Abstract
This document describes the ethical and privacy guidelines regarding the PRECIOUS system and service implementation. The document provides information on how PRECIOUS follows the EU fundamental ethical principles, including those reflected in the Charter of Fundamental Rights of the European Union. The document also takes into account the opinion of the European Group on Ethics in Science and New Technologies. The document provides detailed information regarding how these issues are managed and taken into consideration in the planning and design of the service.
<table>
<thead>
<tr>
<th><strong>Nature:</strong></th>
<th>R (R: Report, P: Prototype, O: Other)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dissemination Level:</strong></td>
<td>PU (CO: Confidential, PU: Public)</td>
</tr>
<tr>
<td><strong>Version:</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Date:</strong></td>
<td>31.10.2014</td>
</tr>
</tbody>
</table>
| **WP number and title:** | WP 2: Requirements identification and socio-economics  
D2.4 Ethical and privacy guidelines for PRECIOUS system implementation |
| **Deliverable leader** | University of Helsinki |
| **Authors** | Johanna Nurmi, Ari Haukkala, Alessio Falco  
/ University of Helsinki |
| **Contributors:** | Carlos Ramos/EuroFIR  
Carmina Castellano Tejedor/VHIR  
Christophe Lohr/Telecom Bretagne  
Christopher Helf/UNIVIE  
Edward Mutafungwa/Aalto  
Hannes Weisgrab/UNIVIE  
Helmut Hlavacs/UNIVIE  
Jose Costa-Requena/Aalto  
Niklas Ravaja/UH  
Patrick Zwickl/UNIVIE  
Peter Reichl/UNIVIE  
Philippe Tanguy/Telecom Bretagne  
Pilar Lusilla/VHIR  
Sarah Kuczora/Campden Bri  
Teemu Kärkkäinen/Aalto  
Tero Myllymäki/Firstbeat  
Timo Korhonen/Aalto |
| **Status:** | |
**Document History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Status</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.03.2014</td>
<td>0.1</td>
<td>Draft</td>
<td>Initial ToC Suggestion (by Ari Haukkala)</td>
</tr>
<tr>
<td>19.5.2014</td>
<td>0.2</td>
<td>Draft</td>
<td>First draft put together (Johanna Nurmi)</td>
</tr>
<tr>
<td>24.9.2014</td>
<td>0.3</td>
<td>Draft</td>
<td>Second draft and presentation for Plenary meeting in Vienna (by Johanna Nurmi)</td>
</tr>
<tr>
<td>29.9.2014</td>
<td>0.4</td>
<td>Draft</td>
<td>Third draft sent to partners for contributions and comments (by Johanna Nurmi)</td>
</tr>
<tr>
<td>17.10.2014</td>
<td>0.5</td>
<td>Draft</td>
<td>Contributions and comments merged into a new version sent to QEG (Johanna Nurmi and Alessio Falco)</td>
</tr>
<tr>
<td>22-29.10.2014</td>
<td>0.5.1</td>
<td>Draft</td>
<td>Input from QEG</td>
</tr>
<tr>
<td>30.10.2014</td>
<td>0.6</td>
<td>Draft</td>
<td>Document modified based on comments of the QEG</td>
</tr>
<tr>
<td>31.10.2014</td>
<td>1.0</td>
<td>Final</td>
<td>Final version sent to Jose Costa-Requena</td>
</tr>
</tbody>
</table>

