Ethics Review Committee of the Faculty of Science
Example Data storage (February 2021)

Below an example from an approved study of how personal data (in this case recordings of individual participants in a study) may be stored and anonymized in a safe way. (NB: Information on the specific aims and nature of this study has been removed.)

3. Data management

3.1. Storage and anonymization

The consent forms that are signed and returned by participants are digitally scanned and temporarily stored on a laptop of Leiden University with an encrypted hard disk, and as soon as possible transferred to a secure cloud environment of SURFdrive, within Leiden University. The hardcopy versions will be destroyed. Providing informed consent digitally is also possible via a Qualtrics form, these forms will after submission also be transferred to an encrypted hard disk and uploaded to the secure cloud environment of SURFdrive, and deleted from Qualtrics.

Every individual, and accompanying data, is assigned a unique participant number that is pseudonymised by a key created by and stored at a trusted third party, such as ZorgTTP and Blackberry Workspaces. The trusted third party has no access to personal data. The researchers and SURFdrive have only access to the pseudonymised data. The researchers can only in exceptional cases ask for the pseudonymisation key, for example to erase data from participants who withdrew consent during the project. This means that during the project the data are fully pseudonymized. After the project the encryption key can be destroyed, yielding a fully anonymous data set for future research purposes.

Recordings will be transferred from the voicerecorder or app to an encrypted hard disk of a laptop of Leiden University as soon as possible after data collection. Once they are removed from the voice recorders they will be uploaded to the secure cloud environment of SURFdrive within Leiden University. The procedure for the app is the same, after data collection the data are transferred to an encrypted hard disk and uploaded to the cloud, or, if the app is sufficiently developed, will be stored in the secure cloud environment of SURFdrive directly.

3.2 Data editing, transcription, and annotation

Recordings are, after data collection, unprocessed .wav files in the SURFdrive environment. These files will be cut using software as Audacity, and assigned the pseudonymised unique participant number. Any potentially identifying information will be cut out.