TIMESPAN
Management of chronic cardiometabolic disease and treatment discontinuity in adult ADHD patients
H2020 – 965381

D7.4. – EDMB report (incl. EDAC feedback) on TIMESPAN ethics and data management implementation (incl. evaluation of the independent ethics advisor)

Dissemination level	Public
Contractual date of delivery	30. September 2022
Actual date of delivery	29. September 2022
Type	Report
Version	2 (Revised February 8th 2023)
Filename	TIMESPAN_Deliverable Report_D7.4.
Workpackage	7
Workpackage leader	Patric IP (HKU)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 965381.

This report reflects only the author's views and the Commission is not responsible for any use that may be made of the information it contains.

Author list

Organisation	**Name**	**Contact information**
HKU	Patric IP	patricip@hku.hk
ORU	Henrik Larsson	Henrik.Larsson@oru.se

History of changes

Version	**Submission date**	**Request EC** **Comment TIMESPAN**
1	29.09.2023	-
2	08.02.2023	**Request EC:** Could you please confirm in the report that all transfers to the UK imply GDPR-compliance of the UK databases? **Comment TIMESPAN:** We can confirm all transfers from VHIR to UK imply GDPR compliance and compliance of the UK databases.

Abbreviations

EDAC	Ethics and Data Management Advisory Committee
AI	Artificial Intelligence
ADHD	Attention Deficit Hyperactivity Disorder
DMP	Data Management Plan
PI	Principle Investigator
DPO	Data protection officer
UCN	unique code number
DLNN	deep learning neural networks
EEA	European Economic Area
SSH	Secure Shell
ACLs	Access Control Lists
RSA	Rivest-Shamir-Adleman
eCRF	electronic Case Report Form
GPS	Global positioning system
EDA	electrodermal activity
AE	adverse event
RPD	Raw physiological data
PPD	Processed physiological data
MDA	Meta data
HWD	Hardware data
CSV	Command separated values

Table of Contents

1. Executive Summary 5

2. Deliverable report 5

3. Conclusion 8

1. Executive Summary

This deliverable contains the Ethics and Data Management Board report (incl. EDAC feedback) on TIMESPAN ethics and data management implementation. In addition, the report deals with:

- Prevention of misuse of research participant's data (data security measures to prevent unauthorized access and data breach, anonymization techniques, encryption, secure data transfer, controller processor agreement ensuring high security standards (for the remote collection)). Such measures will mitigate the possible risks for the research participants.
- Ethical considerations in relation to AI applications (terms of fairness, discrimination, inequality, avoidance of harm, conflicts of autonomy, beneficence, non-maleficence, justice, the "black box" problem in AI, and accountability).
- Next to that the entire report has been evaluated by an independent ethics advisor

2. Deliverable report

TIMESPAN's main objective is to advance the management of adult Attention Deficit Hyperactivity Disorder (ADHD) and cooccurring cardiometabolic disease by improving the identification and treatment of individuals with these comorbidities. In this project, we will process sensitive personal data from available (a) prescription/electronic health record databases and national registers; B) available cohort studies with data collection (for details please see Appendix 1) and newly collected data (Remote measurement technology data via ART-Carma UK and ART-Carma Spain). Extensive work has been and constantly will be devoted to harmonize variables across data sources and to build common protocol(s) and distributed network approach to harmonize study designs, analyses, data cleaning and result outputs across all collaborating sites. This approach is used to adhere to the fact that most data need to stay within each country, cannot be shared in raw form, and must be analysed at the servers of the host university. That is, according to international and national regulations, it is not possible to make data openly accessible and only some partners are allowed to provide access to the data.

TIMESPAN will intensively investigate a huge amount of data. In order to ensure that data is managed properly we will provide an ethical strategy and (FAIR) data management plan (DMP) to allow for maximal transparency, open access/science, usability and reproducibility. Data sustainability will be accomplished by placing all the data management and analyses codes in an online repository (i.e., Github) and by providing a description of how to access raw data of each data source. In addition, we will also maximize transparency and enable future research by presenting aggregated data for all study variables (i.e., made available in the appendix of all publications). We can confirm all data transfers to UK imply GDPR compliance and compliance of the UK databases.

- For details please see D7.2. Data Management Plan.
- For details on data storage and management across sites in the newly collected cohort see Appendix MS52 Interim Report to EDAC on newly collected cohort – already reviewed by the EDAC

Background:

The purpose of collecting new data from detailed day-to-day monitoring of adult ADHD patients through active and passive are:

- Our first main aim is to obtain real-world data from the patient's daily life on the extent to which ADHD medication treatment and physical activity, individually and jointly, may influence cardiometabolic risks in adults with ADHD. This will provide new insights into disease patterns and help improve the safety and effectiveness of pharmacological (i.e., ADHD medication treatment) and non-pharmacological (i.e., physical activity) interventions for patients with ADHD and co-occurring cardiometabolic disease.
- Our second main aim is to obtain in vivo, real-world data from the patient's daily life on adherence to pharmacological treatment and its predictors and correlates, over a remote monitoring period of 12 months that starts from pre-treatment initiation. The long-term goal is to use these data to improve the management of cardiometabolic disease in adults with

ADHD, and to improve ADHD medication treatment adherence and the personalisation of treatment.

