approved assurance from the Department of Health and Human Services Office for Human Research Protections (OHRP) or the DoD. The recipient requests access to study data at his/her sole risk. Investigators requesting data from the NTRR will submit a Data Access Request form, a current biographical data sketch, and institutional review board approval (if appropriate). Requests will include a brief description of the proposed research use of the requested NTRR data.

Data Access Process

Access to data for research purposes will be provided through the NTRR Data Use Committee. Membership of this committee includes researchers and staff with expertise in relevant scientific disciplines, research participant protection, and privacy. The NTRR Data Use Committee will review the requests and make a determination based on the investigator's professional experience, affiliation with a research institution, and the scientific merit of the request. It is anticipated that most requests will be appropriate and can be approved rapidly, and that only a few will require clarification. In the event that requests raise concerns related to privacy and confidentiality, risks to populations or groups, or other concerns, the NTRR Data Use Committee will consult with other experts as appropriate. A request to appeal the decision is allowed and will be reviewed by the NTRR Steering Committee.

If the data access request is approved, the investigator's institution must execute a Data Transfer and Use Agreement with the National Trauma Institute prior to receiving data via secured transfer. Investigators and institutions seeking data from the NTRR will be expected to meet data security measures (such as physical security, information technology security, and user training). Investigators will agree, among other things, to:

- Use the data only for the approved research; if the recipient investigator wants to use the data to investigate additional research questions, a second data access request form must be submitted.
- Protect data confidentiality;
- Follow appropriate data security protections;
- Follow all applicable laws, regulations, and local institutional policies and procedures for handling NTRR data;
- Not attempt to identify individual participants from whom data within a dataset were obtained;
- Not sell any of the data elements from datasets obtained from the NTRR;
- Not share with individuals other than those listed in the request any of the data elements from datasets obtained from the NTRR;
- Agree to the list of approved research uses;
- Provide IRB approval memorandum and continuing reviews (if appropriate);
- Agree to report, in real time, violations of the NTRR Data Sharing Policy to the NTRR Executive Committee;
- Provide annual progress reports on research using NTRR data;
- Notify the NTRR Executive Committee of policy violations;
- Submit annual progress reports detailing significant research findings; and
- Include acknowledgements of the original research group/investigator who collected the data and the NTRR in all publications and presentations.

APPENDICES

NTRR Data Submission Request Form

NTRR Data Access Request Form

FDP Data Transfer and Use Agreement (DTUA) Project Glossary of Terms

FDP DTUA Guidance Chart

FDP Tool for Classifying Human Subjects Data

The NTRR has adopted data use guidance, definitions, tools, and use agreement templates developed by the Data Stewardship Subcommittee of the Federal Demonstration Partnership (http://sites.nationalacademies.org/PGA/fdp/index.htm). The Data Stewardship Subcommittee advises government and research partners on administrative requirements imposed across federal agencies related to data security, retention, sharing, and integrity.(2)

REFERENCES

1. Smith SL, Price MA, Fabian TC, Jurkovich GJ, Pruitt BA, Jr., Stewart RM, Jenkins DH. The National Trauma Research Repository: Ushering in a new era of trauma research. Shock. 2016;46(3 Suppl 1):37-41.
2. Partnership DSSotFD. FDP Data stewardship Washington, DC: The National Academies of Sciences, Engineering and Medicine; 2018 [updated 4/6/2018; cited 2018 6/6/2018]. Available from: http://sites.nationalacademies.org/PGA/fdp/PGA_170894.

National Trauma Research Repository
Data Submission Request

Date: _____
Type of Request: ☐New ☐Renewal

Submitting/Contributing Investigator Information

First Name: _____ Last Name: _____
Degree: _____ Academic Position (or Title): _____
Institution: _____ Department: _____
Telephone: _____ E-mail Address: _____

Project Director/Principal Investigator Contact Information (if different from above)

First Name: _____ Last Name: _____
Degree: _____ Academic Position (or Title): _____
Institution: _____ Department: _____
Telephone: _____ E-mail Address: _____

Senior/Key Person Profile (Collaborating Investigator)

First Name: _____ Last Name: _____
Degree: _____ Academic Position (or Title): _____
Institution: _____ Department: _____
Telephone: _____ E-mail Address: _____
Project Role: _____ Other Project Role Category: _____

Senior/Key Person Profile (Collaborating Investigator)

First Name: _____ Last Name: _____
Degree: _____ Academic Position (or Title): _____
Institution: _____ Department: _____
Telephone: _____ E-mail Address: _____
Project Role: _____ Other Project Role Category: _____

Submit a CV or biographical sketch for each investigator.

Project Information

1. Project Summary/Abstract and hypotheses:
   _____

2. Are human subjects involved? Yes ☐No ☐
   If yes:
   Is the project exempt from federal regulations? ☐Yes ☐No
   If yes, check appropriate exemption number. ☐1 ☐2 ☐3 ☐4 ☐5 ☐6

   IRB Approval Date: _____

3. Is the study registered on www.clinicaltrials.gov? ☐Yes ☐No
   If yes:
   Funding agency: _____

4. Was the study extramurally funded? ☐Yes ☐No
   If yes:
   Funding agency: _____
   Grant title: _____
   Award number: _____

5. Attachments

   Please upload electronic copies of the study protocol, questionnaires and clinical report forms, study manuals, data dictionary and other supporting documents via the NTRR website.

National Trauma Research Repository (NTRR)
Data Sharing Agreement

I, _____, request approval to submit data and images to the National Trauma Research Repository (NTRR) to share data for research. I agree to the following terms:

1. Research Project. These data will be submitted solely in connection with the research project specifically indicated and described in the contributor information and certifications section.

Data submitted to NTRR may be made available by NTI and DoD for either collaborative research (i.e., to accelerate research on ongoing studies) or general research purposes (i.e., meta-analyses and other secondary uses of the data).

This Data Submission Agreement (DSA) covers only the research project as contemplated in the Submitting/Contributing Investigator Information and certifications section. The contributor will submit a completed DSA (this document) for each research project for which submission is requested.

2. Non-transferability of Agreement. This DSA is not transferable. Contributing investigator agrees that substantive changes the contributing investigator makes to the research project requires execution of a new DSA, in which the new research project is designated. If the contributing investigator changes institutions and wishes to retain submission privileges to NTRR, a new DSA in which the new institution acknowledges and agrees to the provisions of the DSA is necessary.

3. Use of Common Data Elements. Contributing investigator agrees to use the NTRR Common Data Elements (CDEs) as appropriate for their research. NTRR staff will work with researchers to map their study variables to specific CDEs and develop unique data elements (UDEs).

4. Non-Identification of Subjects. Contributing investigator agrees the data have been either de-identified or conform with limited data set requirement. Contributing investigator further agrees not to disclose the identities of research participants to NTRR in the future and to verify that data lack identifiers after submission. Contributing investigator agrees to notify NTRR as soon as possible if, upon review of NTRR data, the Contributing investigator discovers identifying information in that data.

5. Data Disclaimers. Contributing investigator agrees that DoD and NTI do not and cannot warrant the results that may be obtained by using any data included in NTRR. DoD and NTI disclaim all warranties as to the accuracy of the data in NTRR or the performance or fitness of the data or data analysis tools for any particular purpose.

6. Supporting Materials. Contributing investigator agrees to provide NTRR with supporting information and documentation to enable efficient use of the submitted data by investigators unfamiliar with the data including but not limited to:

- Research protocol(s)
- Study questionnaire(s)
- Study manuals
- Human research protection documents (IRB submission, consent forms, and related documents)
- Description of variables measures
- Other supporting documentation, as appropriate

7. Data Accuracy. Contributing investigator certifies to the best of his/her knowledge and belief that the data submitted to NTRR are accurate. Contributing investigator also agrees to perform the specified quality control activities (including data validation) within a timeframe specified by the NTRR Policy. Contributing investigator further agrees to notify NTRR as soon as possible if, upon review of NTRR data, the contributing investigator discovers data quality concerns.

