Physiological data collection for research at the USZ

Data Collection

What data will you collect or create?

We will collect physiological data from experiment participants such as

- ECG signal from the brain, heartbeat, temperature, blood pressure, transpiration rate - continous signal
- age, body mass, height - numeric data type
- scope of physical activity, gender - factor data type
- images from MRI scanner - jpeg files

All are stored as xlsx, csv files, on a hard drives and in an Electronic Lab Notebook. This allows data to be stored, backed up, shared and long-term accessed.The files are sent to the Hospital's cloud with set deadlines of expiration of data access.

How will the data be collected or created?

Participants give informed consent before participating. For personal information (age, gender, physical activity) participants fill in a questionnaire prior to the experiments.

Then measures are taken from the participants using thermometer, electrocardiograph, manometer, eye tracker, neuroimaging techniques (MRI scanner, EEG or PET) and other physiological measurement tools. As participants are regularly examined by doctors, they also provide their blood and brain drug concentration over the period of experimnets.

Each participant has an assigned number and folder in the data set. We will use ISO standards for dates and a naming convention :

File Naming Convention

- Project lead's last name or initials.
- File creator's last name or initials.
- Project name/acronym.
- Date file created/generated (in YYYY-MM-DD format)
- Version number

Documentation and Metadata

What documentation and metadata will accompany the data?

An excel file with participants' names and associated numbers will accompany the data files to decode participants and their attributes.

Readme text file with the following information will also accompany the study :

- statistics about the data (total number of observations)
- models of the tools used
- type of data
- instructions for experimentators

An addition Word file will include the questionnaries templates with predefined questions.

Ethics and Legal Compliance

How will you manage any ethical issues?

The consent is required from participants before storing data as a consent questionary describing all the legal impolications. Anonimization can be done by hashing/encryption of personal and identifiable data.

- the basic database's (with participants' names) access is regulated for patient's doctors.

- another data without identification (names, date of birth) can be accessed with a barcode or a random numer assigned to a patient.

How will you manage copyright and Intellectual Property Rights (IP/IPR) issues?

The data is own by the USZ and Intellectual Property rights are owned by the researches that conduct experiences and USZ as a whole.

Storage and Backup

How will the data be stored and backed up during the research?

- The Data will be stored on the Cloud-server of the at the research organisation and hospital (project collaboration platform).
- If an data is processed on local drives, the files and folders need to be saved in the following folder:

  :/projects/data

- Set up of the data space in the Project Collaborative Platform
  - Implementation of the UUID generator
  - DOI registration request
  - Preparation of templates for:
  - Data descriptor (general, text format, pdf output)
  - Metadata: text template, spreadsheet template

- This folder is secured and all files are automatically uploaded and backed-up.
- It will require 500gigabyte, hence we will require additional storage.
- The data will be backed up end of the week, and uploaded automatically to the server.
- The IT admin in responsible and recovery of the data.
- Barring any major incidents on the server, the data can be retrieved from the cloud-server if any mishaps occur on the local data.

How will you manage access and security?

- Only authorised user will be given access to the data i.e.
  - the project supervisor
  - the project leader
  - the project collaborators/ hospitals
- A password protected will be provided to the authorised person
  - two-factor security of access will be established using the Authenticator app
- Collaborators will need to provide an email address and a phone number for accessing the data
- Data encryption will be put in place before the data is uploaded to the main secure system
- GDPR will be applied and personal data
- Files uploaded and backed-up to the secure server will appear in a color-coded format (e.g. green-> for uploaded and backed up, blue-> for only local files, red-> unsaved files)

Selection and Preservation

Which data are of long-term value and should be retained, shared, and/or preserved?

- Patient critical Meta data and business critical data will be long-term data on:
  - Long-term is defined to 10 years
  - Observations, findings and Results will also be kept for Long-term
  - Each dataset is initially assigned to a unique ID and classification, automatically generated through a Universally Unique Identifier (UUID) application.
- Processed data will be kept for 5 years
- The data can be used for future research studies
- Data can be used Research Paper publications in international journals
- No additional cost is associated with the maintenance of data on the main server (10 years)
- A dedicated software will be deployed for saving the data with specific identifiers which will allow the definitions of the data retain-ability
- A training will be established for familiarising the project participant on different classes of the data

What is the long-term preservation plan for the dataset?

- Once the project is completed, it will be the responsibility of the project leader to close the project.
- When the project is closed, the project supervisor will sign-off the main server location to be moved to the archived repository
- Only authorised user will be given the access to the archive folder
- No additional cost will be accrued for the data preservation
- It is the responsibility of the project leader to prepare data for sharing / preservation

- Internal audits of the folder may take place each quarter for the assuring the quality of the data and folders

Data Sharing

How will you share the data?

In general only data related to publications will be made openly available In general, the proejct-leader will decide on a case-by-case basis which data can be released in order to avoid issues related to IP rights protection or access.

- Digital search engine will allow university researchers to look for keywords related to the projects which will allow them to find out the existence of the data
- The data could be shared within the ZHAW researchers, under the condition of maintaining the confidentiality and not divulging the trade-secrets
- the data can only be used for research and non-commercial purposes
- Credits and citation will be given by the future users to the project team
- A handle request will be established and access to only the relevant files will provided
- The data-request form will be established for access the data in future
- The data-log will be established and password secured will be put in place to identify who is accessing the data and when it is access
- Reports from unauthorised attemps to access the data will also be logged-in
- An NDA will be established so that the data is not dispersed to any third-parties

Are any restrictions on data sharing required?

- Personal and confidential information and data will be restricted before sharing
- Normalisation of any identifiers will be established during the project i.e. keeping the identity of any individual secured
- Specific agreements with the Editors of scientific/technological journals will be considered and provided.
- Results of the study and any improvements will only be exclusive between ZHAW and the external partner
    - Hospital
    - Machine manufacturers
    - Software manufacturers
- A data sharing agreement will be required if the request is coming from outside of ZHAW
- NDA will still be established between external parties and the project leader

Responsibilities and Resources

Who will be responsible for data management?

The directors of departments, principal investigators of each experiment and Data Stewards are responsible for implementing the DMP, and ensuring it is reviewed and revised. Researches are trained by their superiors in order to collect, store and handle data in accordance with the DMP. Data ownership and responsibilities for research data management will be part of an agreement between the research organization and the hospital.

What resources will you require to deliver your plan?

A data steward is required to set the right training for the researchers. DMSP resources will include

- Onboarding and Offboarding Checklists
- ELN Resources (Electronic Lab Notebook)
- Metadata Guide