International Network for Cross-Linguistic Research on Brain Health

Data Governance Committee

Data sharing recommendations

Include Network – Data Governance Committee

Data sharing recommendations

1. Rationale

The following guidelines have been developed by the Include Network's Data Governance Committee to provide information and resources for facilitating the data sharing process. Our committee is available to provide guidance and support throughout the process.

The guidelines cover several important aspects of data sharing, including legal and ethical consent, data anonymization or de-identification, data accuracy and quality checks, suggestions for data sharing agreements, and recommendations for secure data transfer. By following these points, you can maintain the integrity and privacy of shared data while maximizing its scientific value.

We understand that each site may have unique requirements and specific regulatory frameworks to consider. Therefore, we have included templates and references to relevant laws and regulations, such as the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA), which can assist you in tailoring the guidelines to your specific needs.

Please note that the Data Governance Committee has a strictly supportive role. It is not mandatory to follow these recommendations. The Committee has no supervisory power nor responsibility over data sharing practices for matchmaking projects. We simply aim to facilitate the process through suggestions, materials, and tools.

2. Legal and ethical consent

We kindly suggest that, before sharing any data, each site of the Include Network ensures that appropriate legal and ethical standards are observed. Specific projects might require introducing amendments to the informed consent so as to explicitly state the purpose of data sharing and any potential risks. Relevant insights can be found in the websites of the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA).

Here, we provide an amendment template for your convenience

> "In order to promote transparency and scientific replicability, the data collected in this study will be anonymized and uploaded to general databases, such as the Open Science Framework (OSF)[1,2], and shared with other researchers. The privacy and confidentiality of the study participants will be protected, as no data will allow their identification, and all personally identifying information that could

[1] Examples can be found here.
[2] Repositories that can be used according to the SNSF are listed here.

be used for that purpose will be removed. Their privacy and confidentiality will be protected at all times, and necessary measures will be taken to prevent the disclosure of sensitive information. Access to the anonymized data will be solely for scientific purposes. This study will be conducted in accordance with the highest ethical standards, always respecting the rights of the participants involved, as all regulations and ethical principles required by the ethics committee for the use and storage of the data in question will be complied with. The processing, communication, and transfer of personal data of all participating subjects will comply with the provisions of ***complete with the country regulations***."

Examples:

European Union. Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights, and the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the Protection of Personal Data (GDPR).

United States. The Health Information Portability and Accountability Act (HIPAA), 45 CFR 160, and 162, 164, and to ensure compliance with all applicable state and federal confidentiality and privacy laws and regulations.

For examples of data repositories, please see here.

Please contact The Data Governance Committee should you have doubts about this point.

3. Anonymizing or deidentifying data

Whenever possible, anonymize or de-identify the data to protect the privacy of individuals. Remove or encrypt any personally identifiable information (PII) such as names, addresses, phone numbers, and social security numbers. Ensure that the de-identification process is robust and cannot be reversed at the Data Recipient Center.

Raw data. This is considered a special case because it represents the original, unprocessed information collected directly from sources, often in its most granular form. Unlike processed data, which has undergone some level of analysis or transformation, raw data retains its raw and unaltered state. As a result, raw data can present unique challenges and considerations when it comes to data sharing and privacy protection. In this case, please contact the Data Governance Committee for advice and recommendations.

For more information please see the Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

To aid in the anonymization process, feel free to explore Open Brain Consent resources.

4. Ensuring data accuracy and quality

Prior to sharing, verify the accuracy and quality of the data. Perform data cleansing and validation processes to eliminate errors, inconsistencies, and duplicates. Maintain data integrity by providing clear documentation about the data collection methods and any limitations or biases associated with the dataset.

5. Establishing clear data sharing agreements

To ensure effective control over data transfer, we recommend that at least one representative from each involved site sign an agreement that clearly specifies the data transfer process. Create a formal data sharing agreement that comprehensively outlines the terms, conditions, and restrictions associated with data sharing. It is important to address the following aspects:

(a) Permitted uses: Clearly define and specify the permitted uses of the shared data, ensuring alignment with the intended purpose and compliance with applicable privacy laws and regulations, such as the GDPR or HIPAA.

