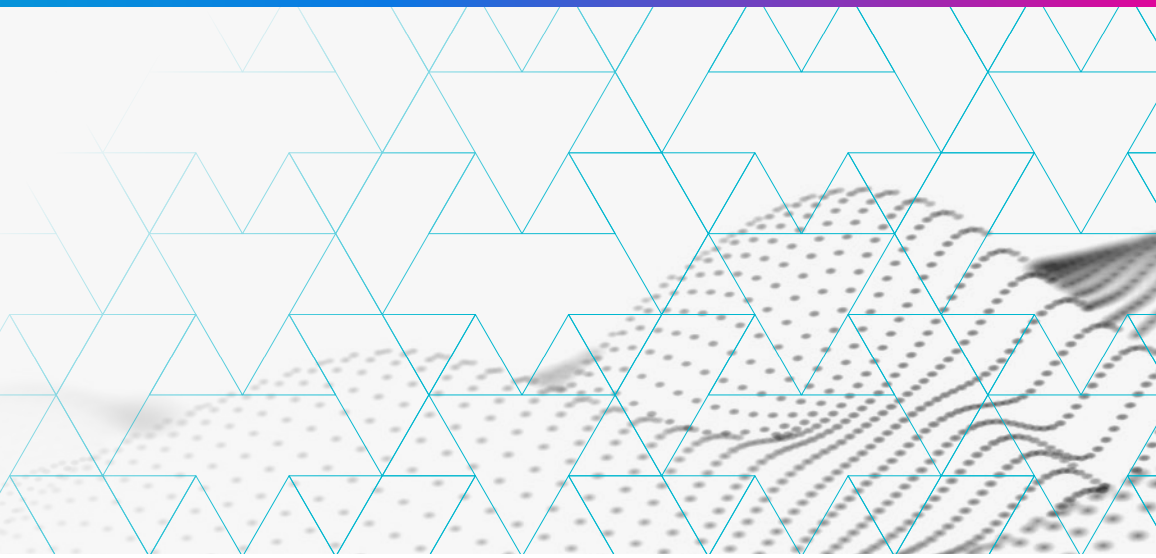
ADDI
Alzheimer's Disease
Data Initiative

Legal and Regulatory FAQs (non-GDPR)



These questions and answers are designed to assist researchers in understanding certain legal considerations that frequently arise when initiating and conducting a research project. This brief set of FAQs does not address all legal considerations involved in conducting a research project; each researcher should consult with his or her institution's own legal counsel before beginning any research project.

UPDATED NOVEMBER 2020

U.S. REGULATIONS

Common Rule

To what activities does the Common Rule apply?

The Common Rule applies to research involving human subjects that is conducted or supported by any of the 20 federal departments and agencies that have adopted (or intend to follow) the Common Rule. This includes, for example, research funded by the National Institutes of Health. In practice, many academic and health care institutions in the United States apply the Common Rule to all research that they conduct regardless of whether the research has federal support.

What are the Common Rule changes that took effect in January 2020?

Beginning January 20, 2020, the revised Common Rule requires single institutional review board (IRB) review for all U.S. sites in multi-site research subject to the Common Rule, unless more than single IRB review is required by law. These regulatory changes are designed to streamline the IRB review process for multi-site studies.

Must a research study involving secondary research comply with both the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Common Rule?

The revised Common Rule exempts from its requirements secondary research (i.e., research that involves the use of data collected during another primary or initial activity) that uses identifiable private information when that use is regulated under HIPAA as "research," "public health activities and purposes," or "health care operations." This exemption applies when the researchers are covered by HIPAA either because they are a HIPAA covered entity in their own right or because they are performing the research in their role as a member of the workforce of a HIPAA covered entity or business associate.Thus, such researchers will now be able to rely solely on compliance with HIPAA instead of being required to comply with both HIPAA and the Common Rule.

Am I required to adhere to the Common Rule if I did not receive federal funding to support my research?

It depends. The Common Rule itself applies only to human subject research "conducted, supported, or otherwise subject to regulation by" the U.S. Department of Health and Human Services and nineteen other federal departments and agencies that have jointly adopted (or intend to follow) the Common Rule. However, as noted above, many U.S.-based institutions have, as a matter of internal policy, determined to apply the Common Rule's protections to all research involving human subjects in which the institution is engaged.

HIPAA

To whom does HIPAA apply?

The HIPAA Privacy Rule applies to "covered entities," which are defined as (i) health care providers who transmit information in specific electronic formats in connection with financial or administrative activities related to health care (e.g. insurance claims submission), (ii) health plans, and (iii) health care clearinghouses). HIPAA also applies to "business associates," which are entities that use protected health information ("PHI") to perform certain functions or activities on behalf of a covered entity.

How do I know if HIPAA applies to my research activity?

Researchers who work for covered entities are subject to the HIPAA Privacy Rule with respect to their use and disclosure of PHI. In certain cases, researchers who work for entities that function as business associates may also be subject to the HIPAA Privacy Rule.