Next to that TIMESPAN will also use available data from prescription/electronic health record databases and national registers in Sweden, Denmark, US, Norway, UK, Hong Kong, Iceland and Australia, as well as from the cohort studies with already collected data from Sweden (Lifegene, Swedish Twin registry), the Netherlands (LIFELINE, Trails, Neuroimage), Iceland (SAGA) and Estonia (Estonian Biobank).

1) Prevention of misuse of research participant's data (data security measures to prevent unauthorized access and data breach, anonymization techniques, encryption, secure data transfer, controller processor agreement ensuring high security standards (for the remote collection)). Such measures will mitigate the possible risks for the research participants.

- Access to these data sources have been obtained/are obtained after ethical approval (in the relevant country) and protocol approval (from relevant data source owner).
- Pseudonymized data are then provided to the host (i.e., researcher team at each collaborating site) and data is stored at a secure server at the host university.
- In general, secondary statistical analyses are conducted by the host guided by metadata (for variable harmonization), common protocol(s) and distributed network approach for harmonization of study design, analysis details, data cleaning and result outputs across all collaborating sites
- International and national regulations do not allow making any of the data openly accessible. For example, the Swedish register-data underlying this project contain sensitive personal information and therefore cannot be made openly accessible as they are subject to secrecy in accordance with the Swedish Public Access to Information and Secrecy Act. Researchers may apply for access to the data through the Swedish Research Ethics Boards (www.etikprovningsmyndigheten.se) and from the primary data owners Statistics Sweden (www.scb.se), and the National Board of Health and Welfare (socialstyrelsen.se), in accordance with Swedish law.
- Informed consent:
  - According to national law informed consent is not needed for the available data from prescription/electronic health record databases and national registers in Sweden, US, Denmark-register, Norway, UK, Hong Kong, Iceland, UK and Australia.
  - Informed consent is available for the cohort studies with data collection from Sweden (Lifegene, Swedish Twin registry), the Netherlands (LIFELINE, Trails, Neuroimage), Iceland (SAGA) and Estonia (Estonian Biobank). The Danish iPSYCH cohort data use a system of passive consent together with an easily accessible opt-out option (see further information (only in Danish) at https://nyfoedte.ssi.dk/opbevaring-og-brug-af-proeven).
  - Informed consent are available for the newly collected data in ART-Carma UK and ART-Carma Spain. ART-CARMA has been registered on https://clinicaltrials.gov/.
- Data security:
  - The general approach in TIMESPAN is that all data from prescription/electronic health record databases and national registers and cohort studies with data collection are pseudonymized and all data are stored locally on secure servers at the host university without access to the identity of the individuals. Secure access will require individual investigators to have a user name and password to access the data files. In some WPs, data will be shared with other partners within TIMESPAN. More specifically, personal data will be shared with SUNY, our United States Partner in TIMESPAN. SUNY will be provided with access to prescription/electronic health record databases and national registers from Sweden, Denmark, UK, and Hong Kong, as well as from the available cohort studies with data collection from the Netherlands and Estonia. Iceland will also

share data with Sweden. Only coded pseudonymized data will be shared via remote access. The sharing of data within TIMESPAN will comply with the General Data Protection Regulation and any other applicable law or regulation regarding data sharing. The sharing will be provided after data processing agreement and/or European model contract has been approved by all involved. Data Transfer agreement are in place for some of the data sets and for the others data transfer agreement are still under negotiation with the respective legal departments. At each site there will be a study coordinator (Principal Investigator; PI) responsible for data storage and data management. At each site there is a data protection officer (DPO) appointed to safeguard the rights of the research participants (see D7.2. Data Management Plan).

- Data will be stored locally on a secure server at each host university responsible for a data source. Data will be stored locally 10-30 years at the host university on permanent and secure files following the guidelines for record retention at the host university. Whenever possible, at the end of the project, the data collected within TIMESPAN will be placed in local or national repositories for use by others, according to the ethical procedures of the individual partners.

2) Ethical considerations in relation to AI applications (terms of fairness, discrimination, inequality, avoidance of harm, conflicts of autonomy, beneficence, non-maleficence, justice, the “black box” problem in AI, and accountability).

- Ethical considerations in relation to AI applications are considered and further developed in terms of fairness, discrimination, inequality, avoidance of harm, conflicts of autonomy, beneficence, non-maleficence, justice, the “black box” problem in AI, and accountability.
- Although prediction models can be extremely useful in clinical settings, they can have the unintended effect of continuing or worsening health care disparities. This problem occurs when a model is developed in a group that is heavily weighted toward one ethnic, economic or another social group. That model might not be valid for other groups that had not been represented in the predictive modelling effort. This issue is especially acute for genomic data because most large samples have been collected from people with European-American ancestry. This problem is exacerbated by the fact that machine learning models are a "black box" that does not allow for easy interpretation of these models make their decisions.

TIMESPAN addresses these issues in several ways.

