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/