8. Notification to DoD and NTI of Publication. Prompt publication or other public disclosure of the results of the research project is required. Contributing investigator agrees to notify NTI as to when and where a publication (or other public disclosure) from the research project will appear. Notification of such publications can occur by sending an email to admin@ntrr-nti.org with the title, authors, place of publication, and publication date.

9. Data Access for Research. Contributing investigator agrees that data and supporting materials submitted to NTRR may be accessed and used broadly by qualified researchers for research and other activities as authorized by and consistent with law.

10. Non-Research Access. Contributing investigator acknowledges that data and supporting materials submitted to NTRR become U.S. Government records that are subject to the Freedom of Information Act (FOIA). DoD and NTI are required to release Government records in response to FOIA requests unless they are exempt from release under one of the FOIA exemptions. Contributing investigator further acknowledges that data and supporting materials may be used or released consistent with law.

11. Acknowledgments. In all oral and written presentation, disclosures, and publications based upon dataset(s) submitted to NTRR, contributing investigator agrees to cite NTRR, the relevant NTRR dataset identifier (a Digital Object Identifier (DOI)), and the contributing investigators' federal research funding sources in each publication to which such datasets contribute (for abstracts, as space allows). The publication should include the following acknowledgment or similar language:

> Data and research tools used in the preparation of this manuscript reside in the Department of Defense (DOD) and National Trauma Institute (NTI) supported National Trauma Research Repository (NTRR). Digital Object Identifier: [insert DOI here] This manuscript reflects the views of the authors and does not reflect the opinions or views of the Department of Defense of the National Trauma Institute.

12. Non-Endorsement Liability. Contributing investigator agrees not to claim, infer, or imply endorsement by the United States Government, the Department of Defense, the Department of Health & Human Services, or the National Trauma Institute, the entity, or personnel conducting the research project or any resulting commercial product(s). The United States Government assumes no liability except to the extent provided under the Federal Tort Claims Act (28 U.S.C. § 2671-2680).

13. Contributing Investigator's Compliance with Institutional Requirements. Contributing investigator acknowledges that these data were collected in a manner consistent with all applicable laws and regulations, as well as institutional policies. Contributing investigator further acknowledges that the data were collected pursuant to an informed consent, if applicable, that is consistent with the data submission, and that the data submitted were collected in accordance with applicable DHHS/FDA and DoD regulations, or applicable foreign law concerning the protection of human subjects, and other applicable U.S. federal and state laws, if any.

14. Contributing Investigator's Permission to Post Information Publicly. Contributing investigator agrees to permit DoD and NTI to summarize and release for public use on the NTI website the supporting materials along with the contributing investigator's name and organizations/institutional affiliation.

15. Privacy Act Notification. The contributing investigator agrees that information collected from the contributing investigator, as part of the DSA, may be made public in part or in whole for tracking and reporting purposes. This Privacy Act Notification is provided under 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 contributing Investigator comes from the authorities regarding the establishment of the NTI's 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. These records will be maintained in accordance with the Privacy Act System of Records. The primary uses of this information are to document, track,

monitor and evaluate the submission of data from clinical, basic, and population-based research activities and to notify contributing investigators in the event a potential error in the dataset is identified or in the event of updates or other changes to the database.

The Federal Privacy Act protects the confidentiality of the contributing investigator's NTI and DoD records. DoD and NTI will use the data collected for the purposes described above. Also, the Act allows the release of some information in the contributing investigator's records without the contributing investigator's permission; for example, if it is required by members of Congress or other authorized individuals.

16. Security. Contributing investigator acknowledges the expectations set forth by the attached "NTRR Information Security Best Practices" for the use and security of data.

17. Amendments. Amendments to this DSA must be made in writing and signed by authorized representatives of both parties.

18. Termination. Either party may terminate this DSA without cause by providing 30 days written notice to the other party. NTRR will retain a copy of all data already submitted to NTRR for which data quality activities have been completed, except if research participants withdraw consent for sharing of their data through the NTRR repository and DoD and NTI are informed by the contributing investigator to withdraw the data. Contributing investigators agree to immediately report violations of NTRR Policy to the NTRR Steering Committee. Additionally, DoD and NTI may terminate this agreement with five days written notice if the agencies determine, in their sole discretion, that the contributing investigator has committed a material breach of this DSA. The agencies may, in their sole discretion, provide Contributing investigator with 30 days' notice to remedy a breach before termination. Closed accounts may be reactivated upon submission of an updated Submission Request and DSA.

19. One-Year Term and Access Period. Researchers who are granted permission to submit data to NTRR receive an account that is valid for one year. This DSA will automatically terminate at the end of one year. An account may be renewed upon recertification of a new DSA. Accounts that remain inactive for 12 consecutive months may be closed at the discretion of the NTRR staff.

NTRR 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 NTRR to submit, access, and analyze data. Keeping NTRR information secure through these best practices is important. Subject to applicable law, contributing investigators agree to immediately report breaches of data confidentiality to the NTRR Data Use Committee at admin@ntrr-nti.org.

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, NTRR Information Security Best Practices and all existing policies and procedures relevant to the use of NTRR, including but not limited to, the NTRR policy at the NTRR website.
- Follow the NTRR password policy which includes:
    - Choose passwords of at least seven characters including at least three of the following types of characters: capital letters, lower case letters, numeric characters and other special characters.
    - Change your passwords every six months.

    - Protect your NTRR password from access by other individuals—for example, store it electronically in a secure location.
- Notify NTRR staff, as permitted by law, at admin@ntrr-nti.org of security incidents, or any incidents of suspected fraud, waste or misuse of NTRR or when access to NTRR is no longer required.

Security Standards

- Protect the data, providing access solely to authorized researchers permitted access to such data by your institution or to others as required by law.
- Store NTRR data on a secured computer or server with strong password protection with the latest security patches and 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. 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 and as specified in the data use agreement.

By signing and dating this Data Submission Agreement as part of submitting data in NTRR, I certify that I will abide by the certifications, policies and procedures for the use of the NTRR. I further acknowledge that I have shared this document and the NTRR policies and procedures with any research staff who will participate in the contribution of data to the NTRR for this study.

X_____

Signature:_____ Date: _____

National Trauma Research Repository
Data Access Request

Date: _____
Type of Request: ☐New ☐Renewal

Recipient Investigator Information

First Name: _____ Last Name: _____
Degree: _____ Academic Position (or Title): _____
Institution: _____ Department: _____
Telephone: _____ E-mail Address: _____

Project Director/Principal Investigator Contact Information (if different from above)

First Name: _____ Last Name: _____
Degree: _____ Academic Position (or Title): _____
Institution: _____ Department: _____
Telephone: _____ E-mail Address: _____

Senior/Key Person Profile (Collaborating Investigator)

First Name: _____ Last Name: _____
Degree: _____ Academic Position (or Title): _____
Institution: _____ Department: _____
Telephone: _____ E-mail Address: _____
Project Role: _____ Other Project Role Category: _____

Senior/Key Person Profile (Collaborating Investigator)

First Name: _____ Last Name: _____
Degree: _____ Academic Position (or Title): _____
Institution: _____ Department: _____
Telephone: _____ E-mail Address: _____
Project Role: _____ Other Project Role Category: _____

Submit a CV or biographical sketch for each investigator.

Proposed Project Information

1. Project Summary/Abstract and hypotheses:

_____

2. Are human subjects involved? Yes ☐ No ☐

If yes:

Is the project exempt from federal regulations? ☐Yes ☐No

If yes, check appropriate exemption number. ☐1 ☐2 ☐3 ☐4 ☐5 ☐6

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

IRB Approval Date: _____

3. Which study(ies) listed in the NTRR do you plan to use for your project? List all:

_____

National Trauma Research Repository (NTRR)
Data Use Certification

I, _____, request approval to access data from the National Trauma Research Repository (NTRR) for research purposes. I agree to the following terms:

Terms and Conditions

1. Research Project. These data will be used by recipient investigator solely in connection with the Project Summary/Abstract. If the project involves contributing investigator(s), their names and the work they will perform are also included in the recipient investigator Information and Certifications section of this Data Use Certification (DUC).

