FPF Corporate Academic Data Stewardship Research Alliance
Contract Guidelines

The following document sets out guidelines, best practices, and sample language relevant to contracts between a company and a researcher for data sharing for academic / scientific research purposes.

The terms described and provided below are for informational purposes only. They may not be suitable for all contracts and may require modification as appropriate. Nothing in this document is intended to provide, nor should be construed as, legal advice. These guidelines are not a substitute for obtaining professional legal counsel from a qualified attorney on your specific matter.

These guidelines reflect the objectives and goals of the FPF Corporate Academic Data Stewardship Research Alliance, in particular enabling the responsible sharing of data in order to advance scientific research. For instance, the suggested terms reflect a preference toward allowing for and encouraging broad publication and disseminating of research results (while protecting privacy of individual research subjects), and favoring academic independence and freedom over potential commercial interests in tightly controlling research and publication. While such an approach is encouraged as a general matter, here too, the specific language may not be appropriate in all cases and may be modified.

The contract provisions described below assume a scenario in which the Data Supplier transfers personal data to one or more Researchers. They do not specifically address scenarios where a Researcher is given only limited on-site access or similar controlled access to data, or where data is made available through a third-party data exchange or data repository. Some (but not all) of the provisions below will nevertheless be applicable to such scenarios. And future versions of this document may specifically address those types of arrangements.

Topic	Description	Sample Language
Definitions	Define key terms (Personal Data, Covered Data, etc.)	"Covered Data" means all information provided or made available by Data Supplier under this Agreement for a Research Purpose. "Confidential Data" means any nonpublic Covered Data including information relating to Data Supplier's products, services, systems, policies, practices, technology, inventions, know-how, as wells as information about Data supplier's customers or users, employees, and business partners, including Personal Data. All Covered Data shall be presumed

Topic	Description	Sample Language
		to be Confidential Data unless (1) Data Supplier has designated such data otherwise in writing or (2) Researcher can demonstrate that such data is public and the public availability of such data is not the result of an act or omission by Researcher. "Personal Data" means any information, including public information, (i) relating to an identified or identifiable natural person or household; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; or (ii) that otherwise is regarded as personal data or personal information under applicable laws and regulations. "Research Group" means the group of institutions, including Researcher, that have been given access to Covered Data by Data Supplier for a common Research Purpose, and that are a party to this Agreement or have signed a substantially similar agreement with Data Supplier.
Scope & Purpose of Research	Specify the research purpose. The references to "scientific or historical research" and "designed to develop or contribute to generalizable knowledge" borrow language from GDPR and HIPAA respectively and are, in part, intended to help ensure the research fits with certain exceptions in those laws (and others).	Data Supplier will provide Covered Data to Researcher for the following specified Research Purpose(s): [*insert description of nature, scope, intent, and anticipated outcomes of research*]. The Research Purpose(s) shall be limited to scientific or historical research designed to develop or contribute to generalizable knowledge and to advance the public interest.
Basis for Personal Data Sharing and Use	Describe the basis / justification for provision of Personal Data. For example: • Is the data sharing authorized or consented to by the data subject?	Data Supplier warrants that it has the necessary authorization or permission required under applicable data protection law to provide the Covered Data to Researcher.

Topic	Description	Sample Language

for the Research Purpose	• Has the data sharing been reviewed and approved by an IRB or similar body?
	• For EU data, what is the lawful basis for sharing the data (e.g. consent of the data subject, "legitimate interests")?
	  ○ Where the Researcher is an EU government entity or acting under the authority of an EU government entity, the lawful basis of "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" might apply.
	  ○ There are other lawful bases available under EU law, but they are quite narrow and unlikely to apply to most research purposes.
	• For health data subject to the HIPAA Privacy Rule, is the sharing based on:
	  ○ the individual's authorization,
	  ○ an IRB waiver,
	  ○ meeting the HIPAA de-identification standard,
	  ○ being a limited data set (LDS) disclosed under a data use agreement (DUA)
	  ○ data being limited to decedents, or
	  ○ access for proposes that are preparatory to research?
		OPTIONAL: For Personal Data from the EU and other jurisdictions with similar requirements, the transfer and use for the Research Purpose of any Personal Data included within the Covered Data is based on [*insert description of lawful basis or bases for the sharing and use of the data such as consent of the data subject or "legitimate interests"*].
		
