ehcoBUTLER

Data Management Plan

ehcoBUTLER Project

Version: 1.08
April 30th2015

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

DOCUMENT CONTROL

Title: Data Management Plan

Date: April30th 2015

Author: YourDATA s.r.l.

Distribution: Public

Project: ehcoBUTLER (GA 643566)

Filename: ehcoBUTLER_DMP_Data_Management_Plan_v01r08f.docx

DOCUMENT CHANGE RECORD

Date	Version	Author	Change Details
Apr 13th 2015	1.00	YourDATA	Initial Version
Apr 14th 2015	1.01	everis	Revision
April 15th 2015	1.02	YourDATA	Revision
April 20th 2015	1.03	NFE	Input section 1, 2 and 3 Revision
April 20th 2015	1.04	CIBER	Input section 1, 2 and 3 Revision
April 27th 2015	1.05	YourDATA	Revision
April 28th 2015	1.06	YourDATA and NFE	Revision
April 29th 2015	1.07	YourDATA	Revision
April 30th 2015	1.08	YourDATA and everis	Final version

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

TABLE OF CONTENTS

1 INTRODUCTION 4
1.1 Purpose of this document. 4
1.2 Intended audience 4
1.3 Overview of the document 4
1.4 References and applicable documents 5
1.5 Terminology 5
1.5.1 Abbreviations and acronyms 5
1.5.2 Definitions 5
1.5.3 Additional Definitions 5
2 DATA SET 6
2.1 Description of data 6
2.1.1 What data will we collect? 6
2.1.2 How will the data be collected or created? 6
2.1.3 What documentation and metadata will accompany the data? 8
2.1.4 How will we manage copyright and Intellectual Property Rights (IPR) issues? 8
2.1.5 How will the data be stored and backed up during the research? 9
2.1.6 How will we manage access and security? 10
2.1.7 Which data should be retained, shared, and/or preserved? 11
2.1.8 What is the long-term preservation plan for the dataset? 12
2.1.9 Who will be responsible for data management? 12
3 ETHICAL AND LEGAL ISSUES 13
3.1 Ethical Issues 13
3.2 Privacy 13
3.3 Risk related to data and privacy 13
4 HISTORY OF CHANGES 14
4.1 Version 1.00 (YourDATA) 14
4.2 Version 1.01 (Everis) 14
4.3 Version 1.02 (YourDATA) 14
4.4 Version 1.03 (NFE) 14
4.5 Version 1.04 (CIBER) 14
4.6 Version 1.05 (YourDATA) 14
4.7 Version 1.06 (NFE and YourDATA) 14
4.8 Version 1.07 (YourDATA) 14
4.9 Version 1.08 (YourDATA and everis) 14

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

1 INTRODUCTION

1.1 Purpose of this document.

The Data Management Plan (DMP) purposes are:

- to support the data management life cycle for all data that will be collected, processed or generated by the Project,
- to provide an analysis of the main elements of the data management policy that will be used by the applicants with regard to all the datasets that will be generated by the Project;
- to provide detail and guarantee about the preservation of the data collected during the Project, as well as any results derived from the associated research;
- to provide detail on how we plan to address the Ethical issues related to data that will be collected during the Project timeframe;
- to create a document which explains the management of data collected during the Project.

The DMP is not a fixed document, but evolves during the Project.

1.2 Intended audience

This document is oriented to:

- the project's participant organizations;
- the local Ethics Committee;
- the beneficiaries' personnel and all stakeholder involved by the Project;
- the European Commission.

1.3 Overview of the document

This document contains details on:

- a brief description of data types which will be collected during the Project, explaining the procedures used to collect or create them;
- the typology of information needed to read and interpret the data and the needed documentation to help reader to understand and reuse the data. It will be coherent with the Commission Recommendation of 23rd June 2009 number 498;
- copyright and IPR issues;
- ethical issues related to data storage, persons authorized to see/use them and how long they are kept; managing ethical concerns that include the anonymization of data; procedures used to obtain the consent requested to allow data sharing and reuse;
- description of the procedures used to obtain the consent requested to allow data sharing and reuse;
- a brief description of ethic committees.

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

1.4 References and applicable documents

Commission Recommendation of 23 June 2009 on reference metadata for the European Statistical System (2009/478/EC)

1.5 Terminology

1.5.1 Abbreviations and acronyms

- **EC**: European Commission.

