IISPV
INSTITUT D'INVESTIGACIÓ SANITÀRIA PERE VIRGILI

PROPOSAL FOR THE DATA MANAGEMENT PLAN

Describe the type and format of the data to be collected/generated within the framework of the project, the planned procedure for accessing them (who, how and when they will be able to access them), ownership of the data, the repository in which they are expected to be deposited, and procedure envisaged to guarantee the specific ethical or legal requirements that will apply.

Type and format of the data to be collected/generated in the framework of the project:

Provide information regarding the data that are going to be processed (identifying, habits, health, genetic, biometric, biological samples).

The data will be processed in the form of (identifying, coded, pseudonymised or anonymised). Only the data that are necessary to fulfil the objectives of the research shall be collected.

***pseudoanonymisation**, understood as the processing of personal data in such a way that they can no longer be attributed to a data subject without using additional information, provided that this information is recorded separately and is subject to technical and organisational measures designed to ensure that the data is not attributed to a natural person, whether identified or identifiable. Not to be confused with coded data. There must be an explanation of how this procedure has been implemented.*

If the data are processed ***anonymously*** the anonymisation process must be described.

Intended procedure for access to the data (by whom, how and when they can access them).

It is necessary to indicate how the data will be processed; that is, where they will be stored and the IT resources that will be used.

• In relation to where they will be stored, you must indicate whether your own servers or those of a third party are used, as well as whether cloud storage tools or data management platforms are used by third parties (for example Redcaps), and their characteristics.

• It will be necessary to make a brief description of the security measures that guarantee that the data is only accessible to the research team, such as access code and passwords.

•The information storage and exchange tools used must always be institutional or else verify through the Information Systems Department that they are secure tools.

• If the data are stored on external servers, it must be guaranteed that these are secure and the security measures applied to access them must be explained in detail, including a description of who accesses the data and when, how and where they are stored.

• Unsecured commercial cloud storage tools that do not guarantee GDPR compliance must not be used.

•If data are processed in the project with non-institutional software, it is necessary that the code developed for the applications use code obfuscation techniques, especially in mobile applications, and that the applications developed follow secure development methodologies.

In the case of biological samples, the following must be borne in mind:
If using biological samples: Detail the source of the biological samples. If biological samples are collected from a healthcare process or if additional samples are collected; if they come from another centre, from a project already approved by an ethics committee (indicate reference), if they were obtained with the patient's Informed Consent for later use; if they come from the Biobank or from a registered collection (indicate references)

Samples that are added to a collection for biomedical research purposes kept outside the organisational scope of a biobank may only be used by a line of research and by the entities or persons that appear in the consent document, unless there is a new express consent of the source subject for another purpose or to transfer the sample to a third party. At this point, it may be possible to allow samples to be shared in collaborative projects in which the lead investigator of the collection participates if the informed consent document refers to this point.

For example:

"In accordance with Law 14/2007, the samples will be collected directly from the data subject // the samples will be deemed care surplus and the procedure laid down by the regulations for the use of biological samples shall be followed to authorise their use. The samples will be added to the Biobank [*] // in the collection [*] // they will only be used in the project and will be subsequently destroyed"

Ownership of the data, the repository in which it is expected to be deposited, and the procedure in place to guarantee the specific ethical or legal requirements that apply.

Identify the entity that decides with regard to the processing of the data, that is, who is/are the **data controller(s)/co-data controllers** of the processing (when two or more controllers jointly determine the objectives and the means of the processing).

Other subjects who will access the data or who will receive it shall also be described, although they are not considered to be the party responsible for the processing, who will be the **data processor**: (the natural or legal person, public authority, service or any other body that processes personal data on the controller's behalf).

The data communications that will take place within the framework of the project and their legitimate basis must be described in detail, distinguishing between the data controller and the **international data transfers** (International data transfer is considered to be sent outside the European Economic Area when there is no agreement that guarantees that the country or entity of destination of the data meets the minimum requirements under EU regulations).

For example:

"The Hospital [*] and the Promoter [*] act as data controllers in the framework of this observational study. The company [*], when supplying [*] the patients, must have their data for the provision of the service, so it will act as the data processor // The project database

will be housed in the company servers [*], so it will act as the data processor.

International data transfers are not planned // The data will be sent to [*], a country for which there is an adequacy decision in accordance with article 45 of the GDPR.

It must indicate where the data to be used in the framework of the research project come from, as well as the legitimate basis for its use. The data may be sourced:
- Directly from the owner of the data in the framework of the specific research. (The data were obtained directly from the participants in the project with their consent)
- From pre-existing processing (data reuse).

For example:

"The variables necessary to carry out the study have been obtained directly from the project participants through their consent, in accordance with the provisions of articles 6.1.a) and 9.2.a) of the GDPR. The variables necessary to carry out the study have been obtained from the centre's clinical history, after undergoing a pseudonymisation process by the Institution's information systems, in accordance with the provisions of articles 6. e), 9.2. j) + 89 GDPR, as well as supplementary provision 17.2.d of the LOPD-GDD."

To guarantee the data processing, technical and organisational measures will be applied, which, by default, will process only the personal data necessary for each specific purpose of the data processing. The permits established by both the General Data Protection Regulation of the EU, Regulation (EU) 2016/679, and the Spanish Organic Law 3/2018 on Protection of Personal Data and Guarantees of Digital Rights will be obtained.