This DUC covers only the research project contemplated in the Project Summary/Abstract section. Recipient investigator agrees that data will not be used in any research that is not disclosed and approved as part of the research project. The recipient will submit a signed certification (this document) for each research project for which data are requested.

2. Non-transferability of Agreement. This DUC is not transferable. Recipient investigator agrees that any substantive change recipient investigator makes to the research project requires execution and approval of a new DUC, in which the new research project is designated. If the recipient investigator appoints another principal investigator to complete the research project, a new DUC in which the new recipient investigator is designated is necessary. If the recipient investigator changes institutions and wishes to retain access to NTRR data, a new DUC must be executed and approved.

3. Non-Identification of Subjects. Recipient investigator agrees that data will not be used, either alone or in conjunction with any other information, in any effort whatsoever to establish the individual identities of any of the subjects from whom data were obtained. Recipient investigator agrees to notify NTRR as soon as possible if, upon the use of NTRR data, the recipient investigator discovers identifying information in those data.

4. Data Disclaimers. Recipient agrees that DoD and NTI do not and cannot warrant the results that may be obtained by using any data included therein. DoD and NTI disclaim all warranties as to the accuracy of the data in NTRR or the performance or fitness of the data for any particular purpose.

5. Notification of NTRR of Publication. Prompt publication or other public disclosure of the results of the research project is required. Recipient investigator agrees to notify NTRR via email as to when and where a publication (or other public disclosure) from the research project will appear.

6. Data Access for Research. Data from active and completed studies are eligible for restricted controlled access by qualified recipient investigator under the terms outlined in this agreement. Recipient investigator of controlled access data acknowledges that other researchers have access to the data and that downloading, utilization, and duplication of research are distinct possibilities.

7. No Distribution of Data. Recipient investigator agrees to retain control over data and further agrees not to transfer data, with or without charge, to any other entity or any individual, except for collaborators with approved DUCs. Recipient investigator agrees not to sell the data in any form to any entity or individual or to distribute the data to anyone other than his/her research staff and collaborators with an approved DUC, who will also agree to the terms within this DUC.

8. Acknowledgments. Recipient investigator agrees to acknowledge the contribution of the NTRR bioinformatics platform, the relevant NTRR dataset identifier(s) (digital object identification), and the contributing investigator(s) in any and all oral and written presentations, disclosures, and publications resulting from any and all analyses of data using the NTRR tools, whether or not recipient investigator is collaborating with contributor investigator(s). The manuscript should include the following acknowledgment or other similar language:

Data and/or research tools used in the preparation of this manuscript reside in the Department of Defense (DOD) and National Trauma Institute (NTI) supported National Trauma Research Repository (NTRR). Digital Object Identifier: [insert DOI here] This manuscript reflects the views of the authors and does not reflect the opinions or views of the Department of Defense of the National Trauma Institute.

If the research project involves collaboration with contributing investigators or NTRR staff, the recipient investigator will acknowledge contributor investigator or NTRR staff as co-authors, if appropriate, on any publication. Also, recipient investigator agrees to include a reference to NTRR datasets analyzed and to cite NTRR and the federal funding sources in abstracts as space allows.

9. Non-Endorsement Liability. Recipient investigator agrees not to claim, infer, or imply endorsement by the United States Government, the Department of Defense, the Department of Health & Human Services, or the National Trauma Institute, the entity, or personnel conducting the research project or any resulting commercial product(s). The United States Government assumes no liability except to the extent provided under the Federal Tort Claims Act (28 U.S.C. § 2671-2680).

10. Recipient Investigator Compliance with Institutional Requirements. Recipient investigator acknowledges that access to NTRR data, if provided, is for research that must be authorized by the recipient investigator's Institution, which may or may not require operation under an Office of Human Research Protections (OHRP)-approved Assurance as determined by the institution. Furthermore, recipient investigator agrees to comply with all applicable DoD and DHHS/FDA rules for the protection of human subjects, and other federal and state laws for the use of these data. Recipient investigator agrees to report promptly to NTRR any proposed change in the research project and any unanticipated problems involving risks to subjects or others. This DUC is made in addition to, and does not supersede, any of recipient investigator' s institutional policies or any local, State, and/or Federal laws and regulations that provide additional protections for human subjects.

11. Recipient Investigator's Permission to Post Information Publicly. Recipient investigator agrees to permit DoD and NTI to summarize on the NTRR website the recipient investigator's research use of NTRR along with the recipient investigator's name and organizational/institutional affiliation.

12. Privacy Act Notification. In order to access the NTRR, the recipient investigator agrees to provide the information requested below.

The recipient investigator 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 investigator comes from the authorities regarding the establishment of NTI, 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. These records will be maintained in accordance with the Privacy Act System of Record Notice 09-25-0156 (http://oma.od.nih.gov/ms/privacy/pa-files/0156.htm) 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 NTRR Informatics 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 and NTI records. DoD and The Federal Privacy Act protects the confidentiality of the Recipient's DoD and NTI records. DoD and NTI 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. Also, the Act allows the release of some information in the recipient investigator's records without his/her permission; for example, if it is required by members of Congress or other authorized individuals.

13. Security. Recipient acknowledges the expectations set forth by the attached "NTRR Information Security Best Practices" for the use and security of data.

14. Annual Update. The recipient will provide to admin@ntrr-nti.org an annual summary of research accomplishments from using NTRR and an updated biographical sketch or CV. Future access to NTRR will be contingent upon receiving the annual update.

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

17. Termination. Either party may terminate this DUC without cause by providing 30 days written notice to the other party. Recipient investigator agrees to immediately report violations of NTRR Policy to NTRR via email to admin@ntrr-nti.org. Additionally, DoD and NTI may terminate this agreement with five days written notice if the DoD and NTI determine, in their sole discretion, that the recipient investigator has committed a material breach of this DUC. DoD and NTI may, in their sole discretion, provide recipient investigator with 30 day-notice to remedy a breach before termination. Upon termination of the DUC, use of the data must be discontinued. Closed accounts may be reactivated upon submission of an updated Access Request and DUC.

18. One Year Term and Access Period. Accounts with active grants are valid for one year and will be renewed annually by the NTRR operations team. Accounts that remain inactive for 12 consecutive months may be closed at the discretion of the NTRR staff.

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

NTRR 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 NTRR to submit, access, and analyze data. Keeping NTRR information secure through these best practices is important. Subject to applicable law, recipient investigators agree to immediately report breaches of data confidentiality to the NTRR Data Use Committee at admin@ntrr-nti.org.

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, NTRR Information Security Best Practices and all existing policies and procedures relevant to the use of NTRR, including but not limited to, the NTRR policy at the NTRR website.
- Follow the NTRR password policy which includes:
    - Choose passwords of at least seven characters including at least three of the following types of characters: capital letters, lower case letters, numeric characters and other special characters.
    - Change your passwords every six months.
    - Protect your NTRR password from access by other individuals—for example, store it electronically in a secure location.
- Notify NTRR staff, as permitted by law, at admin@ntrr-nti.org of security incidents, or any incidents of suspected fraud, waste or misuse of NTRR or when access to NTRR is no longer required.

Security Standards

- Protect the data, providing access solely to authorized researchers permitted access to such data by your institution or to others as required by law.
- Store NTRR data on a secured computer or server with strong password protection with the latest security patches and 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. 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 and as specified in the data use agreement.

By signing and dating this Data Access Request and Certifications as part of requesting access to data in NTRR, I certify that I will abide by the certifications, policies and procedures for the use of the NTRR. I further acknowledge that I have shared this document and the NTRR policies and procedures with any research staff who will participate in the use of NTRR data for this study.