		OPTIONAL: For Personal Data that constitutes Protected Health Information (PHI) subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the use and disclosure of the data is based on: (*choose all that apply*)
		☐ the data being de-identified according to the standards set out in the Privacy Rule prior to disclosure
		☐ the individual's authorization
		☐ a waiver approved by an Institutional Review Board (IRB) or Privacy Board
		☐ the data constituting a limited data set disclosed pursuant to a data use agreement
		☐ the data being limited to PHI of decedents
		☐ the access to PHI being limited to purposes that are preparatory to research

Description of Covered Data	Briefly describe each data set to be shared. List the *types or categories* of data elements to be included. For any Personal Data, also describe the categories of data subjects (consumers, patients, employees, etc.). If the list of data is extensive or highly detailed, it may make sense to include it in a schedule or	The following Confidential Data will be made available to Researcher: The following non-Confidential Data will be made available to Researcher:

Topic	Description	Sample Language
	appendix. Note also that if EU model clauses are used, a description of Personal Data will be included in Annex B to the clauses.	
Data Usage	The data is to be used only for the research purpose and not for any other purposes. To the extent the research is subject to an IRB review, the approved protocols of the IRB must be followed.	Researcher will use Covered Data only for the specified Research Purpose(s). OPTIONAL: All use of Covered Data will be in accordance with the then-current protocol(s) as approved by any IRB(s) of record. Researcher will not use Covered Data, or any portion or derivative thereof, for any other purpose without the written authorization of Data Supplier.
Transfers to Third Parties	Prohibit unauthorized sharing of the data. The "except as permitted" language allows for sharing with service providers and as required by law per those other provisions of the Agreement.	Researcher will not sell, rent, share, distribute, or otherwise transfer any Confidential Data and Personal Data, to any third party for any purpose whatsoever, except as expressly authorized in writing by Data Supplier or as expressly permitted under this Agreement. Permitted transfers include: (1) Controlled subsidiaries and affiliates of the Researcher to the extent that the Researcher has and exercises the authority to ensure such subsidiaries and affiliates access, use, and protect that data in compliance with the terms of the Agreement; (2) Other members of the Research Group that are bound by the terms of this, or a substantially similar, Agreement with Data Supplier; (3) Students enrolled or affiliated with the Researcher or other member of the Research Group, provided the student has signed an attestation in accordance with section [xx] of this Agreement; (4) Service Providers, subject to the requirements of section [xx] of this Agreement; and (5) As required by law, subject to the requirements of section [xx] of this Agreement.

Topic	Description	Sample Language
Publication Expectations	Publication of results are permitted and encouraged. Limited right of pre-publication review by the Data Supplier. Note that encouraging publications, particularly if peer-reviewed and/or in the public domain, and showing that the research is in the public interest (as opposed to a purely commercial interest) may have regulatory advantages under certain privacy laws. For example, under the CCPA, there is a limited exception to the right of deletion that applies to "public or peer-reviewed scientific, historical, or statistical research in the public interest." And under the GDPR, the higher level of restrictions on the processing of special categories of sensitive personal data (including health data) don't apply where the "processing is necessary for reasons of public interest in the area of public health."	Researcher is permitted and encouraged to publish the results and finding of the research, including making available information to support such results, to other scholars, researchers, and research organizations for purposes of verifying and reproducing those results. Notwithstanding the foregoing, no Confidential Data or Personal Data may be included in the publication or supporting information without the written authorization of Data Supplier. Researcher has a right to publish regardless of Data Supplier's approval or agreement with the results and findings. Nevertheless, Data Supplier will have the opportunity to review drafts of any publications and supporting information pertaining to or containing the results and findings of research that utilized Covered Data sufficiently ahead of the planned publication or disclosure date (in any event at least thirty (30) days ahead of such date) . Such review is solely to identify: (1) that the publication is within the scope of the agreed upon Research Purpose, (2) any Confidential Information or any Personal Data that may be included or revealed in those materials that should be modified or removed, or (3) statements regarding access to data that could convey an inaccurate or incomplete impression regarding privacy or security protections of the data that should be corrected. At the end of the review period, and once any issues identified in the review have been cured, Researcher will have the right to publish the materials that have been reviewed by Data Supplier. Once a work has been reviewed, the content may be further disclosed in substantially the same form on multiple occasions without additional review by Data Supplier.
Data Minimization and De-Identification	Language to support and encourage the use of de-identification as a best practice designed to	Researcher will apply appropriate data minimization measures, including de-identification (pseudonymization, aggregation,