- Key features of our prediction modelling are leveraging existing high-quality health relevant data from multiple sources, creating novel, AI disease-risk models using deep learning neural networks (DLNNs), and assessing their accuracy, reliability, reproducibility and generalisability across countries, ethnicities and genders.
- For genomic data, we are creating an innovative model that uses adversarial learning to assure that our models learn from valid disease associated genomic features rather than features associated with ethnicity, race or ancestry.
- We will adhere to the FAIR data principles and assure the appropriate use and interpretation of our data along with systematic efforts to reduce health care disparities by clarifying the relevance of our algorithms to both genders and to minority groups in the populations studied. We will adhere to the FAIR data principles using the Fairlearn Python functions for machine learning. Fairlearn is an open-source, community project aimed at improving the fairness of AI systems (https://fairlearn.org/). The Fairlearn functions will be integrated into our workflow to assess fairness metrics for racial, ethnic, gender, immigration status and other disparities. We will also apply Fairlearn disparity mitigation strategies as needed to eliminate any disparities detected in our algorithms.
- Although we cannot completely solve the "black box" problem, we will report feature importance scores, which quantify the effect that each feature has in the decision-making process implemented by algorithms. That will provide some insight into potential biases. For example, if socioeconomic status or sex is an important predictive feature, we will need to do

additional modeling of substrata to be sure that such variables are used validly (e.g., as they would be for modeling hypertension) or if they reflect a modeling bias that should be corrected.

- The SUNY site has also led an effort to develop guidelines for reporting machine learning investigations in neuropsychiatry. These standards, which are described in a manuscript submitted for publication, are meant to help researchers avoid errors and misinterpretations, including those that lead to health care disparities.

3. Conclusion

Our Ethics and Data Management Board report (incl. EDAC feedback) describes TIMESPAN ethics and data management implementation as well as a) approaches to prevent misuse of research participant's data and b) ethical considerations in relation to AI applications. The report covers both newly collected data and available data from prescription/electronic health record databases, national registers and cohort studies.

Appendix 1:

Report MS 52 Interim Report to EDAC on newly collected cohort (regarding data storage and management across sites) - already including response from the EDAC that have been addressed by involved partners.

The following report should provide additional information on the newly collected cohort and here mainly regarding data storage and data management across the participating sites KCL and VHIR. Below you can find an overview list of ethical documents that are required for the newly collect cohort (ART-CARMA study).

Ethical documents needed for ART-CARMA study
Research Protocol (it is possible in English but it is mandatory to present a Summary in Spanish)
Participant information sheet
Informed consent form
Study measures (e.g., clinical symptom questionnaires)
Study documents that we share with participants (e.g., Technology User guide)
Confirmation of funding
Confirmation of sponsorship approval
DPIA
List of researchers (For P6VHIR)
Funding source (for VHIR)
CRF (for Spain)
EIPD
CV IP
Study measures (questionnaires, etc.)
Study documents share with participants (Technology User Guide)

General information on data security

We have ensured the highest standards of data security are in place. To maintain participant pseudonomity, their data will be pseudonymised. Their personal information will be stored separately in REDCap from information collected from the apps (including the questionnaires) and wearable. Personal information will only be accessed by the immediate research team for the purpose of contacting the participant during their involvement in the study. EmbracePlus data collected by Empatica will be pseudonymised (dummy information, such dummy name and email address will be entered into the Empatica accounts). Empatica will not have access to personal information or questionnaire data.

Two independent ethics committees have reviewed and given approval for both KCL and VHIR. No concerns over the misuse of research findings related to collection of data on antisocial behaviour through remote technology were raised by the ethics committees. KCL have also received confirmation from the King's Data Protection Office that data collection and processing is being carried out according to EU and national legislation.

Dissemination of research findings from ART-CARMA will be reviewed by the TIMESPAN steering committee/consortium to ensure no objections from TIMESPAN steering committees are raised.

Data storage:

P6 VHIR:

Details on our data processing operations: Data were stored in a standard SQL database. Data can be imported and exported out from the database on many standard data formats. The database can be also accessed using open application programming interface (REST API, ODBC). A database manager will be appointed for data format and collection coordination, curation, preservation, access control and user management. Access to this information and to the identity of the study participants will be strictly restricted to the physicians in charge of the patient and with their explicit authorization to data managers in charge of the study, study monitors and authorized regulatory bodies. The name or any other identifying information of participating patients will not be used in publications resulting from the study.

Details of the security measures to prevent unauthorised access to personal data: Data can be imported and exported out from the database on many standard data formats. The database can be also accessed using open application programming interface (REST API, ODBC). A database manager will be appointed for data format and collection coordination, curation, preservation, access control and user management. Access to this information and to the identity of the study participants will be strictly restricted to the physicians in charge of the patient and with their explicit authorization to data managers in charge of the study, study monitors and authorized regulatory bodies. The name or any other identifying information of participating patients will not be used in publications resulting from the study. All the personal information will be handled according to General Data Protection Rules and this will be explained in detail to the participants. In addition, the following data protection principles will be observed:

- Data are fairly and lawfully processed
- Data are used only for the specified research purpose
- The amount of data collected is relevant and not excessive
- All reasonable efforts are taken to ensure data accuracy
- The data are used in accordance with the rights of data subject
- The data are stored securely

Details of the anonymisation/pseudonymisation techniques. In order to protect the confidentiality of participants' personal data, a series of procedures to maintain secrecy will be enforced: To maintain participant pseudonomity, their data will be pseudonymised. Participant's name will be replaced with a code, which will be randomly generated and a combination of a human readable ID (usually a number), project name, and site location, and the information collected from the apps and wearable will only be associated with this code. Participants are aware of how their data is pseudonymised and this information is included in the Participant Information Sheet. Their personal information will be stored separately from information collected from the apps and wearable.

