Unification of treatments and interventions for tinnitus patients

Proposal No.: 848261

Deliverable D2.2:

Report on Legal and Ethical Issues Monitoring

Deliverable No. D7 – WP2

Authors	Susanne Staudinger, Stefan Schoisswohl, Winfried Schlee (UHREG)
Responsible of Deliverable	Winfried Schlee (UHREG)
Target Dissemination Level	Public
Status of the Document	Version 1

Table of contents

Table of Figures

1 Introduction

This deliverable will cover all issues described in Task 1.5 of the proposal:

Within this Task, the legal and ethical issues throughout the whole duration of the project will be monitored. In addition, a data privacy framework will be developed, that covers the internal processing of personal data within the project, including ethical and legal aspects. In the following we will describe the Informed Consent Procedures, the techniques of anonymisation and pseudonymisation, the lawful use of sensitive health-related data, the rules of secure data transfer within the UNITI Consortium, the accordance with GDPR, the feedback process to individuals, regulatory issues and related EU as well as national legislation and the collecting and shipping procedures

2 Informed Consent Procedure

2.1 General ICF

Participants are provided with the patient information leaflet (PIL) and informed consent form (ICF) prior to the screening visit by e-mail or post (information obtained throughout pre-screening). These documents contain detailed information about study participation, including the purpose of the study and what is required as study participant as well as potential risks and benefits. During the Screening procedure; participants will be informed about the aim and methods of the study by a member of the clinical research team (CRT) and have the opportunity to ask questions about the study, the PIL or ICF. If they consent to participation, they will be requested to date and sign the ICF in the presence of the assigned clinical investigator/ member of the CRT. At the same time the assigned clinical investigator/member of the CRT will also sign the ICF- participants will be given a copy of the ICF to keep for their own records, the original will be retained by the CRT, separated from other study documents.

2.2 Blood sampling ICF

Also during screening procedure participants will be sufficiently informed about blood sample collection and what exactly happens with their sample (with respect to EU and country-specific regulations). For this purpose, participants will sign an extra ICF. Giving a blood sample is voluntary. Refusal to sign the ICF for the blood sample does not preclude participation in the study

2.3 Procedures for withdrawing consent

Patients can withdraw their consent to participate at any time during the study without giving reason and without any disadvantage. If this occurs, participants can request that their study data are removed from the database and excluded from future analysis. All documentation that is needed for possible regulatory audits, e.g. the signed informed consent, cannot be deleted, even if this is requested by the patient.

3 Anonymisation and Pseudonymisation Techiques

The EU Tinnitus database does not store personal information like names, addresses, phone numbers, e-mail addresses, or IP addresses that can be used to identify a certain participant directly. Data that is entered directly in the database will be stored with a 6 digit code, randomly generated by the database. This code is used as a Unified Identifier Code (UIC) throughout the UNITI trial.

To enable responses to requests in accordance with GDPR, the association between a patient's real identifier and the UIC is kept separately and, if stored electronically, password protected. These associations are only accessible to authorized and authenticated users with appropriate permissions who may need to access a patient's real identity.

Once data is exported from the database, instead of the UIC, a cryptographic hashcode is generated from the UIC and will be used as anonymized identifier.

Personal information of individual patients is maintained only within the system of the local centre, which has responsibility for the patient and, therefore, needs to identify the patient. The identification of an individual patient via e.g., the value of the external identifier attribute, enables an anonymization or a permanently deletion of the study data if this is requested by the patient. The deletion process will be conducted by the data administrative staff of the local systems of the centres according to the rules set by the General Data Protection Regulation (GDPR) – but always in consultation with the local data protection officer.