Topic	Description	Sample Language
	protect the privacy of individual data subjects and reduce the risk of data sharing. If the data is being shared on the basis of a legal provision or exception that is conditioned on the use of de-identification, the de-identification employed should meet the applicable legal standard. This is most likely to occur with respect to HIPAA-covered entities. Optional language regarding de-linking data from the Data Supplier for cases in which the Data Supplier does not wish to be identified or associated with any particular data.	masking, etc.), to Personal Data to the greatest extent such measures are compatible with the research purpose. [OPTIONAL FOR SHARING UNDER THE HIPPA DE-IDENTIFICATION EXCEPTION: The de-identification method used shall comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule set out at 45 CFR 164.514.] Researcher will not attempt to re-identify or otherwise extract Personal Data from Covered Data. [OPTIONAL: In addition, Researcher will de-link Covered Data from the Data Supplier such that the data can no longer be traced back to its source.]
Data Security	Requirement to ensure adequate and appropriate levels of data security.	Researcher will implement and, at all times, maintain appropriate administrative, physical, and technical safeguards to prevent any unauthorized access, use, storage, processing, or disclosure, or the destruction, loss, or alteration, of any Confidential Data or Personal Data. Such security measures will include access controls, encryption, or other means, as appropriate. Upon request of Data Supplier, Researcher shall provide a description and assessment of the security measures in place. OPTIONAL: Upon request of the Data Supplier, Researcher will provide a report of a security audit performed by a qualified third-party auditor.
Training & Attestation	All personnel with access to the data should receive sufficient training to ensure they understand the Researcher's rights and obligations with respect to the data	Researcher's employees and students, as well as personnel of any Service Providers, who have access to Confidential Data or Personal Data shall receive information sufficient to ensure they understand the permitted scope of data use, as well as the restrictions and required protections relevant to the data,

Topic	Description	Sample Language
		and must sign an attestation to that effect before gaining access to the data. [OPTIONAL: Such individuals will also receive privacy and security training designed to provide awareness of basic data protection principles and best practices.]
Data Breach	Language to ensure that the Data Supplier receives prompt notice of any data breach, and has a reasonable opportunity to work with the Researcher regarding the response to the breach.	If Researcher becomes aware of a security breach that may involve the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Covered Data, it will notify Data Supplier of the breach within 72 hours of becoming aware of the security incident. Researcher will promptly and without delay (1) investigate the breach; (2) take reasonable steps to mitigate the effects and to minimize any damage resulting from the breach; and (3) provide Data Supplier with additional detailed information discovered through the investigation and remediation. Researcher and Data Supplier will communicate and coordinate candidly and in good faith regarding the investigation and remediation of the breach and with respect to any notifications to government authorities or individual data subjects related to any breach of Covered Data.
Data Retention	It may be difficult to require a specific retention timeframe given that research projects can take a long time and scientific research often requires that the data be available to test and replicate initial conclusion. Nevertheless, the parties should agree on the retention periods or the criteria used to determine retention periods. And having some language regarding retention in the contract is a recommended best practice.	Researcher will retain the Covered Data for only as long as is necessary to achieve the Research Purpose or in accordance with applicable law. When retention of the Covered Data is no longer necessary, Researcher will securely return or destroy the Covered Data.

Topic	Description	Sample Language
Law Enforcement Requests	Protections to be followed if the Researcher receives a request or demand to disclose Covered Data, and enabling the Data Supplier to intervene.	If Researcher receives an order, demand, or other request from law enforcement, other government agency, or other third party for Covered Data, it will (1) reject or oppose the request unless there is no reasonable legal basis to do so, (2) attempt to redirect the requestor to request the data directly from Data Supplier, and (3) provide prompt notice the Data Supplier before complying with any request unless legally prohibited from doing so.
Service Providers and Vendor Management	This language acknowledges and allows that the Researcher may allow access to Covered Data by service providers, but requires certain restrictions and protections. It may be prudent or necessary to provide more detail on what needs to be in the contract with the Service Provider – including all the elements specified in GDPR Art. 28(3) and CCPA §§ 1798.140(v) & 1798.140(w)(2)(A). Sample language reflecting those elements is set out in the subsections under (3) to the right.	Researcher may provide access to Covered Data to third parties it has contracted with to provide limited or ancillary services on its behalf (Service Providers), subject to the following conditions and limitations. (1) Researcher conducts reasonable due diligence with respect to each Service Provider's ability to comply with its obligations including the protection of Covered Data. (2) Service Provider may access Covered Data only to the minimal extent necessary to carry out the specified services in support of the Research Purpose and may not use the data for any other purpose. (3) Each Service Provider has entered into a written agreement with the Researcher that includes terms regarding the use and protection of data that are compliant with applicable data protection law and are no less restrictive and protective than the terms of this Agreement. a. In particular, such agreement shall specify: i. the nature, purpose, and subject matter of the processing; ii. the type of Personal Data and categories of data subjects; iii. the duration of the processing; and iv. the obligations and rights of Researcher with respect to the personal data. b. Further, such agreement shall require that the Service Provider will:

Topic	Description	Sample Language
		i. use, retain, disclose, or otherwise process the Personal Data only within the scope of the business relationship between the Service Provider and the Researcher, and only on documented instructions from Researcher for the specific purpose of performing the services specified in this Agreement, or as required by law, and not for any other purpose; ii. not sell the Personal Data for any purpose; iii. implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data; iv. ensure and hereby certifies that persons authorized to process the personal data understand the restrictions on the Personal Data as set out in the agreement and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; v. engage another service provider (i.e. a Subprocessor) and allow such Subprocessor to access Personal Data only with the prior written authorization of Researcher and only pursuant to an agreement that contains the same data protection obligations as between Researcher and the Service Provider; vi. assist Researcher in complying with its obligations under this Agreement and applicable data protection law, taking into account the nature of processing and the information available to the Service Provider; vii. after the end of the provision of services or when access to the Personal Data is no longer necessary to provide the services, whichever is sooner, either (at the choice of the Researcher): 1. return to the Researcher all copies of the Personal Data, or

Topic	Description	Sample Language
		2. delete all the Personal Data and certify to the Researcher that all copies of the Personal Data have been irretrievably deleted; viii. make available to Researcher all information necessary to demonstrate compliance with the agreement and applicable data protection law and allows for and contributes to audits, including inspections, conducted by Researcher or another auditor mandated by Researcher; and ix. notify Researcher immediately if: 1. any processing beyond the documented instructions from the Researcher is required by law (unless Service Provider is prohibited by law from providing such notice); or 2. in the Service Provider's opinion, an instruction from Researcher for the processing of Personal Data infringes applicable data protection law. (4) Researcher will provide to the Data Supplier, upon request, a list of all Service Providers that have been given access to the Covered Data.
Cross-Border Data Transfers	For EU data, the contract should address cross-border data transfers. This sample language assumes Standard Contractual Clauses will be the preferred approach. Note that the nature of scientific research would likely make the Researcher a "controller" rather than a "processor" under EU law, thus the controller-to-controller clauses are the appropriate version.	Personal Data transferred from the European Union, European Economic Area, or Switzerland will be governed by the controller-to-controller Standard Contractual Clauses set out in Exhibit 1 hereto.
Compliance with Applicable Law	Catch-all language requiring both parties to comply with applicable law with respect to the Covered Data.	Data Supplier and Researcher will comply at all times with any applicable laws, orders, and regulations with respect to the Covered Data, including those relating to privacy and data protection.

Topic	Description	Sample Language
Data Ownership and IP Rights	Include terms clarifying ownership of the Covered Data remains with the Data Supplier. The "no consideration" language is intended to help shield this data sharing from being considered a "sale" of personal information under the California Consumer Privacy Act (CCPA). Optional terms to consider: • addressing ownership of research results, including algorithms or neural networks trained on Covered Data, • restricting the Researcher from seeking patent protection of research results, and • requiring or encouraging the Researcher to publish research results (excluding Confidential Data and Personal Data) in the public domain (see also the Publication Expectations section above).	Ownership of Covered Data remains with the Data Supplier. The parties agree that this Agreement does not constitute a sale of Personal Data. No payment or other valuable consideration whatsoever has been or will be provided by Researcher to Data Supplier for access to or receipt of any Personal Data. [Optional terms TBD]
Termination	The agreement should remain in effect for as long as the Researcher retains Confidential Data or Personal Data. Termination should be contingent upon the return of the data.	This Agreement shall be effective on data Covered Data is first provided to or accessed by Researcher; it shall remain in force as long as Researcher retains any Confidential Data or Personal Data included in or derived from Covered Data, unless otherwise terminated by law. Researcher may terminate this Agreement by returning or destroying all Confidential Data and Personal Data included in or derived from Covered Data and providing written verification of this action to Data Supplier. If Data Supplier becomes aware of a pattern of activity or practice on the part of Researcher that constitutes a material breach of this Agreement, Data Supplier shall have the right to summarily terminate this Agreement and require Researcher to return or destroy all Confidential Data and Personal Data

Topic	Description	Sample Language
		included in or derived from Covered Data, and provide written verification of this action to Data Supplier. Sections [*x, y, and z – including those relating to publication and data ownership*] shall survive termination of this Agreement.
Remedies and Indemnifications	There may be challenges with regard to remedies and indemnifications, especially when the Researcher is a public university. In some cases, the remedy may be limited to the right to terminate as described above.	TBD
Other	Choice of law, etc.	TBD