Details of the data transfers (type of data transferred and country to which it is transferred – for both EU and non-EU countries): The clinical data regarding the phenotype characteristics of the ADHD and the outcomes to measure the pharmacological treatment response. The data will be transferred from Spain to the UK and Sweden. Empatica will collect and store data in Empatica servers on participants' pulse rate, pulse rate variability, temperature, sp02, electrodermal activity and physical activity. EmbracePlus data collected by Empatica will be pseudonymised (dummy information, such as dummy name and email address will be entered into the Empatica accounts). Google Firebase will also store some event log data generated by the app. Participants will be given information about 3rd partied accessing portions of pseudonymised data. Only pseudonymised data will be shared with Empatica. No data access outside European Economic Area (EEA). Third partied will not be making decisions about the data. We can confirm all transfers from VHIR (Spain) to UK imply GDPR compliance and compliance of the UK databases.

P7 KCL:

Details of the security measures to prevent unauthorised access to personal data: All investigators and research workers will comply with the requirements of the Data Protection Act 1998 with regards to the collection, storage, processing and disclosure of personal information and will uphold the Act's core principles.

- All personally identifiable information is kept in REDCap, which is only accessible by the immediate research team.
- All other data are linked through pseudonymised identifiers.

- Transfer of data between different components is secured using industry standards. Data extracted from the platform are also secure and private; only people who have rights can access it.
- Every person accessing the data has an account and is accountable for their actions. Audit rules will be in place.
- The data will be retained in their original form for 10 years, the mapping between personal identifiable data on REDCap and other data types will be deleted, after which only de-identified data are stored.

Data will be placed within the secure network of King's College and Rivest–Shamir–Adleman (RSA) asymmetric public key encryption will be applied to access. All the data will be stored psuedonymised and highly restricted access will be given to specific authorised researchers. Industry grade security will be used to secure data access. Authorised access to secure Storage Server using RSA encryption over Secure Shell (SSH). Access Control Lists (ACLs) and user-groups will be used to control object level permissions in the storage for each user. Information sheet and consent forms will provide details about how participants personal data is handled. Participants will also have the opportunity before giving sign consent to ask the research worker any questions regarding this. All the personal information will be handled according to General Data Protection Rules and this will be explained in detail to the participants.

To maintain participant pseudonomity, their data will be pseudonymised. Participant's name will be replaced with a code, which will be randomly generated and a combination of a human readable ID (usually a number), project name, and site location, and the information collected from the apps and wearable will only be associated with this code. Their personal information will be stored separately in REDCap from information collected from the apps and wearable.

Details of the data transfers (type of data transferred and country to which it is transferred – for both EU and non-EU countries): Empatica will collect and store data in Empatica servers on participants' pulse rate, pulse rate variability, temperature, sp02, electrodermal activity and physical activity. EmbracePlus data collected by Empatica will be pseudonymised (dummy information, such as dummy name and email address will be entered into the Empatica accounts). Google Firebase will also store some event log data generated by the app. Participants will be given information about 3rd partied accessing portions of pseudonymised data. Only pseudonymised data will be shared with Empatica. Third partied will not be making decisions about the data. We can confirm all transfers to UK imply GDPR compliance and compliance of the UK databases

P17 EMPATICA:

Details of the data transfers (type of data transferred and country to which it is transferred – for both EU and non-EU countries): Since sdk is used and it is stored on RADAR cloud. Other than that, the pseudonymised data will be transferred to Italy to our data scientists for analysis.

Details of the anonymisation /pseudonymisation techniques. Data processed by the Empatica is pseudonymised (participant's name is replaced with a code). Empatica will not have access to personal identifiable information. Raw data is recorded to a buffer on the EmbracePlus and transmitted in packets to a paired smartphone when the devices are in range. The entire EmbracePlus system is encrypted and firmware updates are transmitted in an encrypted format that must be decrypted before updates are installed to reduce the likelihood of fraudulent FW being installed. Data from the EmbracePlus is transmitted using the Bluetooth 4.0. The Bluetooth communication settings are configured with one service and one characteristic and the following security provisions:

- Security mode - Level 4
- Security requirement - Level 2
- Encryption Level:
  - STK generation method –'Just Works'- Unauthenticated
  - with bonding

  - encryption key size 56 bits
- Empatica applications that handle Embrace raw data store and transmit the data using encryption. Communication to the Cloud is handled through the SDK and data will be transferred to RADAR.

Strong cryptography and security protocols provide strong authentication, encryption and digital signatures to protect sensitive data and electronic transactions transmitted over open, public networks. For example, SSL/TLS, IPSEC, S/MIME, SSH, etc.
Strong cryptography and security protocols (e.g. AES-256) provide encryption for Customer data stored on server infrastructure.
All remote access protocols used to access information on Empatica server perform encryption.
Only Authorized users/clients will be allowed to access the servers.

Data Management:
General information for the **A**DHD **R**emote **T**echnology study of **ca**rdiometabolic **r**isk factors and **m**edication **a**dherence (‘ART-CARMA’): We have ensured the highest standards of data security are in place. Data are encrypted at all stages of transmission, and are held on secure servers not exposed to the internet. Information is not stored on mobile devices other than for temporary caching, and is cleared once uploaded. Data uploads will happen via wi-fi connections only, to avoid using participants' own data allowances, although any additional burden on contract costs and data usage will be reviewed in the process evaluation. We do not anticipate that participation will be associated with any significant risks of harm to the user. Participants may not necessarily be in contact with healthcare services during the course of the study, but for those that are, their relationships with their care teams will not be impacted.
The project will be conducted per the Declaration of Helsinki and Good Clinical Practice, adhering to principles outlined in the UK Policy Framework for Health and Social Care Research.
Mental capacity will be assumed unless there is evidence to suggest otherwise. Consent procedures will be developed ensuring the material is easy to understand. All project workers responsible for recruiting patients will receive adequate training in taking informed consent.
Participants’ privacy and confidentiality will be respected throughout the course of the study. De-identified data will be encrypted and transferred via internet and Bluetooth connections to secure servers managed by the university. Each participant will be assigned a sequential identification number, used to collect, store, and report participant information. Identifiable information will be stored within a separate password protected eCRF, accessible only to members of the immediate research team. The identification number will be common across the eCRF and the platform.

P6 VHIR:
Details of the technical and organisational measures to safeguard the rights of the research participants: All study investigators shall treat all information and data relating to the study as confidential and with respect to the participant’s privacy. Participating sites team members shall not disclose such information to any third parties or use such information for any purpose other than the performance of the study. Relevant clinical, demographic and self-reported information will be centrally collected in the harmonized electronic Case Report Form (eCRF) designed for this purpose. Epidemiological and patient-related data will be coded in such a way that individual persons cannot be identified from the corresponding data according to the General Data Protection Regulation (EU) 2016/679 (unique pseudocode identifier). Specifically, all identities will be pseudonymized and will be coded with the anonymized identifiers. A separate database will link the unique pseudocode to the participant’s names. The electronic database will be highly secured to protect data.
Details of the anonymisation /pseudonymisation techniques. In order to protecting the confidentiality of participants' personal data, a series of procedures to maintain secrecy will be enforced: To maintain participant pseudonomity, their data will be pseudonymised. Participant’s name will be replaced with a code, which will be randomly generated and a combination of a human readable

ID (usually a number), project name, and site location, and the information collected from the apps and wearable will only be associated with this code. Their personal information will be stored separately from information collected from the apps and wearable. Each individual will be assigned a unique code number (UCN) immediately after collection, project name, and site location, and the information collected from the apps and wearable will only be associated with this code and thus the UCN are devoid of any identifying data. The UCNs serve as the primary identifiers and thus will be used throughout. Personally-identifiable data will not leave the unit from which they originated and will be stored separately to the main project database and inaccessible to unauthorized persons Information from the wearable and smartphone apps will be encrypted (scrambled) so that only the research team can see it. Transfer of data between different components is secured using industry standards. Data extracted from the platform are also secure and private; only people who have rights can access it.

Why can the research objectives not be reached by processing anonymised/ pseudonymised data (if applicable)? All personally identifiable information collected (e.g., name, date of birth, telephone number, email address, home address, diagnosis) is required to identify individuals for recruitment and to maintain contact with participants during the 12-month study period and contact with clinics. All personally identifiable information will be stored separately in REDCap which only the immediate research team can access. All other data will be stored pseudonymised and highly restricted access will be given to specific authorised researchers. Industry grade security will be used to secure data access

- A copy of notification/authorisation for processing of sensitive data (if required) will be made available at month 3, if required.
- We confirm that we comply with the laws of the country where the data was collected. YES.

Our research involves profiling, systematic monitoring of individuals or processing of large scale of special categories of data, intrusive methods of data processing (such as, tracking, surveillance, audio and video recording, geo-location tracking etc.) or any other data processing operation that may result in high risk to the rights and freedoms of the research participants. YES.

- Details on methods used for tracking, surveillance or observing participants:
- Participants will be asked to download three apps onto their phones: the RADAR Passive App and Active App, and the EmbracePlus app (Care App). The first app records passive data, which will run in the background, requiring no further input from participants, and collect data on ambient noise, ambient light, phone usage information, passive audio, Global Positioning System (GPS) location, Bluetooth connectivity, weather conditions, battery life, gyroscope, steps, acceleration. Features of the passive audio, rather than raw audio itself, are extracted from the audio on the phone for transmission. GPS location data will be randomised; that is, providing relative location data, not absolute coordinates. This prevents identification of an individual’s home address or precise geographical location. The second app, collects active data that participants actively provide, such as the completion of questionnaires, providing their weight and blood pressure. Participants will also be asked to wear an EmbracePlus during the study period and download the Empatica Care App EmbracePlus combines the precision of Empatica’s validated biomarkers with a comfortable design, enabling high-accuracy measurement of heart rate and heart rate variability, interbeat interval, electrodermal activity (EDA), autonomic stress, physical activity and sleep.
- How will harm be prevented and the rights of the research participants safeguarded? Explain: In order to protecting the confidentiality of participants' personal data, a series of procedures to maintain secrecy will be enforced: Each individual will be assigned a unique code number (UCN) immediately after collection, and these UCN are devoid of any identifying data. The UCNs serve as the primary identifiers and thus will be used throughout. Personally-identifiable data will not leave the unit from which they originated and will be stored separately to the **main project database and inaccessible to unauthorized persons.**

How will the rights of the research participants be safeguarded? Explain: In order to protecting the confidentiality of participants' personal data, a series of procedures to maintain secrecy will be enforced: Each individual will be assigned a unique code number (UCN) immediately after collection, and these UCN are devoid of any identifying data. The UCNs serve as the primary identifiers and thus will be used throughout. Personally-identifiable data will not leave the unit from which they originated and will be stored separately to the main project database and inaccessible to unauthorized persons. Data will be started only after subjects have read the information sheet and have signed the informed consent form.

We will use only data and information relevant for the objectives of TIMESPAN project. Data not related with the final objectives of TIMESPAN will not be processed. We confirm the lawful basis for the data processing.