1.5.2 Definitions

Words beginning with a capital letter shall have the meaning defined either herein or in the Rules or in the Grant Agreement related to the Project;

1.5.3 Additional Definitions

- **Project**: Project refers to the ehcoBUTLER project funded from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566;

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

2 DATA SET

2.1 Description of data

The data that will be gathered in ehcoBUTLER is mostly related to personal data of ehcoBUTLER solution's end users, which will be collected during trials at the project's Pilot sites. Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link. Examples of such data are factors that link to a person's physical, physiological, mental, economic, cultural or social identity. The definition is very broad and coves any information related to an identifiable, living individual. Processing is also broadly defined and involves any manual or automatic operation (paper, IT, CCTV system, etc.) on personal data, including its collection, recording, organization, storage, modification, retrieval, use, transmission, dissemination or publication, and even blocking, erasure or destruction (Directive 95/46/EC, Article 2b).

2.1.1 What data will we collect?

Several types of data will be collected and analysed during the research in the Project. This data consists of end-user information obtained through the interaction with the ehcoBUTLER system and through the research with end users during the pilot and in other phases of the Project.

This data will be accessible for the Project researchers to reach the Project objectives. In addition it can be made accessible for caregivers, care professionals or family members with consent from primary end user according to the research phase or specific pilot characteristics. The overall kind of data will be the needs of health of users. Another kind of data which will be managed during the Project will be related to care professionals, user's family members or informal carers.

Mainly, the data that will be collected are:

- Age
- Gender
- Technological skills
- Educational level
- Living situation
- Care support
- Cognitive health level (MMSE)
- Self-rated health status
- Self-rated mobility status
- Nutrition requirements
- Mood condition
- Activities
- Interaction with ehcoBUTLER

2.1.2 How will the data be collected or created?

End user data will be collected through different means according to the research phase of the Project. Data will be gathered from surveys, questionnaires, user tests and pilot tests. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive lays down a series of rights on how to collect and create data.

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

These are:

- The right of access to his/her personal data;
- The right of erasure, blocking, or rectification of the data, which do not comply with
- The provisions of the Directive, are incomplete or inaccurate;
- The right to be informed of all relevant details relating to the data processing and the rights granted to him/her;
- The right to a judicial remedy for any breach of the above mentioned rights.

The rules according to the directive are:

- Data must be processed fairly and lawfully.
- They must be collected for explicit and legitimate purposes and used accordingly.
- Data must be relevant and not excessive in relation to the purpose for which they are processed.
- Data must be accurate and where necessary, kept up to date.
- Data controllers are required to provide reasonable measures for data subjects to rectify, erase or block incorrect data about them.
- Data that identifies individuals must not be kept longer than necessary.

Personal data can only be processed (e.g., collected and further used) if:

- The data subject has unambiguously given his or her consent, i.e. if he or she as agreed freely and specifically after being adequately informed;
- Data processing is necessary for the performance of a contract involving the data subject or in order to enter into a contract requested by the data subject, e.g. processing of data for billing purposes or processing of data relating to an applicant for a job or for a loan;
- Processing is required by a legal obligation;
- Processing of data is necessary to protect an interest that is essential for the data subject's life. An example is in the case of a car accident and the data subject is unconscious; emergency paramedics are allowed to give blood tests if it is deemed essential to save the data subject's life;
- Processing is necessary to perform tasks of public interests or tasks carried out by official authorities (such as the government, the tax authorities, the police, etc.).

Finally, data can be processed whenever a party has a legitimate interest in doing so. However, this interest cannot override the interests or fundamental rights of the data subject, particularly the right to privacy. This provision establishes the need to strike a reasonable balance, in practice, between the business's interest of the data controllers and the privacy of data subjects. This balance is first evaluated by the data controllers, under the supervision of the data protection authorities, although, if required, the courts have the final decision.

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

2.1.3 What documentation and metadata will accompany the data?

The documentation that will accompany the data will be coherent with the Commission Recommendation of 23rd June 2009 number 498.