4 Lawful use (processing, transfer, storage, access) of Sensitive Health-related Data

4.1 Unified Database for Clinical Data

The following illustration (figure 1) shows the process of collection, processing, storage, access and transfer of sensitive health-related data in accordance with applicable national and EU legal requirements within the unified database https://tinnitus-database.eu:

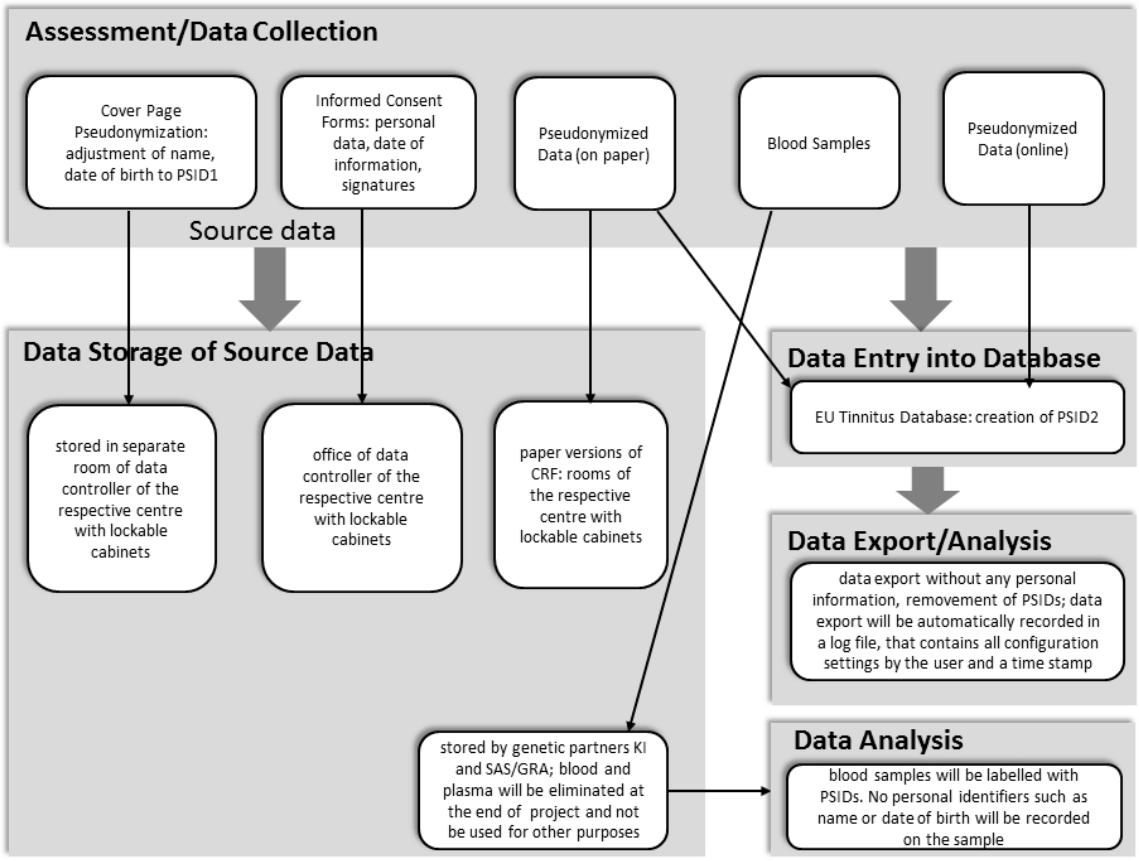

Figure 1 Schema for data collection, processing, storage, access and transfer of the health-related data within the UNITI project

Role based access control. Different levels of access to the database are provided subject to the roles of individual users. Users are members of staff of the different clinical centres. In general, users are researchers and they can only see the data of their own centre. At the

moment, the roles supported (Clinical) Centre Editors, Experts and Administrators. Role based access control is enforced by a role management system, allowing Centre Editors to view and edit individual patient datasets of their respective centre. In addition to the rights of Centre Editors, Centre Experts can export data of all the patients of their centre for data analysis. Centre Administrators have all rights of the Centre Editors and Centre Experts but they can also add new users to the database or remove users from it. There is also a database administrator user (Superadmin) based at the University of Regensburg, who has access to the data from all centres. Our expectation is that the above role types will remain in UNITI and may be expanded by other additional roles (e.g., Centre admin users with enhanced rights.

4.2 Secure Data transfer

The rules for secure data transfer within the UNITI consortium are laid down in the UNITI Consortium Agreement, chapter 12, and are presented in detail in chapter 5 of this deliverable.

4.3 Unified Database for Smartphone Data

Introduction: The unified database for smartphone data has the purpose to store the data that is collected with the smartphone apps within UNITI.