X_____

Signature:_____ Date: _____

FDP Data Transfer and Use Agreement Project Glossary of Terms

A

Accounting of Disclosures
This provision of the Privacy Rule gives individuals the right to receive a list of certain disclosures that a covered entity has made of their protected health information in the past 6 years, including disclosures made for research purposes. (AOD) This term is specific to data use agreements covering protected health information.[1]

Aggregate Data
Aggregate Data is data that has been gathered, processed and expressed in a summary or report form for reporting purposes such as making comparisons, predicting trends or other statistical analyses. Aggregate data is collected from multiple sources and/or measures, variables or individual human subjects. Since aggregate data is the consolidation of data from multiple sources, it is typically not able to be traced back to a specific human subject.

Authorization
When referring to a study participant an individual's written permission to allow a covered entity to use or disclose specified protected health information (PHI) for a particular purpose. Authorization states how, why, and to whom the PHI will be used and/or disclosed for research, and seeks permission for that use or disclosure.[2] This term in this context is specific to data use agreements covering protected health information. This term may also be used in the more general sense of permission, for instance an authorization by one party of the data use agreement to allow the other party to provide the data to additional third parties. Care should be taken to establish the appropriate context when using this term.

B

Business Associate
Per 45 CFR § 160.103[3], a person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of protected health information, such as data analysis, claims processing or administration, utilization review, and quality assurance reviews, or any other function or activity regulated by the HIPAA Administrative Simplification Rules[4], including the Privacy Rule. Business Associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves disclosure of protected health information by the covered entity or another business associate of the covered entity to that

---

[1] Accounting of Disclosures: http://www.ncbi.nlm.nih.gov/books/NBK9572/
[2] Authorization (NIH): http://www.ncbi.nlm.nih.gov/books/NBK9572/
[3] 45 CFR § 160.103 Definitions, Business Associates:
http://www.ecfr.gov/cgi-bin/textidx?SID=79ebd0f150de1f75940e9e91d731998a&mc=true&node=se45.1.160_1103&rgn=div8
[4] HIPAA Administrative Simplification Rules: http://www.hhs.gov/hipaa/for-professionals/other-administration-simplification-rules/index.html

person or entity.[5] Special attention should be paid to the term "on behalf of" in the definition. Academic Institutions are rarely Business Associates since the term is not applicable to collaborative relationships.

Business Associate Agreement (or Business Associate Contract)
An agreement that contractually defines the rights and responsibilities between a covered entity and a Business Associate that would not otherwise be bound by HIPAA. A covered entity's contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e)[6]. For example, the contract must: Describe the permitted and required uses of protected health information by the business associate; Provided that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract. Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).[7] A Business Associate Agreement or Contract is not appropriate when a covered entity is disclosing PHI to another entity for use in a research project.

C

Classified Information
Per FAR clause 2.101, "Classified information" means any knowledge that can be communicated or any documentary material, regardless of its physical form or characteristics, that: (1) is owned by, is produced by or for, or is under the control of the United States Government or has been classified by the Department of Energy as privately generated restricted data following the procedures in 10 CFR 1045.21[8]; and (2) Must be protected against unauthorized disclosure according to Executive Order 12958[9], Classified National Security Information, April 17, 1995[10], or classified in accordance with the Atomic Energy Act of 1954[11]. See also Data Classification.

Clinical Study
A research study using human subjects or data from living human subjects to evaluate the effect of interventions or exposures on biomedical or health-related outcomes. Two types of clinical studies are interventional studies (or clinical trials) and observational studies.

---

[5] http://www.ncbi.nlm.nih.gov/books/NBK9572/

[6] 45 CFR 164.504(e): Uses and disclosures: Organizational requirements: http://www.ecfr.gov/cgi-bin/text-idx?SID=938e08839465e82e2c30c3bd4a359ce2&node=pt45.1.164&rgn=div5%23se45.1.164_1402#se45.1.164_1504

[7] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

[8] 10 CFR 1045.21 Privately Generated Restricted Data: https://www.gpo.gov/fdsys/granule/CFR-1999-title10-vol4/CFR-1999-title10-vol4-sec1045-21

[9] Executive Order 12958: 32 CFR 701.23 https://www.law.cornell.edu/cfr/text/32/701.23

[10] Classified National Security Information, April 17, 1995: Executive Order 13526 https://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information

[11] Atomic Energy Act of 1954: Nuclear Regulatory Legislation, 109th Congress: Session NUREG-0980 Vol. 1, Mo. 7. Office of the General Counsel, U.S. Nuclear Regulatory Commission: http://science.energy.gov/~/media/bes/pdf/nureg_0980_v1_no7_june2005.pdf

Code of Federal Regulations (CFR)
A codification of the general and permanent rules published in the Federal Register by the Executive departments and agencies of the Federal Government in the United States.

- 21 CFR Part 50 Protection of Human Subjects[12]
- 21 CFR Part 54 Financial Disclosure by Clinical Investigators[13]
- 21 CFR Part 56 Institutional Review Boards[14]
- 21 CFR Part 312 Investigational New Drug Application[15]
- 21 CFR Part 314 Applications for FDA Approval to Market an New Drug or an Antibiotic[16]
- 21 CFR Part 320 Bioavailability and Bioequivalence Requirements[17]
- 45 CFR Part 46 Protection of Human Subjects (Common Rule)[18]

Coded Data
See Data Classification

Common Rule
The federal rule that governs most federally funded research conducted on living human subjects and aims to ensure that the rights of human subjects are protected during the course of a research project, historically focusing on protection from physical and mental harm by stressing autonomy and consent.[19]

Competent Authorities
See Regulatory Authorities

Confidentiality
When referring to a study participant addresses the issue of how personal data that have been collected for one approved person may be held and used by the organization that collected the data, what other secondary or further uses may be made of the data, and when the permission of the individual is required for such uses.[20] This term in this context is specific to data use agreements covering protected health information. This term may also be used in the more general sense of limiting access, for instance the providing party of the data use might want to stress the confidentiality of data relating to a pending patent request. Care should be taken to establish the appropriate context when using this term.

Confidential Disclosure Agreements
See Non-Disclosure Agreement

---

[12] 21 CFR Part 50: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=50
[13] 21 CFR Part 54: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=54
[14] 21 CFR Part 56: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=56
[15] 21 CFR Part 312: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRsearch.cfm?CFRPart=312
[16] 21 CFR Part 314: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRsearch.cfm?CFRPart=314
[17] 21 CFR Part 320: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRsearch.cfm?CFRPart=320
[18] 45 CFR Part 46: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRsearch.cfm?CFRPart=46
[19] Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule; Nass SJ, Levit LA, Gostin LO, editors. Washington (DC): National Academies Press (US); 2009. http/www.ncbi.nlm.nih.gov/books/NBK9572/
[20] IBID., http://www.ncbi.nlm.nih.gov/books/NBK9572/

Covered Entity
Per 45 CFR § 160.103[21], A health plan, a health care clearinghouse, or a health care provider that transmits health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services has adopted a standard.[22] Note: This term is specific to data use agreements covering protected health information (PHI).

D

Data Breach

- General: unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal or other information maintained by the agency or institution

- HIPAA: an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information; an impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
    - the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
    - the unauthorized person who used the protected health information or to whom the disclosure was made;
    - whether the protected health information was actually acquired or viewed; and
    - the extent to which the risk to the protected health information has been mitigated.

Data Classification
Government or legal classifications for certain types of data and information. Government may elect through legislation or practice to codify certain groups of data by classifying them to facilitate consistent data management in accordance with government expectations and needs.

Data Classification, HIPAA:

HIPAA (defined under H) requires entities performing a covered function to identify and classify data based on these identifiers:

1. names (including initials),
2. geographic location smaller than a state (i.e. address),
3. any dates specific to an individual except year (i.e. date of birth, hospital admission and discharge dates, date of death, et cetera) and for those over 89 must aggregate into a single category of age 90 or older any year that might be indicative of age;
4. telephone numbers;
5. fax numbers;

[21] 45 CFR § 160.103 Summary: http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
[22] Nass SJ, Levit LA, Gostin LO, editors The HIPAA Privacy Rule;: http://www.ncbi.nlm.nih.gov/books/NBK9572/

6. e-mail addresses;
7. social security number;
8. medical record number;
9. health plan number;
10. account numbers of any kind;
11. certificate or license number(s);
12. Vehicle identifiers and serial numbers, including license plates;
13. device identifiers and/or serial numbers;
14. web URLs;
15. IP addresses,
16. biometric identifiers,
17. photographic images; and
18. any other unique identifier.