**Peer Review History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Reviewed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.10.2014</td>
<td>0.4</td>
<td>Carmina Castellano Tejedor</td>
</tr>
<tr>
<td>8.10.2014</td>
<td>0.4</td>
<td>Tero Myllymäki</td>
</tr>
<tr>
<td>8.10.2014</td>
<td>0.4</td>
<td>Philippe Tanguy</td>
</tr>
<tr>
<td>9.10.2014</td>
<td>0.4</td>
<td>Jose Costa-Requena</td>
</tr>
<tr>
<td>10.10.2014</td>
<td>0.4</td>
<td>Philippe Tanguy</td>
</tr>
<tr>
<td>10.10.2014</td>
<td>0.4</td>
<td>Sarah Kuczora</td>
</tr>
<tr>
<td>10.10.2014</td>
<td>0.4</td>
<td>Carlos Ramos</td>
</tr>
<tr>
<td>14.10.2014</td>
<td>0.4</td>
<td>Philippe Tanguy</td>
</tr>
<tr>
<td>15.10.2014</td>
<td>0.4</td>
<td>Christopher Helf</td>
</tr>
<tr>
<td>15.10.2014</td>
<td>0.4</td>
<td>Patrick Zwickl</td>
</tr>
<tr>
<td>15.10.2014</td>
<td>0.4</td>
<td>Hannes Weisgrab</td>
</tr>
<tr>
<td>15.10.2014</td>
<td>0.4</td>
<td>Teemu Kärkkäinen</td>
</tr>
<tr>
<td>16.10.2014</td>
<td>0.4</td>
<td>Carmina Castellano Tejedor</td>
</tr>
<tr>
<td>17.10.2014</td>
<td>0.4</td>
<td>Ari Haukkala</td>
</tr>
<tr>
<td>18.10.2014</td>
<td>0.5</td>
<td>Jose Costa-Requena</td>
</tr>
<tr>
<td>22.10.2014</td>
<td>0.5</td>
<td>Sarah Kuczora</td>
</tr>
<tr>
<td>23.10.2014</td>
<td>0.5</td>
<td>Carmina Castellano Tejedor</td>
</tr>
<tr>
<td>24.10.2014</td>
<td>0.5</td>
<td>Edward Mutfungwa</td>
</tr>
<tr>
<td>27.10.2014</td>
<td>0.5</td>
<td>Philippe Tanguy</td>
</tr>
<tr>
<td>28.10.2014</td>
<td>0.5</td>
<td>Sarah Kuczora</td>
</tr>
<tr>
<td>28.10.2014</td>
<td>0.5</td>
<td>Teemu Kärkkäinen</td>
</tr>
<tr>
<td>28.10.2014</td>
<td>0.5</td>
<td>Ari Haukkala</td>
</tr>
<tr>
<td>29.10.2014</td>
<td>0.5</td>
<td>Hannes Weisgrab</td>
</tr>
<tr>
<td>29.10.2014</td>
<td>0.6</td>
<td>Jose Costa-Requena</td>
</tr>
</tbody>
</table>
Table of Contents

1. Introduction .................................................................................................................. 5
   1.1 Overview of EU ethical directives and guidelines ..................................................... 5
   1.2 Summary of ethical considerations in PRECIOUS project ..................................... 6
   1.3 Description of the PRECIOUS service .................................................................. 6
2. Informed consent .......................................................................................................... 9
3. Privacy .......................................................................................................................... 10
   1.1 Security IT configuration ...................................................................................... 10
4. Data management ........................................................................................................ 11
   4.1 Data protection ...................................................................................................... 11
   4.2 Data collection ...................................................................................................... 12
   4.3 User Data Management ...................................................................................... 13
   4.4 Data management during field testing .................................................................. 15
   4.5 Data storage considerations .................................................................................. 16
5. How the possible risks of the PRECIOUS service have been addressed ............. 18
   5.1 Gamification ......................................................................................................... 18
   5.2 HealthCOIN ......................................................................................................... 19
   5.3 Sensors and actuators ........................................................................................... 19
   5.4 Context monitoring ............................................................................................... 21
   5.5 Concerns associated to monitoring food intake .................................................... 21
   5.6 Concerns associated to physical activity .............................................................. 22
   5.7 Concerns associated to measurement and analysis of heartbeat data ................. 23
   5.8 Psychological risks to be addressed ...................................................................... 23
6. Ethics and privacy from the viewpoint of PRECIOUS usage scenarios ............ 24
   6.1 Family ................................................................................................................... 25
   6.2 Retired couple ....................................................................................................... 25
   6.3 Student .................................................................................................................. 25
   6.4 Young single professional .................................................................................... 25
   6.5 Accessibility .......................................................................................................... 26
7. Conclusion .................................................................................................................... 26
8. Next steps ..................................................................................................................... 27
9. References .................................................................................................................... 27
List of acronyms