There may be several reasons for withdrawal from the study:

1. Participant choosing to no longer participate: participants will be informed both in writing and verbally that participation is voluntary, that non-participation will not influence their medical care, and that they are free to withdraw from the study at any point without providing reasons.
2. The research team may withdraw the participant in the event of inter-current illness, adverse event (AE), protocol violation, administrative or other reasons.

In the case of participant self-withdrawal, all attempts will be made to follow-up with the participant to establish cause of withdrawal, and to collect qualitative data regarding experience of participation. All data, including those from withdrawn participants, will be included in the final analysis. If a participant withdraws from the study prematurely, we will consider replacing the participant if resources allow and if recruitment is ongoing for the study.

Our research includes export of personal data from the EU to non-EU countries. YES.

- The clinical data regarding the phenotype characteristics of the ADHD and the outcomes to measure the pharmacological treatment response. The data will be transferred from Spain to the UK. Empatica will collect and store data in Empatica servers on participants pulse rate, pulse rate variability, temperature, sp02, electrodermal activity and physical activity. EmbracePlus data collected by Empatica will be pseudonymised (dummy information, such as dummy name and email address will be entered into the Empatica accounts). Google Firebase will also store some event log data generated by the app. Participants will be given information about 3rd partied accessing portions of pseudonymised data. Only pseudonymised data will be shared with Empatica. No data access outside European Economic Area (EEA). Third partied will not be making decisions about the data. How will the rights of the research participants be safeguarded? Explain:
- In order to protecting the confidentiality of participants' personal data, a series of procedures to maintain secrecy will be enforced: Each individual will be assigned a unique code number (UCN) immediately after collection, and these UCN are devoid of any identifying data. The UCNs serve as the primary identifiers and thus will be used throughout. Personally-identifiable data will not leave the unit from which they originated and will be stored separately to the main project database and inaccessible to unauthorized persons.
- We confirm that we comply/will comply with Chapter V of the GDPR. YES

P7 KCL:

Details of the technical and organisational measures to safeguard the rights of the research participants: A data protection impact assessment (DPIA) has been completed. KCL's Data Protection Officer (DPO), Mr Albert Chan (info-compliance@kcl.ac.uk), was involved in this. The DPO contact details will be provided on the Information Sheet so that participants can contact him if they have any questions about their data. To safeguard participants rights, we will use the minimum personally-identifiable information possible.

Details of the anonymisation /pseudonymisation techniques: To maintain participant pseudonomity, their data will be pseudonymised. Participant's name will be replaced with a code, which will be randomly generated and a combination of a human readable ID (usually a number), project name, and site location, and the information collected from the apps and wearable will only be associated with this code. Their personal information will be stored separately in REDCap from information collected from the apps and wearable. Participants name will be replaced with a code, which will be randomly generated and a combination of a human readable ID (usually a number), project name, and site location, and the information collected from the apps and wearable will only be associated with this code. Information from the wearable and smartphone apps will be encrypted (scrambled) so that only the research team can see it. Transfer of data between different components is secured using industry standards. Data extracted from the platform are also secure and private; only people who have rights can access it. Pseudonymised data will be securely stored on servers managed by the Institute of Psychiatry, Psychology and Neuroscience, KCL, and also on 3rd party servers, which can provide additional security and backup. These data will not be linked back to participants personal information. All details of how data is pseudonymised will be included in the Information Sheets and Informed Consent Forms.

Details of the data transfers (type of data transferred and country to which it is transferred – for both EU and non-EU countries): All electronic data collected will be streamed to Amazon Elastic Kubernetes System (EKS) server where the RADAR-base platform will be deployed for data collection. Amazon EKS servers will be located in London (UK), adhering to GDPR. Access to RADAR-base stack on Amazon EKS is restricted to system administrators, de-identified archival data storage for the project will be held in a KCL data centre in the SGDP sFTP storage. Authorised access to the data will be restricted to data scientists and analysts. SSH-RSA encryption, sFTP access, Access Control Lists (ACLs) and user-groups will be used to control object-level permissions in the storage for each user. Data collected by Empatica will be pseudonymised (dummy information, such dummy name and email address will be entered into the Empatica accounts). EmbracePlus sensor data will be streamed to Amazon S3 (GDPR compliant) and then pulled to secure sFTP storage placed in KCL.

Details on methods used for tracking, surveillance or observing participants: Participants will be asked to download three apps onto their phones: the RADAR Passive App and Active App, and the EmbracePlus app (Care App). The first app records passive data, which will run in the background, requiring no further input from participants, and collect data on ambient noise, ambient light, phone usage information, passive audio, Global Positioning System (GPS) location, Bluetooth connectivity, weather conditions, battery life, gyroscope, steps, acceleration. Features of the passive audio, rather than raw audio itself, are extracted from the audio on the phone for transmission. GPS location data will be randomised; that is, providing relative location data, not absolute coordinates. This prevents identification of an individual's home address or precise geographical location. The second app, collects active data that participants actively provide, such as the completion of questionnaires, and recording their weight and blood pressure. Participants will also be asked to wear an EmbracePlus device during the study period. EmbracePlus combines the precision of Empatica's validated biomarkers with a comfortable design, enabling high-accuracy measurement of heart rate and heart rate variability, interbeat interval, EDA, autonomic stress, physical activity and sleep.