- **De-Identified Data**
  Data are considered de identified if the covered entity removes 18 specified personal identifiers from the data.[23]

- **Limited Dataset (LDS)**
  Protected Health Information that excludes the following direct identifiers of the patient or of relatives, employers, or household members of the patient: Names; Postal address information, other than town or city, State, and zip code; Telephone numbers; Fax numbers; Electronic mail addresses; Social security numbers; Medical record numbers; Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; Biometric identifiers, including finger and voice prints; Full face photographic images and any comparable images; and Any other unique identifying number, characteristic, or code except as specifically permitted by HIPAA.

- **Full Personal Health Information (PHI)**
  Contains identifiers that could be linked to a specific individual, such as initials or address. See list above

- **Coded Data**
  Data that has: 1) identifying information (such as name or social security number) that would enable the investigator to readily ascertain the identity of the individual to whom the private information or specimens pertains has been replaced with a number, letter, symbol, or combination thereof (i.e., the code); and 2) a key to decipher the code exists, enabling linkage of the identifying information to the private information or specimens. Coded data may constitute a limited data set, as further defined above. Office of Health Policy Research (OHPR) considers private information or specimens not to be individually identifiable when they cannot be linked to specific individuals by the investigator(s) either directly or indirectly through coding systems.[24]

---

[23] IBID., Full Personal Health Information (PHI): http://www.ncbi.nlm.nih.gov/books/NBK9572/

[24] Coded Data for further guidance, see the OHRP website. (https://irb.research.chop.edu/hipaa-glossary and http://www.hhs.gov/ohrp/policy/cdebiol.html

Data Classification, Government Designations:

- **Controlled Unclassified Information (CUI)**
  Information that is not classified, but has been marked by as a federal agency as requiring safeguarding or dissemination controls pursuant to and consistent with applicable law[25], regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.[26]

- **Sensitive but Unclassified (SBU)**
  Means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy[27]32 CFR 149.3.

- **Controlled Technical**
  Technical information with military, intelligence, or space applications that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure or dissemination. This could include information that is transferred out of the U.S. or within the U.S. to a foreign person ("deemed export"). Export-Controlled Information is mainly controlled under the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR).

- **Classified Information**
  Data under Executive Order 13526 of Dec 29, 2009[28] or the Atomic Energy Act[29], as amended, or any predecessor or successor orders that require protection against unauthorized disclosure and is marked to indicate its classified status when in document form.

- **Public Use**
  Data in the public domain; no regulatory prescription for its use.

Data Coordinating Center
In a multi-site study, the center responsible for overall data management, monitoring and communication among all sites including general oversight of the conduct of a human subjects research project.

---

[25] https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information
[26] https://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf
[27]32 CFR 149.3: Data Elements: https://www.gpo.gov/fdsys/granule/CFR-2011-title19-vol2/CFR-2011-title19-vol2-sec149-3

[28] Executive Order 13526 of Dec 29, 2009: https://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information
[29] Atomic Energy Act 1954: https://en.wikipedia.org/wiki/Atomic_Energy_Act_of_1954 See also; US Environmental Protection Act 45 USC section 2011: https://www.epa.gov/laws-regulations/summary-atomic-energy-act

Data Security
Protecting data and databases from destructive forces, the unwanted access or actions of unauthorized users, and corruption. Data security entails assessing the data and establishing means to assure that privacy and confidentiality, integrity, and availability of data are protected. Data Security also entails protecting data and databases from malicious intentions, unintentional loss, theft, or destruction. Data Security is of critical importance for health care records. Data Security entails risk assessment relevant to the type of data.

Data Security includes physical precautions such as: copying the original dataset only once and storing the original physical iteration such as CD ROM in a locked drawer or file cabinet; saving the computer programs used to construct analysis data files, but not Data Files themselves; retrieving paper printouts immediately upon output; shredding printouts no longer in use; password protecting data; signing pledges of confidentiality; and using the data solely for statistical reporting and analysis. Data Security also includes technical precautions such as: centralized authentication systems, firewalls, password management, et cetera.

Data providers often mandate specific data security measures governing access to their data. Data Security is also referred to as Information Security.

Data Transfer and Use Agreement (DTUA)
The template agreement developed by the Federal Demonstration Partnership (FDP) to standardize terms for the transfer of data from one entity to another. The DTUA Template includes a Face Page, Attachment 1 (project specific information), Attachment 2 (selected based upon the type of data being transferred), and Attachment 3 (Third Party Collaborator information).

Data Use Agreement (DUA)
A contractual agreement used to define how access to and/or exchanged data may be used. The primary consideration is the protection of protected health data (PHI) in accordance with HIPAA Regulations found at 45 CFR Part 160-164)[30]. However, DUAs can be used in other situations where the exchange of data is necessary and the agreement should be modified accordingly.
The DUA details:

- Permitted use(s) and disclosure of the data, primarily through publication of research results of the provided data and sets forth the data recipient's responsibilities with respect to them.
- Establishes a term for the use of the provided data and conditions which would be considered to breach the agreement.

A DUA should always be put in place when: the data to be transferred is from human subjects; and or the Data to be transferred is HIPAA protected. Please note that if the data to be provided is completely de-identified and there is no means to re-identify, a DUA is not needed. To meet this qualification the data must be stripped of the data elements cited above in personally identifiable information. If the data contains any of these identifiers then a DUA must be in place. DUA's must also be in place if sponsored funding was involved and there are data ownership and/or dissemination requirements.

[30] 45 CFR Part 160-164: http://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Data Use Committee
No standard federal definition exists for this term. In general used to describe a committee whose primary function is to review and either approve, disapprove or request modifications for the use of data. The term may be used synonymously with the term Privacy Board (see Privacy Board definition.) It may be also be used to describe boards that control access to data repositories whether or not those repositories contain protected health information.

E

F

Fair Credit Reporting Act
The Fair Credit Reporting Act (FCRA) is a federal law that regulates how consumer reporting agencies use personal information. In many ways, the FCRA is designed to help consumers understand their rights.[31]

Fair Information Practices (and Fair Information Practices Principles)
Guidelines developed by the FTC that focus on individuals' right to control the collection, use, and disclosure of information, and imposing affirmative responsibilities to safeguard information on those who collect it. Core principles include: notice/awareness; choice/consent; access/participation; integrity/security; enforcement/redress.[32]

Family Educational Rights and Privacy Act (FERPA)
The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.[33]

Federal Acquisition Regulations (FAR)
The Federal Acquisition Regulations System is established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies. The Federal Acquisition Regulations System consists of the Federal Acquisition Regulation (FAR), which is the primary document, and agency acquisition regulations that implement or supplement the FAR.[34]

Federal Food, Drug and Cosmetic Act (1938)
http://www.fda.gov/AboutFDA/WhatWeDo/History/ProductRegulation/ucm132818.htm[35]
Legislation passed in the United States in 1938 to specifically give authority to the Food and Drug Administration to oversee the safety of food, drugs, and cosmetics. Under this legislation manufacturers

---

[31] Fair Credit Reporting Act: https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf
[32] Fair Information Practices: https://web.archive.org/web/20090205180646/http://ftc.gov:80/reports/privacy3/fairinfo.shtm
[33] https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
[34] Federal Acquisition Regulation (FAR): www.acquisition.gov
[35] Federal Food, Drug and Cosmetic Act (1938) http://www.fda.gov/AboutFDA/WhatWeDo/History/ProductRegulation/ucm132818.htm

were required to test drugs for safety and present the evidence of safety testing to the FDA prior to marketing.