EC: European Commission
EU: European Union
mHealth: mobile health
DMZ: Demilitarized Zone
Executive summary

New technology, such as mobile phones and portable electronic devices, offers unprecedented opportunities for preventive health care in a wide range of settings. Mobile health (mHealth) apps and solutions have shown a promising potential to improve individual well-being. These new possibilities, however, have an important number of ethical implications that need to be taken into consideration in research and practice. Ethical and privacy issues including data collection and protection have to be carefully considered from planning to implementation of health related services.

PRECIOUS integrates technological advancements with understanding from social, behavioural, and nutrition sciences in order to offer evidence-based, customisable motivational support with a focus on diet and physical activity. Physiological sensors, environmental actuators, and self-reports provide data for personalisation and goal achievement. The aim is to help individuals to prevent non-communicable diseases by supporting them in healthy life choices. The personal nature of health related behaviours is taken into account in PRECIOUS so that the service will respect individuals’ right to self-determination in all sectors. Users have the right to set their own health goals, manage or delete their data, switch on and off service features, and leave the service at any time.

This document will present how ethics and privacy are taken into consideration in the developing of PRECIOUS service. Consortium partners representing behavioural and social sciences, computer sciences, nutrition and sport sciences have all reflected how European ethical principles and fundamental rights can be implemented all the fields covered by the service. Questions of anonymity, privacy, and overall data protection have been taken into special consideration during the design and implementation of the system as well in all the phases of the project. The document starts with brief description of context and PRECIOUS service. Secondly, we introduce the principles of the informed consent. As privacy is seen as a central feature in ethical design of the service, it is addressed with several viewpoints from user and service data management to big data considerations. The second part of the document covers possible risks related to the use of PRECIOUS service. We go through risks and solutions related to different features of the service from gamification to sensors, context monitoring, and health behaviours such as food intake and physical activity, and finally, we evaluate the psychological risks related to the use of the service. In the end, ethics and privacy are considered briefly from individual usage scenario viewpoints for understanding the specific needs of each user group.

In this document we aim to demonstrate how the user well-being is the guiding principle of the service design. This document guides the reader through the ethical considerations of the project and provides an overview of the collaborative work of the consortium.
1. Introduction

New technologies have created previously unforeseen possibilities for preventive health care, with increasing scope to track, monitor and guide an individual everywhere and anytime. In the last few years, an abundance of health related mobile applications (onwards, mHealth) have emerged, and new applications are created every day. Today mobile phones include applications that can be easily used to track activities such as daily physical activity and sleep, and phones can be connected to other devices that measure health related user information, for example heartbeat. In addition, some applications target behaviour change mechanisms such as motivation, self-regulation, and social support. The advent of social media has also enabled new ways of sharing personal data and providing social support. This rapidly developing technology offers exciting opportunities for more accurate understanding of human function and behaviour, and the possibility to use this knowledge to increase individual well-being. [1], [2]

1.1 Overview of EU ethical directives and guidelines

Following the rapid advancements of technology in the last few years, the importance of ethical issues related to information and communication technologies has increased. The European Union has responded to this need by publishing several directives and guidelines, on which this document and PRECIOUS are based:

3. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [5]

The European Parliament and the Council states that all FP7 activities must respect fundamental ethical principles reflected in the Charter of Fundamental Rights of the European Union [hereinafter Charter of Rights] [3] and take into account opinions of the European Group on Ethics in Science and New Technologies [8]. The Charter of Rights list the whole range of civil, political, economic and social rights of European citizens and all
persons resident in the EU [3]. These rights are divided into six sections: dignity, freedoms, equality, solidarity, citizens' rights and justice. In particular, the above mentioned aspects are based on the fundamental rights and freedoms recognised by the European Convention on Human Rights [4].