While researchers outside of covered entities and business associates are not subject to HIPAA with respect to their research activities, they must still comply with various state and federal laws affecting privacy and confidentiality. Also, many researchers who do not work for covered entities or business associates obtain PHI from covered entities as part of a research activity. Thus, all researchers should have a basic understanding of HIPAA.

If I am part of a covered entity's workforce, must I always receive a HIPAA authorization to share PHI?

No. Researchers who are part of a covered entity's workforce can share PHI for research without the data subject's authorization by obtaining a waiver of authorization from a cognizant IRB or a privacy board meeting HIPAA's requirements. Waivers of authorization are often obtained in secondary research when it would not be feasible to obtain the data subjects' authorizations. HIPAA also permits covered entities to disclose PHI for research purposes without authorization or a waiver of authorization if the data are considered a limited data set. More information on limited data sets is provided in the questions below. In addition, if the PHI has been de-identified, it is no longer subject to HIPAA's limitations on the use and disclosure of PHI. More information on de-identification is below.

How do I know if my data are considered a "limited data set" under HIPAA?

HIPAA defines a limited data set as a data set from which 16 enumerated direct identifiers (see list below) have been removed.

What constitutes a limited data set under HIPAA?

Information from which the following 16 identifiers have been removed:

- Names
- Postal address information (other than town, city, state and zip code)
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social Security numbers
- Medical records numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate and license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- URLs
- IP address numbers
- Biometric identifiers (including finger and voice prints)
- Full face photographic images (or comparable images)

Do state-based privacy laws or HIPAA take precedence when it comes to data sharing in the U.S.?

The general standard is that if a state law is more protective of the patient, then it takes precedence over HIPAA. If you have a question as to whether a specific state law or HIPAA provision applies in a particular case, you should seek legal counsel.

California Consumer Privacy Act of 2018 ("CCPA")

To whom does the CCPA apply?

The CCPA applies to "businesses" that are for-profit entities, collect California residents' personal information and meet certain other requirements (such as having annual revenues of at least $25 million, handling the personal information of at least 50,000 consumers, or deriving 50 percent or more of annual revenues from selling consumers' personal information).

How do I know if the CCPA applies to my research activity?

CCPA does not apply to research in many situations due to three important exceptions. First, as implied in the answer above, the CCPA does not apply to nonprofit entities. Second, CCPA also does not apply to PHI collected by a covered entity or business associate governed under HIPAA, and also carves out from its application HIPAA covered entities, with respect to their handling of patient information that they maintain in the same manner as PHI. Third, CCPA contains a recently-broadened exception that excludes personal information that is collected, used, or disclosed in "research," as defined in HIPAA,[1] provided that the research is conducted in accordance with HIPAA, the Common Rule, the International Council for Harmonisation Good Clinical Practice, or the U.S. Food & Drug Administration's human subject protection requirements. If none of these exceptions applies, then the CCPA may apply to the research activity.

Other

What is the difference between deidentification under HIPAA and anonymization under the European Union's General Data Protection Regulation ("GDPR")?

HIPAA provides that PHI can be deidentified under one of two methods:

(i) a "safe harbor" method under which 18 enumerated direct identifiers are removed. These include all those identifiers that must be removed from a limited data set, as listed above, as well as:

- (a) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code.[2]

- (b) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, and date of death.[3]

---

[1] HIPAA defines research as a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

[2] For a covered entity to include the initial three digits of zip code within the de-identified data set protected by the safe harbor, the geographic unit formed by combining all zip codes with the same three initial digits must contain more than 20,000 people according to the current publicly available data from the Bureau of the Census. If population for such geographic unit is 20,000 or fewer people, the initial three zip code digits must be changed to '000.'

[3] The covered entity must also remove all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of 'age 90 or older.'

(ii) a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable uses such principles and methods to determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient, to identify an individual who is a subject of the information and documents the methods and results of the analysis.

Notably, HIPAA permits a covered entity to assign a "reidentification" code to information that has been deidentified provided that the code is not derived from PHI and is not used or disclosed by the covered entity for any purpose other than reidentification.

GDPR requires that data be completely "anonymized" to fall outside its protections. GDPR only treats as anonymous that information that has been rendered in a manner such that the data subject is no longer identified or identifiable based on all the means reasonably likely to be used, either by the controller or another person to identify the natural person directly or indirectly. Whether data have been anonymized is a facts-and-circumstances test that can be difficult to meet. Critically, the GDPR is generally understood to treat pseudonymized information (such as key-coded data) as personal data, even in the hands of a person or entity that does not possess the key to reidentify the data subjects.

Should I abide by GDPR regulations on data sharing if I am a U.S. or U.K. researcher who wishes to share my research in a data repository that may be accessed by people in the EU?

As of the date of this guide, the United Kingdom has continued to apply the GDPR even following its departure from the European Union, and it is expected to continue to do so. Thus, United Kingdom-based researchers should abide by the GDPR with respect to any personal data they process (including when sharing such data with other researchers, whether located within or outside of the European Economic Area ("EEA"), i.e., the geographic region in which the GDPR applies).

In most cases, the GDPR would not technically apply to U.S.-based researchers who collect data from persons located in the United States. However, because researchers located in the EEA would need to have a lawful basis for processing personal data, even if the data subjects are located in the United States, EEA-based researchers may require that the U.S.-based researchers provide certain assurances that the data have been collected in conformity with certain requirements of the GDPR, such as following the provision of appropriate notice to the data subjects. If U.S.-based researchers anticipate sharing data with EEA-based researchers, the U.S.-based researchers should ask what type of notice the EEA-based researchers would like to furnish.

Note that, of course, HIPAA requirements will still also apply to U.S. researchers who are part of covered entities with respect to PHI they hold and seek to share.

[4] The European Economic Area ("EEA") includes the 27 member states of the European Union and three additional countries: Iceland, Liechtenstein and Norway.

What are the legal and regulatory differences in genetic data v. clinical research data?

Genetic data are those that contain a particular category of information (i.e., data about the genome), whereas clinical research data refer to the provenance of the data (i.e., data collected during a clinical research study). Genomic data may be collected or generated in the course of a clinical research study and thus considered "clinical research data." Alternatively, genomic data may be created in the course of clinical care and then used for research as a secondary purpose.

When genomic data are used in a research study, laws that apply to the clinical research study and its data apply equally to the subset of clinical research data that are genetic data. When genomic data are used by a HIPAA covered entity, they are generally subject to HIPAA as PHI unless they have been de-identified per the standard set forth above.

In addition to these bodies of law, there are certain unique legal requirements that apply to genetic data. For example, the Genetic Information Nondiscrimination Act prevents certain discrimination against persons by health insurers or employers based on the persons' genetic information. Additionally, many states have imposed their own requirements on the performance of genetic tests and the handling of genetic data. These requirements vary by state and should be reviewed with legal counsel before performing genetic testing on persons located in the applicable state or performing the genetic test in a particular state. (See the immediately following question's answer for more detail).

Are EU and U.S. privacy regulations for genetic data the same as those for other health data?

GDPR considers genetic data, as well as other data concerning health, to be "special categories of personal data" that are subject to additional requirements for processing given their sensitivity. Further, GDPR permits individual EEA member states to impose additional conditions, including limitations, with regard to the processing of genetic data and data concerning health, so it is possible that additional restrictions may emerge throughout the EEA in the future.

In the U.S., many state laws impose heightened protection on certain types of information used in research, including genetic data. For example, New York state requires the specific written informed consent of a person to whom genetic information relates for such information to be disclosed. Additionally, some states treat the results of DNA analysis as property of the person tested.

Why should I develop a data use agreement?

Data use agreements should be put in place when sharing data because they protect data subjects and researchers from future misuse of data or inappropriate data disclosures. Under HIPAA, if a covered entity discloses a limited data set to a researcher, the covered entity is required to enter a specific form of data use agreement with the recipient researcher.

CONSENT

Must I always have a written consent from U.S. participants to share their data?

Typically, yes. However, U.S. law permits IRBs to grant waivers of consent and, for data subject to HIPAA, waivers of HIPAA authorization. Moreover, when consent is relied upon for data sharing, it is important that the written consent clearly provide for the desired purposes of the data sharing with the desired recipients.

What can I do with data I already have if a participant in my U.S.-based study withdraws consent?

U.S. law provides that, upon a subject's withdrawal of consent, researchers must cease collecting additional data, but may continue to use subjects' personal data collected up to the point of withdrawal to satisfy certain legal requirements, such as to account for subjects' withdrawal from the research. If the research data have already been de-identified and shared, the recipients of the data generally can continue using such de-identified data.

How do I know if I can share data from existing studies whose informed consent was collected in the past?

The original informed consent form ("ICF") between the research participant and researcher must be reviewed to determine whether secondary research generally, and the secondary research and recipients specifically contemplated, would be permitted under the provisions of the original ICF.

IRBs

Do IRBs have to review and approve any and all data sharing in the U.S.?

No. In the U.S., mere data sharing for secondary research may occur in many cases without IRB review and approval, if requirements of applicable privacy laws have been satisfied. However, the data recipient who undertakes the secondary research using the shared data may be required to obtain IRB approval for his or her research.

Do I need to receive IRB/REC approval for secondary research in the U.S.?

If the project is not subject to the Common Rule (see questions and answers above), FDA Regulations governing human subjects research, or state laws governing human subjects research, IRB review and approval may not be legally mandated for the secondary research itself. Nevertheless, many institutions' policies and data sharing agreements require IRB review and approval of secondary research.