Federal Information Security Management Act of 2002 ("**FISMA**")
Provides information security standards for resources that support federal operations and assets.[36]

Federal Register[i]
The official daily publication in the United States for federal rules, proposed rules, and notices of federal agencies and organizations, as well as Executive Orders and Presidential Documents.

Federal Trade Commission (FTC)
An independent agency of the United States government[37], established in 1914 by the Federal Trade Commission Act [38], which has responsibility for advancing competition and protecting consumers.[39]

Food and Drug Administration (FDA)
An agency of the U.S. government in the Department of Health and Human Services with the primary purpose of protecting citizens against harmful, unsanitary, or falsely labeled foods, drugs, cosmetics, or therapeutic devices; responsible for the approval of all new drugs and for the final product labeling; also responsible for reviewing safety data for marketed drugs. **Food and Drug Administration Amendments Act, Section 801 (FDAAA 801)**[40]: Section 801 of U.S. Public Law 110-85, enacted on September 27, 2007, which amends Section 402 of the U.S. Public Health Service Act to expand the clinical study registry known as ClinicalTrials.gov and create a clinical study results database.[41]

Foreign Corrupt Practices Act
The Foreign Corrupt Practices Act of 1977 (amended 1988 and 1998) contains rules prohibiting bribery of foreign officials.[42]

G

---

[36] Federal Information Security Management Act of 2002 ("FISMA")
https://www.law.cornell.edu/uscode/text/44/3541
[37] Federal Trade Commission:
https://en.wikipedia.org/wiki/Independent_agencies_of_the_United_States_government
[38] The Federal Trade Commission (FTC) of 1914:
https://en.wikipedia.org/wiki/Federal_Trade_Commission_Act_of_1914
[39] The Federal Trade Commission (FTC): https://www.ftc.gov/
[40] Food and Drug Administration Amendments Act, Section 801 (FDAAA 801):
http://www.fda.gov/RegulatoryInformation/Legislation/SignificantAmendmentstotheFDCAct/FoodandDrugAdministrationAmendmentsActof2007/ucm095442.htm
[41] Clinical Trials.Gov, legislation: https://clinicaltrials.gov/ct2/manage-recs/fdaaa
See also: https://www.gpo.gov/fdsys/pkg/PLAW-110publ85/pdf/PLAW-110publ85.pdf#page=82
[42] Foreign Corrupt Practices Act of 1977 (amended 1988 and 1998:
https://www.law.cornell.edu/uscode/text/15/78dd-1

H

Health Care Clearinghouse[43]
A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and value-added networks and switches, that either process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or receive a standard transaction from another entity and process or facilitate the processing of health information into a nonstandard format or nonstandard data content for the receiving entity.

Health Care Provider
A provider of services as defined in Section 1861(u) of HIPAA, 42 U.S.C. 1395x(u)[44], a provider of medical or health services (as defined in Section 1861(s) of HIPAA, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.[45]

Health Information
Any information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.[46]

Health Insurance Portability and Accountability Act of 1996
An Act that requires, among other things, under the Administrative Simplification subtitle, the adoption of standards for protecting the privacy and security of personally identifiable health information. (HIPAA)[47]

Human Subject
Means a living individual about whom an investigator (whether professional or student) conducting research obtains

- data through intervention or interaction with the individual, or
- identifiable private information

Human Subjects Review Board
See Institutional Review Boards

---

[43] Health Care Clearinghouse: 42 U.S. Code section 1320d Definitions: https://www.law.cornell.edu/uscode/text/42/1320d
[44] See: HIPAA.Com http://www.hipaa.com/about/
And 1861(u) of HIPAA, 42 U.S.C. 1395x(u) http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php
[45] IBID http://www.ncbi.nlm.nih.gov/books/NBK9572/
[46] IBID http://www.ncbi.nlm.nih.gov/books/NBK9572/
[47] IBID http://www.ncbi.nlm.nih.gov/books/NBK9572/

Hybrid Entity
A single legal entity that is a covered entity, performs business activities that include both covered and non-covered functions, and designates its health care components as provided in the Privacy Rule. If a covered entity is a hybrid entity, the Privacy Rule generally applies only to its designated health care components. However, non-health care components of a hybrid entity may be business associates of one or more of its health care components, depending on the nature of the relationship.[48]

I

Information Security
See Data Security

Informed Consent Form
Federal regulations require that researchers obtain legally effective, documented, voluntary informed consent from prospective subjects (or subjects' legally authorized representatives) before subjects may be included in research. This consent is often documented on an Informed Consent form.
The primary purpose of informed consent is to protect the prospective human subjects. Informed consent provides the individual with the pertinent information regarding the research in which they are being asked to participate, and the opportunity to make an informed decision regarding whether or not to participate in the research.

Obtaining informed consent is a continuous process throughout the research, not simply a one-time event when a subject signs a form; therefore, a consent form may represent consent only at a particular time.

The content of the informed consent form may include information regarding permissible and impermissible of uses of subject data collected during the course of the research project.

Institutional Review Board (IRB)
An administrative body established to protect the rights and welfare of human research subjects recruited to participate in research activities conducted under the auspices of the institution with it is affiliated or for whom it is acting. The IRB has the authority to approve, require modification in, or disapprove all research activities that fall within its jurisdiction as specified by both the federal regulations and local institutional policy"[49]).

Investigator
See Principal Investigator

J

K

[48] IBID., http://www.ncbi.nlm.nih.gov/books/NBK9572/
[49] Department of Health and Human Services IRB Guidebook: http://archive.hhs.gov/ohrp/irb/irb_preface.htm

L

Limited Dataset
See Data Classification

Linked Data: a method of exposing, sharing, and connecting data from different sources, or (sometimes) the data itself that is connected or aggregated so as to access or provide more data information. In health care context, Personally Identifiable Information (PII) that is connected (linked) to certain health records that could compromise individual security must be either specifically protected or de-identified (e.g., break the link). Sometimes used to describe data that was not previously linked but now is or may be linked by an identifying key or other method.

M

Material Transfer Agreement (MTA):
A contract, generally without funding, which provides a legal framework to govern the exchange of research materials between academic, government, and commercial organizations. The types of materials transferred under MTAs may include anything from software to cell lines, cultures, plasmids, nucleotides, proteins, bacteria, pharmaceuticals, chemicals, and other proprietary physical materials and transgenic animals. MTAs are important because they delineate the rights, obligations, and restrictions of both the providing and receiving scientists with respect to issues such as:

- Ownership of materials and modifications or derivatives of the materials made by the recipient;
- Limits on the recipient's use of the materials and related liability;
- Provisions governing the return or disposal of the materials at the conclusion of the agreement;
- Restrictions on the recipient's ability to transfer the material, modifications, and derivatives to third parties;
- Rights to inventions resulting from the use of the materials;
- Rights to publish research obtained through the use of the materials;
- Reporting and confidentiality obligations.

See also UBMTA

Note: It is possible that a project could require both a DUA and an MTA. If the institution allows, the terms can be combined into a single agreement. If this is done, please ensure terms covering both types of transfers are included.

Metadata
Metadata is data that describes other data. Meta is a prefix that in most information technology usages means "an underlying definition or description."
Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier. And add footnote http://whatis.techtarget.com/definition/metadataThere are many metadata standards to choose from which are subject driven. One example is the DDI Data

Document Initiative,[50] designed to document numeric data files used in the social and behavioral sciences. When thinking about collecting data the Investigator should consider developing a hierarchy that will allow them to sort the data into its most meaningful categories. Some common metadata categories are listed below.