1.2 Summary of ethical considerations in PRECIOUS project

This document explores these privacy and ethics related issues from the viewpoint of the PRECIOUS system and service. In the design and ongoing development of PRECIOUS, ethical principles are followed and adhered to determinedly. Challenges related to the implementation and usages of the service are described below, along with measures that aim to ensure the users' privacy and anonymity, as well as to limit the potential risks of data exposure. Ethical principles must be an integral part of the development, design, implementation and adaptation of preventive care technologies as they are not a feature that can be simply added to the final product. Therefore, in PRECIOUS we consider ethics and privacy during every phase of the project.

The purpose of this document is to provide information on how ethics and privacy are implemented in PRECIOUS, and to describe the features related to privacy in all data handling and storage related to the service. Privacy refers to vulnerabilities associated with the data used by the PRECIOUS service. From the perspective of EU legislation, privacy has two sides; it is a practical tool for establishing the internal market, and it has the ethical dimension of being a human right [7]. This document focuses on ethics and privacy from the perspective of the individual users of the service and their rights to fair data processing.

Trust in the privacy and ethical principles of a service provider is crucial for the user [9]. This is even more prominent when the user provides personal behavioural and health information to the service [1]. There must be confidence that this data are kept secret, is guarded and processed with sufficient expertise and privacy, they are accessible to the user, and that they are only used for the benefit of the user.

Considering ethical issues during the planning of the service may also be beneficial for the usability of the end product, as it will also take into account the end-users viewpoint. User-centred design is an approach that aims to make technology easy to use and accessible to users with different abilities. Accessibility may include users of different age groups and socio-economic backgrounds, as well as users with disabilities. Mobile health may contribute to more equitable access to well-being. [1]

1.3 Description of the PRECIOUS service

The objective of PRECIOUS is to create a state-of-the-art, evidence based service that motivates and supports healthy lifestyles and thus helps to prevent lifestyle related disorders, with a particular focus on Type 2 Diabetes and cardiovascular diseases. The service, which will be easily accessible from a mobile phone or other computing platforms, is designed to help users to monitor their health behaviours, such as diet, stress level, physical
activity and sleep. Interacting with the user’s behavioural choices, the service provides customised information and suggestions. To tailor the information, the service collects data from various sensors (physiological, environmental, contextual etc.) and self-reported data from the user. This data is personal and confidential and thus needs adequate data protection [1]. PRECIOUS collects health related user information for personalised feedback and for research purposes.

PRECIOUS is a motivational service with the aim to encourage users to achieve their personal behavioural goals. This is in line with human rights in research ethics, for which self-determination, privacy and bodily integrity are central [10]. Therefore, it is natural the ‘Self-determination theory’ [11], presented in detail in Deliverable 3.3 Interim Motivation Service Design Document, is used as a central theoretical framework for developing the PRECIOUS service, in addition to motivational interviewing techniques. Self-determination theory is based on findings that fulfilling basic human needs, self-determination, competence, and social connectedness, leads to sustainable motivation [11]. The motivational basis of the PRECIOUS service will be based on these principles, which emphasise individual freedom and integration. PRECIOUS users will be encouraged to follow their own health goals, whilst being provided with necessary information and tailored feedback about scientifically based recommendations. The health and well-being of every user is the guiding principle of the service design; however, health related behaviours are personal choices, and therefore, recommendations will not be offered in a controlling way.

The PRECIOUS service is a combination of modern technology and motivational techniques that are used to promote and support well-being and healthy lifestyles. Sensors deliver an overall profile of the users’ health status, and based on this information the service provides tailored feedback on exercise, diet, sleep and stress to the user. The feedback is based on the information provided by the user and from sensors, where these are available. Therefore, it cannot be used for clinical diagnoses, but rather it is designed to indicate potentially risky behaviours and motivate the user to make changes.
Figure 1: Components and innovative fusion of PRECIOUS.

**Sensor-service interaction:**

Body sensors track heartbeat, physical activity, stress levels etc., and interact automatically with the PRECIOUS service. Additionally, at home sensors collect data related to the user environment, such as humidity level, temperature, or light intensity. PRECIOUS can deliver feedback into the user’s home through actuators using light or sound notifications. The system can also directly modify the home environment such as lights, temperature or rolling shutters.

**Mobile device-service interaction:**

Mobile devices and personal computers interact with the central PRECIOUS service by transferring recorded data to personal devices located in user’s home such as home servers or the data can be transferred to data centres (i.e. cloud) for further processing.

**User-service interaction:**

Users interact actively with PRECIOUS by entering personal data via mobile devices or personal computers.
**User-user interaction:**

Users can interact with other users for encouragement, goal setting, comparison or competition. The PRECIOUS service may be developed as a social network on its own or it may be used as part of existing social media (Facebook, Twitter, etc.).

In brief, numerous technologies, which involve collection, storage and processing of data from the users’ surroundings (environment), and directly from the users themselves (user input and sensors), are being developed in the PRECIOUS service. Depending on what is collected by these technologies, different ethical and privacy issues arise.

**Mobile applications:**

There is an abundance of health related mobile applications. However, these applications are usually distinct products that cannot be combined or coordinated together. These applications are mostly proprietary, commercial products and it cannot be guaranteed by PRECIOUS that personal data is adequately protected by individual service providers. We are currently evaluating whether the service will recommend the use of existing applications, or if we will develop new applications for the service. PRECIOUS also aims to integrate information from several different applications and, in this way, provide more informed recommendations for the user. An individual’s health is a combination of physiological, psychological and social factors [12], for which an integrated service is more likely to respond to personal needs.

2. Informed consent

Following the Charter of Rights [3] informed consent will be requested from the users of PRECIOUS. Before obtaining consent, the system will provide detailed information regarding the risks and benefits of using the service. It also emphasises that PRECIOUS does not offer clinical diagnoses or guidance [3]. By electronically providing informed consent, the users declare that they have understood and accepted use of the service and are responsible for their own behaviour and decisions.

Additionally, all the persons who take part in research studies within PRECIOUS will be adult volunteers, who are able to give fully informed consent. In its current state, the service is designed for adults and therefore no children will be involved in the studies. There are four target user groups of PRECIOUS (family, retired couple, student and young single professional) which are described in Deliverable 2.1 List of usage scenarios and user requirements and later in this document. The project and the service do not involve the use of human genetic material nor human biological samples. The service will involve human data collection, the ethical and privacy implications of which are discussed later (Section 4 Data Management). The PRECIOUS service used in the field studies may differ in some parts from the PRECIOUS end product described in this document as the studies are conducted during the development of the service. The field studies will be described in detail in the annual ethical reports, and ethical approval will be requested from the local ethical committees before conducting the studies. A field study will be conducted in the Vall d’Hebron Research Institute (VHIR) at the University Hospital Vall d’Hebron in which
PRECIOUS service will be used with participants diagnosed with type 2 diabetes. This study will be described in detail in deliverable 2.1., which includes the final approval from the internal ethical committee of the hospital and complies with the following ethical guidelines:

- The Declaration of Helsinki in its latest version [13]
- The Charter of Fundamental Rights of the EU (Charter of Fundamental Rights of the European Union (2000/C 364/01)) [3]
- The 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 [5]

All versions of the service will include terms and conditions that specify the risks and responsibilities related to the service. The terms and conditions will follow European Union standards and the research trials will follow country specific legislation.

