SOP Data Management

All researchers of the Erwin L. Hahn Institute (ELH) are obliged to the principles of data protection according to the DSGVO.

Generally, data sets of test subjects are to be collected with pseudonyms instead of real names. If this is not possible, the data records are to be pseudonymised as soon as possible and the the real names removed. Data analyses with real names are not permitted.

General:

- The desktop workstations and remote desktops of the ELH are to be used exclusively password protected. Passwords must not be written down. In the event of absence from the workstation, users are required to log out of an active user account (e.g. by pressing the Windows + L keys).
- The storage of personal data on private devices is not permitted. The use of private devices for remote work is allowed.
- Data transfers with data carriers outside the ELH shall, as far as possible be carried out exclusively by means of encrypted hard disks and USB sticks. If possible, direct data transfer, e.g. via VPN tunnel, is to be preferred. After successful data transfer, the data must be deleted from the mobile data carrier.
- Business laptops may be used for the processing of personal data, but it is recommended that the hard disks/data partitions of these laptops be encrypted in an appropriate manner (VeraCrypt or Bitlocker on Windows, system Windows, system encryption on Mac).
- The loss of data carriers and laptops containing personal data must be immediately reported to the Directorate and the respective responsible data protection officer.
- The use of the university cloud systems, such as Seafile (University Medical Center Essen), Sciebo (University of Duisburg-Essen), the ELH Cloud, or similar for sharing pseudonymised data between devices and users is permitted.
- The central storage points for the ELH are (in the short and medium term) the ELH-PACS and the institute's internal network drive *userdata*. Furthermore, some of the structural MRI data will additionally be stored in the PACS archive of the Institute of Diagnostic and Interventional Radiology and Neuroradiology of the University Medical Centre Essen (long-term storage). Measurement data is preferably stored here.
- In case of locally stored data, each user is responsible for sufficient backups.
- In the case of anatomical imaging data, defacing/skull stripping is to be performed before sharing these images with third parties.
- In the event of subsequent withdrawal of consent from a subject, the following actions should be taken immediately, but at the latest within 30 days of receipt of the withdrawal of consent:
    - The withdrawal of consent shall be noted on the subject's consent form.
    - The measurement data and the data obtained/processed from the subject shall be deleted.
    - If the data was shared with cooperation partners, they will be informed immediately that the data is to be deleted and a confirmation of the confirmation of execution will be requested.
    - Receipt of the withdrawal of consent and the execution of the measures taken are documented with date on the pseudonym list.

Study-related:

- Pseudonym lists are compiled individually for each study and contain only three entries: Pseudonym, name and date of birth of the subject. The lists are only accessible to ELH researchers and kept secure.
- Consent forms, contact and account data are kept in study folders sorted by name and stored in a locked filing cabinet on the ELH premises.
- Digital measurement data (image data, behavioural data, scanned questionnaires, etc.) are stored archived on the central storage points of the ELH.
- It is the responsibility of the study leaders, after the end of data acquisition, to back up all measurement data of a study on a USB hard drive and store it in lockable cabinets protected from access by third parties.
- For the publication of source data on OpenScience platforms or, e.g. in manuscripts, the data must be anonymised, i.e. with neutral labels that are not used in the ELH (e.g. sub001, sub002, ... or P1, P2, ...). In the case of image data, it must be ensured that defacing or skull stripping has been performed before the data is published.
- The expiration of deadlines for the deletion/anonymisation of study data shall be checked once a year within the first four weeks of the calendar year and documented in the same folder as the the pseudonyms list. The deletion of data and pseudonym lists must be documented in the same place.