- Subject:
- Description
- Contributor
- Data
- Type
- Format
- Identifier
- Relation
- Coverage
- Rights: funder, owner

Misconduct

Means fabrication, falsification or plagiarism in proposing, performing, or reviewing research, or in reporting research results. *Fabrication* is making up data or results and recording or reporting them. *Falsification* is manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record. *Plagiarism* is the appropriation of another person's ideas, processes, results, or words without giving appropriate credit.[51] Central to the review and evaluation of allegations of research misconduct due to fabrication or falsification of data is the ability to have access to the original data from the research. IHE's share with their research investigators the responsibility for ensuring that research records are accessible and complete. The research data for any project must be kept for a period of 5 years beyond the end of the project. Unavailable, incomplete, or inaccurate research data is frequently cited in findings of research misconduct. Research investigators also share with the IHE the responsibility for ensuring the integrity and objectivity of research conducted at their institution. Accordingly, proper data management is critical.

N

Non-Disclosure Agreement

Non-Disclosure Agreements (NDAs) have many titles: Confidentiality Agreements, Proprietary Information Agreements, Secrecy Agreements, and the like. No matter its title, an NDA is a binding contract, commonly used when two or more parties wish to enter into discussions about specific confidential processes, methods or technology, to consider a potential, future or current relationship, and to agree to restrict the usage and additional disclosure of the shared information, knowledge, or materials. A non-disclosure agreement (NDA) is a signed formal agreement in which one party agrees to give a second party confidential information, such as about its technology, ongoing or planned projects, business or products, and the second party agrees not to share this information with anyone else for a specified period of time. Non-disclosure agreements are common in technology companies where

[50] DDI Data Document Initiative: http://www.ddialliance.org/

[51] Misconduct Definition, NIH: http://grants.nih.gov/grants/glossary.htm#ResearchMisconduct See also NSF: https://www.nsf.gov/oig/_pdf/cfr/45-CFR-689.pdf

products are sometimes jointly developed, and between universities and industry while exploring potential research partnership opportunities.

O

Open Access (OSTP Policy)[52]

In February 2013, the United States Office of Science and Technology Policy (OSTP) issued a Memorandum directing federal agencies with over $100M in annual R&D expenditures to develop plans to provide increased **public (a/k/a "open") access** to the results of federally funded research. The OSTP policy requires that grant recipients whose research results are published in peer-reviewed journals submit the final, accepted manuscript of such articles to the federal granting agency or a designated repository upon acceptance of the article for publication or the final published version if approved by the publisher. Articles are to be made freely, publicly available following an agency-determined embargo period, with agencies commonly calling for a 12-month embargo period. Agency public access plans, initially voluntary programs, are expected to be made mandatory for more and more agencies, eventually all agencies. Other major outside funding sources such as foundations have supported open access for their funded data generation in research.

P

Personal Data

Data which relate to a living person who can be identified from the data and other information that could potentially identify that person, it may be of a financial or medical nature or be the person's name, address or social security number. If medical in nature the information may need to be treated in accordance with HIPAA. When such data is used in as research data special protections must be in place to protect the individual's' identity

Personally Identifiable Information (PII) (See also Data Classification: HIPAA)

Any information maintained by an agency, including: (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[53] When allowing access to PII care should be taken that the data or combination of data elements when linked (i.e. taken in combination) do not allow the individual to be distinguished or traced.

Examples of PII Data

Name:(full name, maiden name, mother's maiden name or alias

Personal identification number: social security number (SSN) passport number, driver's licenses number, taxpayer identification number, patient identification number, and financial account or credit card number(s).

---

[52] Open Access Policy: NIH http://publicaccess.nih.gov/faq.htm NSF https://www.nsf.gov/oig/_pdf/cfr/45-CFR-689.pdf

[53] Even of an organization determines that the information is not PII, the organization should still consider whether the information is sensitive or has organizational or individual risks associated with it and determine the appropriate protections. NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information PII* :(April 2101). P. 2-1.

Address: street address, e-mail address, zip code.
Asset information: such as an internet protocol number (IP address); or Media Access Control (MAC) number.
Telephone numbers
Personal characteristics: photographic images (especially of the face), x-rays, finger prints, or other biometric image (i.e. retina scan, facial geometry et cetera).
Information identifying personally owned property
Information about an individual that is linked or linkable to a. through g. above.

Principal Investigator (PI)
The individual officially responsible for the conduct of a sponsored project, or the individual officially responsible for the conduct of any research project. On research projects the PI is usually a faculty member; on other types of awards, the PI may have an administrative appointment. The PI is always an investigator. **Investigator**[54] is defined within the NIH conflict of interest regulations as the principal investigator and any other person, regardless of their position or title, who is responsible for the design conduct, or reporting of a sponsored research award or proposal for such funding.

Privacy
The collection of PII and overall privacy of information are of concern to both the individual and the organization collecting the data. Treatment of PII is distinct as it needs to be collected, maintained, used, retained (stored) and destroyed in accordance with Federal Privacy Act of 1974 [55](applicable only to federal agencies this Act forms the statutory basis for Fair Information Practices ; as well as other federal laws and regulations. Privacy requires the adoption of internal policies and procedures which ensure that the data is kept secure and used for the purposes for which it was collected. Privacy requires that the individual who provides data is aware of their rights. Also see PII and Personal Data.

Privacy Board
A board that is established to review and approve requests for waivers or alterations of authorization in connection with a use or disclosure of protected health information as an alternative to obtaining such waivers or alterations from an Institutional Review Board. A Privacy Board consists of members with varying backgrounds and appropriate professional competencies as necessary to review the effect of the research protocol on an individual's privacy rights and related interests. The board must include at least one member who is not affiliated with the covered entity, is not affiliated with any entity conducting or sponsoring the research, and is not related to any person who is affiliated with any such entities. A Privacy Board cannot have any member participating in a review of any project in which the member has a conflict of interest.[56]

Protocol
A document that describes the objective(s), design, methodology, statistical considerations, and organization of a study. The protocol usually also gives the background and rationale for the study, but these could be provided in other protocol-referenced documents. Within the context of clinical

[54] See the NIH Conflict of Interest Frequently Asked Questions (FAQ) at: http://grants.nih.gov/grants/policy/coifaq.htm#b1
[55] Federal Privacy Act of 1974, US Department of Justice: https://www.justice.gov/opcl/privacy-act-1974
[56] Privacy Board: http://www.ncbi.nlm.nih.gov/books/NBK9572

research, throughout the International Committee on Harmonization Good Clinical Practice, IHC GCP Guidelines[57], the term protocol refers to protocol and protocol amendments.

Protected Health Information (PHI)
See Data Classification

Public Access
See Open Access

Q

R

Record Retention
The period of time a document(s) should be kept or retained, whether in electronic format or physical format. Record Retention period usually depends on the record type and the business, legal and compliance requirements associated with the record. Record Retention periods may be determined by both federal and state law.

Regulatory Authorities
Bodies having the power to regulate. Within the context of clinical research, in the ICH GCP guideline, the expression "Regulatory Authorities" includes the authorities that review submitted clinical data and those that conduct inspections. These bodies are sometimes referred to as "competent authorities."

Research
A systematic investigation, study or experiment designed to develop or contribute to generalizable knowledge. The term encompasses basic and applied research (e.g., a published article, book, or book chapter) and product development (e.g., a diagnostic test or drug). The term includes any such activity for which sponsored funding is available such as a research grant, career development award, center grant, individual fellowship award, infrastructure award, institutional training grant, program project, research resources award, or other contractual mechanism.[58]

Research data
Research data is factual material commonly retained, collected, observed or created by and accepted in the scientific community as necessary to validate research findings regardless of the format in which it is created.