Details of the methods used for profiling: Multivariate statistical and machine learning approaches including unsupervised clustering and supervised classification/regression and time series analysis will be performed.

Risk assessment for the data processing activities: We will follow standard guidelines and a DPIA has been completed with support from King's Data Protection Officer, Mr Albert Chan (infocompliance@kcl.ac.uk).

P16 EMPATICA:

Our research involves personal data processing. YES.

Empatica deals with different users, for example in the case of research, the only personal data we have is of the researcher and we have no way to identify subjects based on the data collected by the researchers, only they have the „key“ to identify subjects.

Details of the security measures to prevent unauthorised access to personal data. User's personal data will be processed both electronically and/or manually, in any case in such a way as to guarantee the security, protection and confidentiality of the data, thanks to appropriate administrative, technical, personnel and physical measures against loss, theft and unauthorized use, disclosure or modification.

How is all of the processed data relevant and limited to the purposes of the project ('data minimisation' principle)? Explain: The processing of the User's personal data with regard to the Legitimate Interest Purposes (i) the measurement of the service quality and relevant metrics provided through Device and the App; (ii)the management of complaints and disputes; (iii) the performance of the activities necessary to ensure compliance with the applicable national/EU laws and/or respond to request from public and government authorities (iv) the performance of tests, updates and developments of Device, the App and more in general the services provided by Empatica, in order to optimize the services provided to the User also by way of machine learning systems and artificial intelligence provided that the process of personal data, albeit limited to the necessary, is essential in order to carry out such tests activities; is carried out in compliance with article 6, letter f) of the EU General Data Protection Regulation No. 679/2016 (the "Privacy Regulation"), for the pursuit of Empatica legitimate interest, which is adequately balanced with the User's interest since the data processing is performed within the limits strictly necessary to perform such activities. This data processing activity with regard to the Legitimate Interest Purposes is not mandatory and the User can object to the data processing at any time through the modalities

Justification of why research data will not be anonymised/ pseudonymised (if relevant): To protect the subjects identity and prevent parties not directly dealing with the subjects to identify them.

In Empatica's part, we don't expect to get personally identifiable data, only physiological and other health data with some demographic data. The physiological data is pseudonymised. It is necessary to help further refine the analyses and account for differences between subjects groups such as age, gender, etc.

From Empatica wearable, we can get:

- Raw physiological data (RPD) – Any information measured by a sensor available in the Empatica hardware
- Processed physiological data (PPD) – Any information inferred by the analysis of a RPD, (i.e. seizure data)
- Meta data (MDA) – Any information added by the user of Empatica system giving additional information concerning a portion of PPD or RPD (i.e. ground truth, reported seizure)
- Hardware data (HWD)– Any information related to a device including test reports, configuration etc.

Data Team member can access any information of physiological data excluding personal information: RPD, PPD, MDA, HWD

Sensitive systems are provided with dedicated (isolated) computing environment such as running on a dedicated computer, share resources only with trusted application systems.

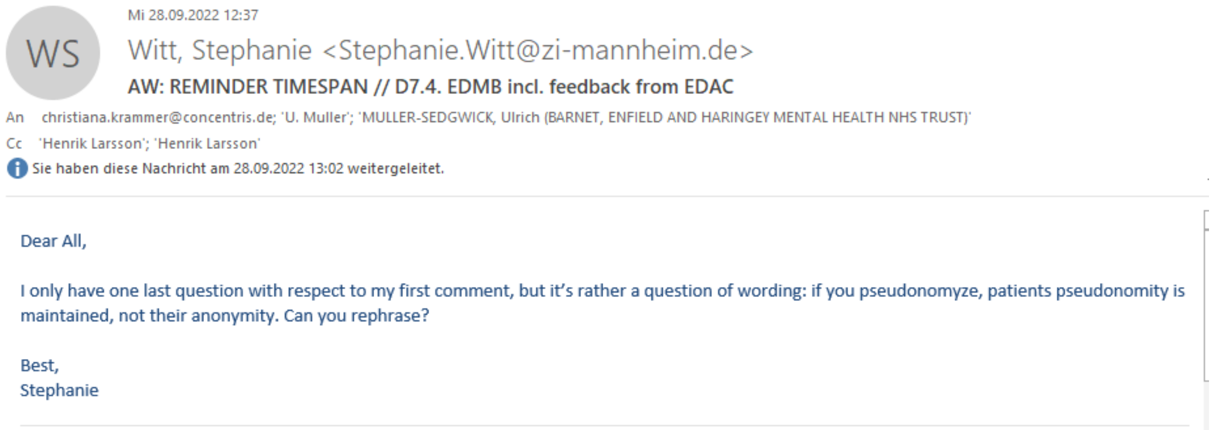
Empatica system allows flexible export of data in open formats

- JSON
- CSV (Command separated values)

Our research involves the processing of genetic, biometric or health data: YES.

We confirm that we comply with the laws of the country where the data was collected. NO. EMPATICA complies with HIPA and GDPR but not country specific regarding collection and data storage.

This deliverable report has been reviewed by the TIMESPAN EDAC. All suggested changes have been included.