Thus, data will contain information about:

- Contacts: Individual or organizational contact details of persons in charge of data management.
- Metadata update: information indicating the date of last version of data (or modifications occurred).
- Statistical presentation indicating: basic description of data, sector of coverage, statistical unit for which data have been collected, statistical population, reference area, time coverage.
- Unit of measure.
- Reference period.
- Project funding information: European Union logo and information about Grant Agreement and the action/program that funds the project.
- Institutional mandate including procedures for data sharing and coordination between data producing agencies.
- Confidentiality: property of data indicating the extent to which their unauthorised disclosure could be prejudicial or harmful to the interest of the source or other relevant parties.
- Release policy including dissemination rules and purposes.
- Information about data collection (source, frequency and adjustments)
- Comments.

2.1.4 How will we manage copyright and Intellectual Property Rights (IPR) issues?

The IPR ownership is defined by the Consortium Agreement and Grant Agreement related to Project.

Such access will be provided by accepting the terms and conditions of use, as appropriate. Materials generated under the Project will be disseminated in accordance with Consortium Agreement. Those that use the data (as opposed to any resulting manuscripts) shall cite it as follows:

The data created by the ehcoBUTLER project, funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 643566. For reuse of this data, please, contact ehcoBUTLER Consortium. www.ehcoBUTLER.eu.

This information will be described also in the metadata.

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

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

The data will be managed by collaborators of participants as well as other scientists interested in ehcoBUTLER relationships.

The knowledge generated by the Project among partners, scientific community, target users and public at large during the Project are managed in two ways, depending on the data source:

1. The non-sensitive data will be organized into a repository that will contain all the knowledge produced by the Project partners. A restricted access is expected for the knowledge that will be used for exploitation purposes; open access for all the other knowledge. Specific attention must be paid to the creation of an open access to the data collected during the trials. To this end, row data will be organized in an exportable format to be used by the scientific community and practitioners for their own purposes. A registered access for data download will be the only request for their use, in order to understand which organization is interested in using them and for which particular scope.

2. To manage and store the sensitive data obtained, all partners from ehcoBUTLER must comply with relevant European and national regulations as well as with the standards of practice defined by relevant professional boards and institutions.

The EU legislation standards for human studies include the following regulations as for the protection of individuals:

- The Declaration of Helsinki in its latest version (recommendation for conduct of clinical research).

- Directive 95/46/EC on the protection of individuals with regard to processing of personal data and on the free movement of such data Council Directive 83/570/EEC amending Directives 65/65/EEC, 75/318/EEC and 75/319/EEC dealing with proprietary medicinal products.

- Directive 95/46/EC (amendment 2003) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the protection of privacy, storing of personal data and on the free movement of such data.

- The charter of fundamental rights of the EU (2000/C 364/01).

- EU Good Clinical Practice Directive (2001/20/EC).

All researchers and clinical professionals involved in the ehcoBUTLER project will comply with the ethical guidelines of their respective professional associations. They should to process private data will respect Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free transfer of such data, all relevant national legislation and regulations and the specific regulations of the institutions in which the trials will take place. In cases where local regulations on privacy or data protection deviate from EU standards, partners must adopt the criteria that provides the strongest protection for participants.

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

Protection of the privacy of participants implies that the subjects have a number of rights that must be respected:

- The right of access to his / her personal data.
- The right of erase, blocking or rectification of the data.
- The right to be informed of all relevant details relating to the data processing and the rights granted to him/her.
- The right to start a judicial process if any violation of the above mentioned rights has been produced.

So, participant can control the access to personal information; he/she decides who has access to the collected data in the future.

No data will be collected or used without the explicit informed consent of the participants. An informed consent form must be given to each participant before the data collection.

The informed consent allows to Individuals to choose in a freely way to participate or not into the trial. The written information is based on the revised version of the Helsinki Declaration of 1964, as lastly amended in Tokyo, 2004, and the Convention of the Council of Europe on Human Rights and Biomedicine (1997). It is fundamental that the consent form includes the indication of how any data storage and handling processes will ensure data protection and confidentiality, that is, description of the procedures for protecting the confidentiality of such personal data. Therefore, participants from ehcoBUTLER should be informed about the confidentiality policy that is used in the research.

As for the development of the databases and documents derived from the data collection, the confidentiality must be strictly maintained. Is not allows that the researcher or other people involved in the trial transfer sensitive data without anonymize it. There are solutions to maintaining confidentiality such as the replacement of the names by codes, keeping the list that links the codes and the names in a secure place with restricted access, encryption of the data, use of secure passwords, and regulations of data access. All personal contact information required will be destroyed at the end of the trial.

In addition, the researchers in the study will not reveal sensitive data about the participants. These same principles will be taken into consideration in the dissemination of data.

2.1.6 How will we manage access and security?

The ehcoBUTLER project will follow the relevant legislation in the countries participating in this project and any applicable EU legislation regarding data protection. Procedures for the collection and storage of personal data will comply with relevant European regulations and directives, in particular with Directive 1995/46/CE on data protection, 1997/66/CE on the handling of personal information and Directive 2002/58/CE (on the same subject).

The Data Management task of ehcoBUTLER focuses on the importance of secure storage, management, and accessing the research information; data must be stored in a secure environment with control access and other security measures obeyed (e.g., proper temperature control). Additionally, sensitive information needs to be stored in the appropriate hardware means, in the appropriate structure and format, corresponding to the related requirements (e.g., paper, disk, etc.). Accessibility to the information needs to be maintained controlled and the networking configurations should not allow data duplication of circulation.

Access to the data files will be restricted to researchers and clinicians involved in the study. Staff involved will be required to sign a confidentiality statement. Only authorized research personnel will be aware of this personal information. For research purposes each participant will be given a numerical code.

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

Main points within the data protection will be the rigorous encryption of participants' data for data transmission with state of the art methods, pseudonymisation, maintenance of data integrity, regulations for data access. Unauthorized access is not possible. In order to protect all information, we will follow the AES (Advanced encryption Standard) strategies for personal password use and data encryption. All personal contact information required during the trials for organizing follow-up assessment will be destroyed at the end of the trial. The researchers in the study will not reveal data from which personal and health information about the participants could be deduced. The same principles will be taken into consideration in the dissemination of data in the publication of scientific papers and the presentation of research reports at scientific conferences.

Data transfer in both electronic and other ways will, therefore, be monitored. Data storage and management considerations also impose thoughts concerning (a) the duration of storage of the sensitive information and (b) if any back up policies shall be implemented. For example, the duration of the storage should define the extent of time needed until destruction of the data occurs, in accordance with the level of importance of the data. This procedure ensures avoidance of the inappropriate use and dissemination of the information.

In the scope of WP2 on the user requirements, iterative evaluations, and pilot studies in WP5, the ehcoBUTLER project will record and store information about end users. This data will be managed in WP7 and used for analysis in WP8.

Any questionnaires or input acquired in the scope of the ehcoBUTLER user involvement processes (especially WP2 and WP5) will be handled in the strictest confidence – the results will be entered immediately into a database or XLS files from where each set of results will be given an automatic number and the personal details omitted. The questionnaires themselves will be kept in a folder, which is kept in a lockable drawer. The questionnaires will be destroyed at the end of the Project. Additionally, all personal data can be modified and even erased on request from the person, e.g., on an XLS file or via an easy to use interface on the related ehcoBUTLER databases. Also, the user should be able to inquire about his/her stored data.

Secure data destruction: In order to prevent the crack of sensitive data and the leak of insecure information, the Project intends to apply safe methods one destructing its data, after the extent of their need. The aim is to guarantee that data is completely destroyed with absolutely no chance of retrieval and deny unauthorized access to any information. The way of destruction depends on the type of the files. Various techniques will be applied in paper, CDs, DVDs, floppy disks, USB drives, etc. The responsible deconstruction staff that will deal with encrypted data will be examined and have signed confidential agreements.

Anonymization: Anonymization will be used to protect the user's identity. This means that only relevant attributes, i.e., gender, age, etc., are documented. The name of the test persons and any kind of identification data will appear on the consent forms, of which one copy is kept by the Project investigator and the other one by the person participating in the ehcoBUTLER user requirements processes. All data will then be anonymized by assigning a numerical code to each user (local database), and stored accordingly (e.g., Subject 1, Subject 2, etc.). All data will also be anonymized in internal reports, internal communications and external publications (e.g., paper publications or the deliverables).

2.1.7 Which data should be retained, shared, and/or preserved?

Information about people such as their age, lifestyle, health, information about relatives or relationships, scientific tests, surveys and interviews

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

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

The dataset associated to users of a specified pilot partner will be conserved according their national laws regarding data protection.