Re-identification
Re-identification is the process of attempting to discern the identities that have been removed from de-identified data.[59]

---

[57] IHC GCP Guidelines:
[58] Research and Development R&D NIH: http://grants.nih.gov/grants/glossary.htm#R
[59] Re-identification see National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

S

Security
The procedural and technical measures required (a) to prevent unauthorized access, modification, use, and dissemination of data stored or processed in a computer system, (b) to prevent any deliberate denial of service, and (c) to protect the system in its entirety from physical harm" (Turn and Ware, 1976)[60]

Sensitive Human Subjects Data
Information that is protected against unwarranted disclosure. Access to sensitive data should be safeguarded. Protection of sensitive data may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations. Sensitive Human Subjects Data includes all data, in its original and duplicate form, which contains:

- Personal Information, Protected Health Information, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[61]
- Student education records, as defined by the Family Educational Rights and Privacy Act (FERPA)[62]
- Customer record information, as defined by the Gramm Leach Bliley Act (GLBA)[63]
- Card holder data, as defined by the Payment Card Industry (PCI) Data Security Standard[64]
- Confidential personnel information, as defined by the State Personnel Act[65] is information that is deemed to be confidential in accordance with the individual State Identity Protection Acts or laws;

Sensitive Data
Any information that is protected by an entity's policy from unauthorized access. This information must be restricted to those with a legitimate business need for access. Examples of sensitive information may include, but are not limited to, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, financial donor information, information concerning select agents, system access passwords, information security records, and information file encryption keys.

Summary Data
See Aggregate Data

---

[60] Turn R, Ware WH. The RAND Paper Series. Santa Monica, CA: The RAND Corporation; 1976. Privacy and security issues in information systems: http://www.ncbi.nlm.nih.gov/books/NBK9572/
[61] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/
[62] Family Educational Rights and Privacy Act (FERPA) http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
[63] Gramm Leach Bliley Act (GLBA) https://www.ftc.gov/tips-advice/business-center/guidance/brief-financial-privacy-requirements-gramm-leach-bliley-act
[64] Payment Card Industry (PCI) Data Security Standard https://www.pcisecuritystandards.org/pci_security/
[65] State Personnel Act http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_126.html

T

U

Universal Identifier (UID) Is a specific numeric, or alphanumeric code used to refers to a specific individual or enitiy.in the case of Coded Data Each assigned UID in a data set is associated with a single entity or individual. The use of UIDs make it possible to address the data pertaining to an individual so that it can be accessed and interacted without disclosing the individuals identity . Examples of UIDs include:

- A Uniform Resource Identifier (URI) is a unique identifier that makes content addressable on the Internet by uniquely targeting items, such as text, video, images and applications.
- A Uniform Resource Locator (URL) is a particular type of URI that targets Web pages so that when a browser requests them, they can be found and served to users. A Universal Unique Identifier (UUID) is a 128-bit number used to uniquely identify some object or entity on the Internet.
- A global unique identifier (GUID) is a number that Microsoft programming generates to create a unique identity for an entity such as a Word document.
- A bank identifier code (BIC) is a unique identifier for a specific financial institution.
- A unique device identifier (UDID) is a 40-character string assigned to certain Apple devices including the iPhone, iPad, and iPod Touch.
- A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN).
- A national provider identifier (NPI) is a unique ten-digit identification number required by HIPAA for all health care providers in the United States.

In order for a data set to be considered a limited data set, some UIDs, such URLs, must be removed.

V

Vulnerable populations
Generally include the economically disadvantaged, racial and ethnic minorities, the uninsured, low income children, the elderly, the homeless, those with human immunodeficiency virus (HIV), prisoners and those with other chronic health conditions, including mental illness.[66]

Waiver of Authorization
The documentation that the covered entity obtains from a researcher or an IRB or a Privacy Board that states that the IRB or Privacy Board has waived or altered the Privacy Rule's requirement that an individual must authorize a covered entity to use or disclose the individual's protected health information for research purposes.[67]

---

[66] Vulnerable Population Health and Human Services, Office of Health Research Protection: http://www.hhs.gov/ohrp/regulations-and-policy/guidance/vulnerable-populations/index.html
[67] Waiver of Authorization: http://www.ncbi.nlm.nih.gov/books/NBK9572/

FDP DTUA Guidance Chart

This chart is designed to provide some guidance on when and how to use the FDP Data Transfer and Use Agreement (DTUA) Template.
Remember to also check your institutional policies and procedures, as these may vary based on institution type (i.e. hospital versus university).

I must have a DTUA when…	I may need a DTUA when….	I may not need a stand-alone DTUA when…
Transferring (including receiving) Human Subject data that includes at least one of the 18 HIPAA identifiers and no other agreement governs the transfer and use: • Personal Health Information (PHI) • Personally Identifiable Information (PII) • Limited data set (LDS) HIPAA identifies **18 key data points** that define the parameters for PHI, PII, LDS or de-identified data sets. Also see the DTUA Glossary for details.	My institution or PI may require a DTUA for transferring non-Human Subject data if no other agreement governs the transfer and use. Provider policy or preference drives requirement to include terms beyond what is strictly required by law, such as: • destruction terms; or • other use restrictions	The practice at my institution does not require a separate DTUA and another agreement exists where the data use terms can be inserted, such as: • Subaward; • Material Transfer Agreement; • Confidentiality agreement; • Collaboration Agreements (including unfunded MOUs); • Clinical trial agreement; or • Notice of award
Use the DTUA with Attachment 2 for with the PII or LDS, as applicable	**Use the DTUA with Attachment 1 for non-human subjects data**	**Incorporate appropriate language**
Transferring Human Subject data that is completely de-identified (e.g. contains no HIPAA identifiers) and no other agreement governs the transfer and use. Other data transfers required by applicable law. Please see the DTUA Glossary for a selected list of other data types and applicable laws (such as FERPA).	Provider policy or preference drives requirement to include terms beyond what is strictly required by law, such as: • Requirement to notify Provider if the data set erroneously includes identifiable information; • Requirements not to re-identify the data; • destruction terms; or • other use restrictions	You may need a Business Associate Agreement (BAA) for non-research or procurement activities. BAAs are typically not appropriate for research activities. See the DTUA Glossary for further information.
Use the DTUA with Attachment 2 for with the PII or LDS, as applicable	**Use the DTUA with Attachment 2 for de-identified human subjects data**	**See Resources for further guidance**

Resources

FDP Data Use Glossary, FDP Data Use Guidance and the DTUA Templates are located here.
If you need an FDP Subaward or contract template, visit here.

FDP Tool for Classifying Human Subjects Data

This chart is designed to streamline review of the type of human subject data for the purpose of classification for a DTUA.
Remember to also check your institutional policies and procedures for further guidance.

18 HIPAA Identifiers that comprise Personally Identifiable Information (PII)

PII may be used alone or with other sources to identify an individual. PII in conjunction with medical records (including payments for medical care) becomes Protected Health Information (PHI).

1. Name (including initials)
2. Address (all geographic subdivisions smaller than state: street address, city, county, zip code)
3. All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
4. Telephone numbers
5. Fax number
6. Email address
7. Social Security Number
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate or license number
12. Any vehicle identifiers, including license plate
13. Device identifiers and serial numbers
14. Web URL
15. Internet Protocol (IP) Address
16. Finger or voice print
17. Photographic image - Photographic images are not limited to images of the face
18. Any other characteristic that could uniquely identify the individual

A data set containing any of these identifiers, or parts of the identifier, is considered "identified"

HIPAA – Limited Data Set

A Limited Data Set must omit all of the HIPAA Identifiers in the left-hand column except for the following:

1. City, state, zip code
2. Dates of admission, discharge, service, date of birth, date of death
3. Ages in years, months or days or hours

To re-iterate: initials are always considered PHI/PII

HIPAA – De-identified Data

All of the 18 HIPAA Identifiers in the left-hand column must be removed in order for a data set to be considered de-identified with caveats for the following:

1. All geographic subdivisions smaller than a state, except for the initial three digits of the ZIP code: (1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000;
2. Ages in years and for those older than 89, all ages must be aggregated into a single category of 90 or older

FERPA – Personally Identifiable Information

In the context of FERPA, PII includes, but is not limited to:

1. Student's name
2. The name of the student's parent(s) or other family members
3. Address of the student or student's family
4. Student's personal identifiers, such as:
    a. Social Security Number;
    b. Student number; or
    c. Biometric record (i.e. Finger or voice print)
5. Student's other indirect identifiers, such as:
    a. Birthdate;
    b. Place of birth; or
    c. Mother's maiden name
6. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty
7. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates