Data Sharing and Ownership Policy

General Overview

As a guiding principle, data collected in many studies is meant to be shared for quality improvement, to improve outcomes for patients. Many studies are also meant to be collaborative projects, which means the policies and procedures related to how data is handled should be as open and transparent as possible. However, it is also important to acknowledge that there are limits to what types of data are shared, and how that data can be shared, based on the legislation and the decisions of professional societies participating in studies. This document is intended to provide a general framework for REDCap data ownership, sharing, and publication.

Data Types

All data collected within the REDCap project should be de-identified, exceptions will be consulted with Data Protection Officer (DPO). Patient data should be uploaded with a pseudonymised ID which does not contain any information connecting the data to a natural person. REDCap platform can automatically generate this pseudonymized ID, or participating scientists can use their own pseudonymizing scheme.

Data collected within REDCap can be divided into three general types, with only the first two types listed below being relevant to most participants.

1. **Patient data**: This is the raw data for individual patients entered into the database in REDCap using one of the available forms.
2. **Results data**: This is a broad category covering all data derived from the patient data, but no longer attributable to any individual patient. This can include descriptive statistics, comparative statistics, graphs, presentations, or any other derived or aggregated data set.
3. **User data**: This is the data collected about each participant when they request to have an account created in REDCap. This includes the user's name, email address, and any relevant details.

Data management

Data management is generally dependent on the data type as described in the "Data Types" section. However, there are general principles which apply to all data types.

Data Destruction: More details can be found in the Data Security Policy document.

Data Auditing: The REDCap platform maintains an auditable log of all changes made to records in the system. This change log is only accessible to authorised employees of the institution and authorised users of the database.

Other policies are specific to the data type:

1. Patient Data and Results data

Patient data are managed by the group which contributed to it. As such it can be added to, modified, viewed, and exported at the discretion of the contributing group. Only registered users associated with the contributing team with corresponding rights, and authorised employees of the institution can access this data.

3. User Data

User data are managed by authorised employees of the institution with the explicit consent of the user. That consent can be withdrawn at any time and user will be suspended.

Data Sharing

As discussed in the general overview, most of the data collected in the REDCap database is meant to be shared towards the purpose of quality improvement.

Principles pertaining to this input are again dependent on the data type.

1. Patient data

Patient data are provided to all who follow the export process and get approval from the committee. The process is specified in more detail in the section Data Request Policy.

2. Results data

Results data can be provided to authorised users.

3. User data

User data can be exported to authorised employees of the institution and authorised users of the project with corresponding rights and reasons.