Each Member State participating in the ehcoBUTLER project must provide one or more supervisory authorities to monitor the application of the Directive. Member States may provide for simplification or exemption from notification for specific types of processing that do not entail particular risks. Exception and simplification can also be granted, in conformity with national law, when the controller has appointed an independent officer in charge of data protection. Member States may require prior checking, to be carried out by the supervisory authority, before data processing operations that involve particular risks may be undertaken. Which types of processing operations involve particular risks is for the member states to determine.

All user involvement activities will be performed respecting the Helsinki Agreement (2001/20/EC), Oviedo Convention and the European Charter of Fundamental Rights. All pilots will fully comply with relevant European and national regulations and with the standards of practice defined by relevant professional boards and institutions. In cases in which local ethical regulations deviate from EU standards, the project will adopt the criteria providing the strongest protection for trial participants.

2.1.9 Who will be responsible for data management?

Each partner must authorize a responsible of data management who will take the responsibility to control the correct storage, management, sharing and security of the dataset.

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

3 ETHICAL AND LEGAL ISSUES

3.1 Ethical Issues

The Project will be clearly explained to each participant. Personal details and health details will not be collected from participants. They will be informed that data collected from the focus group discussions will be anonymised and not published; if any personal information is shared during the discussions it will be deleted as it is not the intention of the Project to collect such data or publish them. Participants will be asked to sign a consent form, which specifies what kind of data will be collected and how they will be managed and used.

3.2 Privacy

Personal views from focus groups will be anonymised and participants will be requested to observe the same confidentiality as the researcher (i.e. Comments made will be non-attributable and the identity of the participants will not be revealed). Personal details and health details will not be collected from participants; any personal information / personal issue shared during the discussions will be deleted as it is not the intention of the Project to collect such data or publish it.

3.3 Risk related to data and privacy

The Project will implement several security measures and protocols. The consortium will pursue the fulfillment of the European Directive during the Project and all sensible data will be encrypted and protected during storage and transmission (which takes place across third-party networks (such as the Internet) so that user's identity and privacy will not be compromised. Integration with standards available security and authenticity technologies, such as single sign-on management or LDAP will be analysed. Various implementations will provide a level of user-security in accordance with open-source security standards. State of the art firewalls, network security, encryption, and authentication will be used to protect collected data. Firewalls prevent the connection to open network ports and exchange of data will be through consortium known ports, protected via IP filtering and password. Where possible (depending on the facilities of each partner and pilot site), the data will be stored in a locked server, and all identification data will be stored separately. A metadata framework will be used to identify the data types, owners, and allowable use. This will be combined with a controlled access mechanism and in the case of wireless data transmission with efficient encoding and encryption mechanisms. Pretty Good Privacy (PGP) technology could be used to provide cryptographic privacy and authentication for data communication. PGP could be used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions.

The security of precious data demands the ability to avoid data theft regardless of the level of cracking techniques. Therefore, the encryption, file and record locking, integrity, the passwords mechanisms as well as the traceability of the data acquisition systems will have be constantly updated to prevent the possibility of decoding the data management system in any level and disseminating private information.

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566

4 HISTORY OF CHANGES

4.1 Version 1.00 (YourDATA)

Initial version

4.2 Version 1.01 (Everis)

- Minor grammar and orthographical changes.
- Format & Style revision
- Contributions to be added included

4.3 Version 1.02 (YourDATA)

- Minor grammar and orthographical changes.
- Format & Style revision.
- Contributions added.

4.4 Version 1.03 (NFE)

- Minor grammar and orthographical changes.
- Format & Style revision.
- Contributions added.

4.5 Version 1.04 (CIBER)

- Minor grammar and orthographical changes.
- Format & Style revision.
- Contributions added.

4.6 Version 1.05 (YourDATA)

- Minor grammar and orthographical changes.
- Format & Style revision.
- Contributions added

4.7 Version 1.06 (NFE and YourDATA)

- Minor grammar and orthographical changes.
- Format & Style revision.
- Contributions added

4.8 Version 1.07 (YourDATA)

- Minor grammar and orthographical changes.
- Format & Style revision.
- Contributions added.

4.9 Version 1.08 (YourDATA and everis)

- Minor grammar and orthographical changes.
- Format & Style revision.
- Final version

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 643566