Mi 28.09.2022 12:37

Witt, Stephanie <Stephanie.Witt@zi-mannheim.de>

AW: REMINDER TIMESPAN // D7.4. EDMB incl. feedback from EDAC

An christiana.krammer@concentris.de; 'U. Muller'; 'MULLER-SEDGWICK, Ulrich (BARNET, ENFIELD AND HARINGEY MENTAL HEALTH NHS TRUST)'

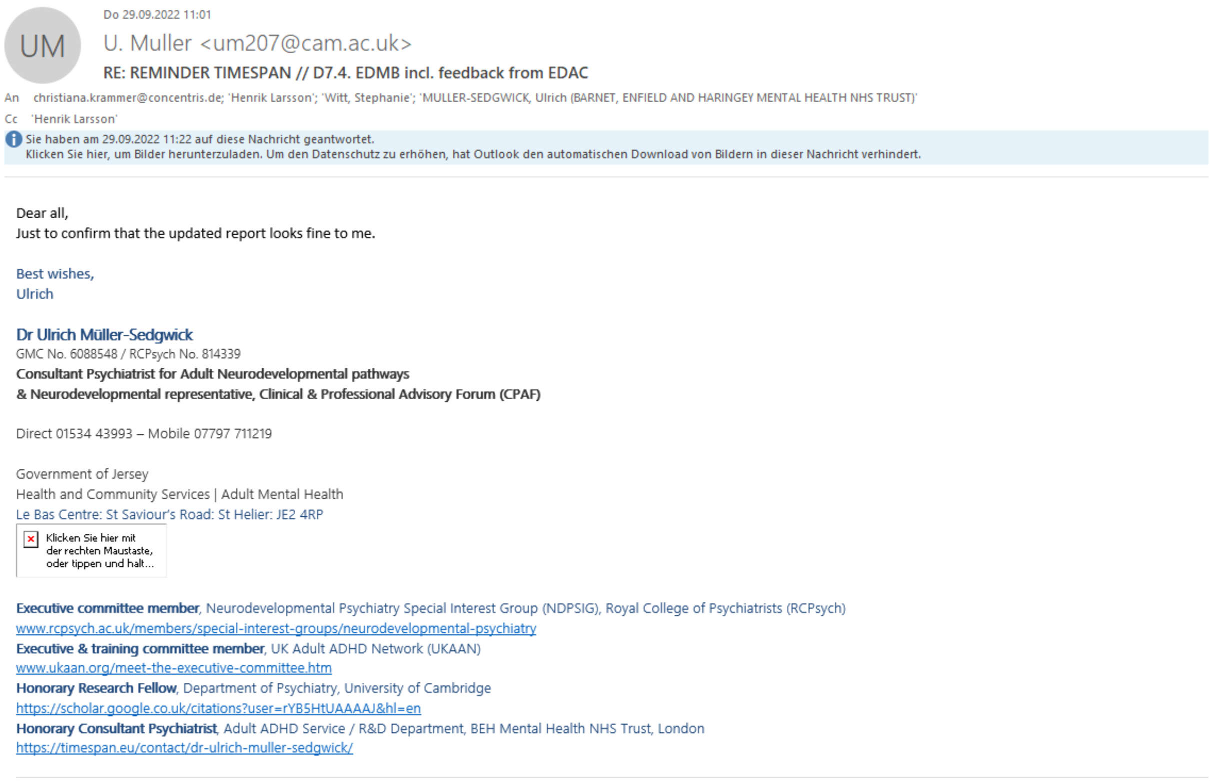
Cc 'Henrik Larsson'; 'Henrik Larsson'

Sie haben diese Nachricht am 28.09.2022 13:02 weitergeleitet.

Dear All,

I only have one last question with respect to my first comment, but it's rather a question of wording: if you pseudonomyze, patients pseudonomity is maintained, not their anonymity. Can you rephrase?

Best,
Stephanie



Do 29.09.2022 11:01

U. Muller <um207@cam.ac.uk>

RE: REMINDER TIMESPAN // D7.4. EDMB incl. feedback from EDAC

An christiana.krammer@concentris.de; 'Henrik Larsson'; 'Witt, Stephanie'; 'MULLER-SEDGWICK, Ulrich (BARNET, ENFIELD AND HARINGEY MENTAL HEALTH NHS TRUST)'

Cc 'Henrik Larsson'

Sie haben am 29.09.2022 11:22 auf diese Nachricht geantwortet.
Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Dear all,
Just to confirm that the updated report looks fine to me.

Best wishes,
Ulrich

Dr Ulrich Müller-Sedgwick
GMC No. 6088548 / RCPsych No. 814339
Consultant Psychiatrist for Adult Neurodevelopmental pathways
& Neurodevelopmental representative, Clinical & Professional Advisory Forum (CPAF)

Direct 01534 43993 – Mobile 07797 711219

Government of Jersey
Health and Community Services | Adult Mental Health
Le Bas Centre: St Saviour's Road: St Helier: JE2 4RP

Klicken Sie hier mit der rechten Maustaste, oder tippen und halt…

Executive committee member, Neurodevelopmental Psychiatry Special Interest Group (NDPSIG), Royal College of Psychiatrists (RCPsych)
www.rcpsych.ac.uk/members/special-interest-groups/neurodevelopmental-psychiatry
Executive & training committee member, UK Adult ADHD Network (UKAAN)
www.ukaan.org/meet-the-executive-committee.htm
Honorary Research Fellow, Department of Psychiatry, University of Cambridge
https://scholar.google.co.uk/citations?user=rYB5HtUAAAAJ&hl=en
Honorary Consultant Psychiatrist, Adult ADHD Service / R&D Department, BEH Mental Health NHS Trust, London
https://timespan.eu/contact/dr-ulrich-muller-sedgwick/