(b) Duration of data sharing: Clearly state the duration for which data sharing is permitted, considering the specific project requirements and timeline. This ensures that data is only used within the agreed-upon timeframe.

(c) Obligations and responsibilities: Clearly outline the obligations and responsibilities of all parties involved in the data sharing process. This includes expectations for data security, confidentiality, and procedures for addressing data breaches, if they occur.

We suggest that each site tailors the agreement according to their specific requirements and needs.

If helpful, we provide a template that can be modified and adapted to suit your particular circumstances:

This Data Sharing Agreement ("Agreement") is entered into by and between [*Name of site/Institution*] ("Data Provider") and [*Name of site/Institution*] ("Data Recipient") collectively referred to as "Parties."

The Data Provider agrees to share data with the Data Recipient for the purpose of [*Specify the purpose of data sharing described in the concept sheet presented to the Research Committee*].

The Data to be shared under this Agreement includes [*Specify the type and description of the data*].

The Data Recipient shall only use the shared data for the following permitted purposes:

[*Specify the permitted uses of the data described in the concept sheet presented to the Research Committee*].

[*Any additional restrictions or limitations on data usage*].

The Data Recipient agrees to implement appropriate technical and organizational measures to ensure the security and confidentiality of the shared data. This includes, but is not limited to, protecting the data against unauthorized access, accidental loss, or destruction.

Both Parties agree to comply with all applicable laws and regulations, including but not limited to the [*Specify relevant data protection laws and regulations, such as HIPAA, GDPR, etc*.].

This Agreement constitutes the entire understanding between the Parties regarding the sharing of data and supersedes any prior agreements or understandings, whether written or oral, relating to the subject matter herein.

Data Provider:	Data Recipient:
[*Name of site/Institution*]	[*Name of site/Institution*]
[*Authorized Signatory*]	[*Authorized Signatory*]
[*Date*]	[*Date*]

6. Implementing secure data transfer mechanisms

Always use secure methods to transfer data to the recipient (e.g. establish secure VPN connections, use secure FTP (sFTP), or encrypt the data files). If you require assistance with data transfer or need recommendations for secure repositories or data transfer methods, please inform us. We are available to provide guidance and support. To assist you effectively, kindly specify the type and approximate size of the data involved. The Data Governance Committee will be available to assist you with these points parallel to the concept sheet submission process. However, it is recommended that the sites wait for approval from the Research Committee before initiating proper data sharing.

7. General information

Here we share below useful links with information on data protection regulations in different jurisdictions. It's important to consult the specific regulations and guidance provided by these entities for detailed and up-to-date information regarding data sharing and privacy requirements.

European Union	General Data Protection Regulation (GDPR)
	European Data Protection Board (EDPB)
United States	Health Insurance Portability and Accountability Act (HIPAA)
	Office for Civil Rights (OCR)
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)
	Office of the Privacy Commissioner of Canada
Australia	Privacy Act 1988
	Office of the Australian Information Commissioner
United Kingdom	Data Protection Act 2018
	Information Commissioner's Office (ICO)
Germany	Bundesdatenschutzgesetz (BDSG)
	Federal Commissioner for Data Protection and Freedom of Information
Argentina	Agencia de Acceso a la Información Pública (Agency for Access to Public Information)
Chile	Law 19.628
Brazil	Autoridade Nacional de Proteção de Dados (National Data Protection Authority)
Colombia	Superintendence of industry and commerce
South Korea	Personal Information Protection Commission
India	Ministry of Electronics and Information Technology
South Africa	Information Regulator
	Protection of Personal Information Act (POPIA)
Turkey	Data Protection Authority (KVKK)
Thailand	National Electronics and Computer Technology Center (NECTEC)