Types of data: The following types of data are stored in the app database and the local smartphone devices:

- questionnaire data collected using Ecological Momentary Assessment (EMA) methodology;
- time stamps of app usage;
- in case of auditory stimulation: subjective ratings of the tinnitus suppression;
- in case of psychoeducation app: results of the quiz;
- in case users allow it: GPS location and sound pressure of the surrounding environment while filling out the EMA questionnaires.

Sources of data: The smartphone device, its sensors and the UNITI app running on it.

Ownership of data: The patient who uses the smartphone device and UNITI app.

Physical database: The data collected from the smartphone is stored in a relational database using Maria DB 11, which runs in a Linux environment (Debian Buster) and a LAMP technology stack. This database will be separate from the UNITI database and may be referred to as the “smartphone database”. The smartphone database will only be accessible to the patients through the UNITI mobile app running on the smartphones of the patients. Access to it will also require the authentication of the particular UNITI mobile app instance as well as the authentication of the user of this app (the patient). Smart phone data will also be stored separately in the UNITI database for analysis purposes.

Pseudonymization of data: The smartphone database does not store personal information like names, addresses, phone numbers, e-mail addresses, or IP addresses that can be used to identify a certain participant directly. Data from the smartphone will be stored in the smartphone database and the UNITI database separately after pseudo-anonymisation as described in Section 3. Furthermore, on the smartphone database, data will be stored in encrypted form.

Access of data: The patients can see their own data on their smartphone device. Such data will be maintained in encrypted form on the mobile accessible only after proper authentication of the patient/user of the mobile. This authentication will be based on password or fingerprint authentication. Mobile app data will also be transferred and backed up periodically on a back-end server of the UNITI platform (separate from the UNITI unified database), to ensure availability in the event of loss of the mobile device and to ensure that the storage space on the device will always be sufficient for storing the latest data of the patient. Backed up data will be stored in encrypted form and will be accessible only to the client app running on the mobile device. Users of the UNITI unified database will not have access to such data (although they will have access to their pseudo-anonymised counterparts).

4.4 Matching data from the EU Tinnitus Database with the App Data

A unique patient identifier will be used in the EU Tinnitus Database as well as for the smartphone apps. This identifier will be used to match the data from the UNITI app with the questionnaire data before and after the clinical intervention.

More details on data handling are also provided in the Data Management Plan in Deliverable D2.1 as well as in Deliverable D1.4 on the POPD requirements.

5 Rules of Secure Data Transfer within the UNITI Consortium (Chapter 12 of CA)

As outlined in the Description of Action, which is part of the Grant Agreement, the joint analysis of existing data, as well as the joint analysis of the data collected within the Clinical Trial, are an integral part of the Project. This requires that a Party that is the owner of the data ("Data Provider") transfers the data to another Party who is analysing the data ("Data Analyst").

The Parties agree to handle these cases as follows:

12.1 Data Provider agrees to disclose the Data to Data Analyst solely to conduct the analysis needed within the Project and to publish the results of the analysis and for no other purpose.

12.2 Data Provider will ensure that all data is genuine and has been obtained in accordance with applicable laws and regulations from research conducted in compliance with sound scientific methods and principles, relevant guidelines and appropriate ethical approvals, and the principles of good laboratory or clinical practice (if applicable).

12.3 Data Provider warrants that it either owns or respectively controls the data to grant access to Data Analyst under this Agreement or that data are in the public domain.

12.4 Data Provider shall only provide such data as necessary for the Project in an anonymized way, where possible.

To the extent the data cannot be fully anonymized for instance by aggregating the data, Data Provider shall only provide pseudonymized personal data which is de-identified to the fullest extent possible to ensure as much as possible that, without access to the master identifier file, all records are unidentifiable. By way of example, but not limitation, Data Provider shall remove

names, and other data elements which could identify data subjects from records, identify records only with arbitrary codes, and will carefully safeguard the key to the coded data.

12.5 Therefore, the Parties recognize that any data disclosed hereunder may constitute personal data as defined in the General Data Protection Regulation (EU) 2016/679, ("Personal Data") including Personal Data concerning health. In such cases, Data Provider and Data Analyst will comply with all applicable laws, standards and regulations in using the Personal Data. For the avoidance of doubt, Data Analyst will not perform any act which could lead to the re-identification of the data subjects, including by linking different sets of data, comparing and processing data. If Data Analyst wishes to obtain supplementary information in the course of the Project concerning the data subjects, the relevant Personal Data will be provided again in such a manner that Data Analyst cannot use the supplementary data to re-identify the data subjects.

12.6 Data Analyst and Data Provider shall use appropriate safeguards to prevent use or disclosure of the Data other than as permitted under this Agreement or applicable laws and regulations, including by transmitting the Data via a secure transfer.

12.7 Data Analyst shall ensure that all employees, agents, contractors, researchers, team members and other contributors with access to the Data comply with the terms of this Agreement, as well as any applicable data privacy and security laws and regulations. Data Analyst shall ensure that only those given access to the Data shall be bound by confidentiality and user undertakings and limitations substantially similar and no less stringent than those provided for in this Agreement.

12.8 Data Analyst will have the right to disclose non-individually identifiable information regarding the Data in a summary form that aggregates more than one data subject's clinical information for scientific journal publication, in all events to the extent permitted under applicable laws and regulations.

12.9 If necessary, the Data Provider shall have the right to request that a bilateral agreement for data sharing is signed between the relevant Parties before any Personal Data is made available. In such separate data protection agreements, Data Analyst and Data Provider shall agree on appropriate safeguards to prevent use or disclosure of the Personal Data other than as permitted under this Agreement or applicable laws and regulations, including by transmitting the Personal Data via a secure transfer.

6 Accordance with GDPR

Data protection is considered and relevant ethical, legal and privacy concerns will be addressed respectively. The Data Protection Officer (DPO) of the University of Regensburg (Germany) is also the Data Protection Officer of the EU Tinnitus Database. He is responsible for overseeing the data protection strategy and implementation to ensure compliance with the EU General Data Protection Regulation (GDPR, 2016/679). Furthermore to ensure that the project will be able to respond to data subject access requests (DSA) under GDPR associations between the pseudo identifiers and real identifiers of subjects will be maintained separately from the clinical data, within the system of the local centre, which has responsibility for the patient and, therefore, needs to identify the patient.

7 Feedback Process for Individuals

The chronic tinnitus patients are among the most important stakeholders in the context of UNITI and tinnitus research in general. Therefore, the feedback by the patients will be essential for the continuous improvement of tinnitus research, of tinnitus treatments and the applications used in UNITI. Patients are actively asked to give us feedback at studie.uniti@tinnitusresearch.net, which is evaluated by the UNITI coordinator team. Furthermore, a systematic collection of patient feedback for the UNITI app is currently prepared used the App Quality User Assessment (AQUA, O'Rourke et al. 2020).

8 Regulatory Issues and Related EU as well as National Legislation

The UNITI mobile application will be available for iOS and Android devices and developed according to the European Guidelines for medical software (IEC 62304, IEC 82304) in a team of psychologists and software developers and experts for medical software regulations.

9 Establishment of Collecting and Shipping Procedures

Samples will be collected once during the RCT, preferably before treatment start.

Blood samples: The blood samples will be shipped the same day of their collection to the Centre for Genomics and Oncological Research GENYO/ Hospital University. The vial will have the unique code of patient and the date of collection, both of them will be marked with a permanent marker pen. It is preferable, PI or site staff to organize the blood samples collections Monday or Tuesday in order the samples to be delivered to central lab within 48h. Each site will be able to send max 13 shipments during the RCT, with 8 samples per shipment.

PI or site staff will communicate with local TNT office 1-2 business day prior to shipment, using a unique code of client that will be distributed to sites upon site initiation visit. TNT will provide to site the appropriate package for samples (Medpack A).

Plasma samples: The plasma samples will be collected and stored at -80^{o}C, until the required number of samples is collected; 100 samples per site. Then PI or site staff will communicate with local TNT office 1-2 business day prior to shipment, using the unique code of client. TNT will provide to site the appropriate package for samples (Medpack) containing dry ice. Plasma samples will be shipped to Karolinska Institute (Stockholm, Sweden).