3. Privacy

Privacy is a fundamental right protected by The European Convention on Human Rights and Fundamental Freedoms [4]. In PRECIOUS, in order to provide an ethical service and respect the users’ privacy, the users’ information will be kept strictly confidential and not shared with third parties. In particular, every precaution will be taken to protect the user’s privacy while using the online data collection service. The use of Privacy Enhancing Technologies for data protection and anonymity is supported by the European Commission [5].

In this regard, we will adhere to anonymisation policies when developing the service. To protect the user’s identity and to ensure anonymity, the user will be offered the option of choosing a pseudonym. The collected data will be encrypted and saved on secured and safe servers.

1.1 Security IT configuration

The security and protection of data is a key element in the design of the service. The users’ experience of data security has also been investigated in a previous EU project, TARGET [9]. The extent to which the data was considered sensitive in a game/virtual environment was found to depend on four factors. First, subjects wanted their data to be preserved in a safe place with security measures. Secondly, the ability to link data to the individual was a concern and the use of pseudonyms (ID code and nicknames) was considered as less threatening than the use of real identities. Thirdly, the nature of data affected the willingness to share information, that is, the subjects wanted to share positive data, but not negative data, about themselves. Fourthly, the subjects wanted to be sure of the validity of data and have an opportunity to correct inaccurate data. These measures are in line with general
recommendations in the field and will also be implemented in the design of the PRECIOUS service. The following recommendations for privacy (based on the TARGET project) are made for the PRECIOUS service:

1. A clear description of which data is collected and why will be given to the users.
2. Collected data will be stored securely and made accessible only to authorised persons.
3. Users will be allowed to use the service with pseudonyms (ID code) instead of their real name.
4. Users will be able to control which data is made public.
5. Users will be given the opportunity to correct/erase erroneous data and stop data sharing at any moment.
6. Users must accept data protection terms and conditions to use the service.

The service will have a set of applications that collect data from sensors and interact with the user through actuators. These applications will either process the data locally to provide user real time information or the applications will send the data to an external server i.e. home server or web server where data would be processed and securely stored. The user can determine the details of the processed data that can be shared with different user groups.

4. Data management

The rapid spread of mHealth services has raised concerns about the appropriate processing of the collected data. In response to these data security and privacy issues, the European Commission has compiled a Green Paper on mHealth, in which it discusses the current use of mHealth best practices [1]. In general, mHealth services collect large amounts of data from sensors within mobile devices, such as location, physical activities, and personal information, which is stored by the user [1]. There are risks in the storage of information, for example databases may be unintentionally leaked, exposed or hacked. Commercial agents outside of the European Economic Area may also misuse data gathered from users [1]. With regard to mHealth services, users have expressed concern about uninvited data sharing with third parties, such as insurance companies or employers [1], [2]. Another risk is the theft or loss of a device used to store data [1]. Management of personal data is guided by several laws and directives. The PRECIOUS system will comply with the Data Protection legislation and reasonable precautions will be taken to protect the user’s data from misuse [7].

4.1 Data protection

PRECIOUS follows European data protection law, which is two-fold by its legal bases [14]. Firstly, privacy is a human right, regulated by the Council of Europe Treaty No 108 / 1981 (ETS 108) [7]. Secondly, data protection is based on the European Union Data Protection Directive 95/46/EC [5], which introduces data protection also as a mechanism for supporting the internal market. This directive emphasises transparency in processing of personal data,
free movement of the data, and ensures the individuals’ right to privacy [14]. This is the basis for the security policies of PRECIOUS and it will be implemented in the collection, storage, and processing of the data. Data protection will include five principles, which are presented in textbox 1. Users will be fully informed about all data collected by the service and will be given the opportunity to cease their use of the service, as well as all data collection, at any moment. All users and study participants will be presented with the terms and conditions of the service in order to enable informed consent for the use.

Textbox 1. Reproduced from Raento, 2007[5], [14]

<table>
<thead>
<tr>
<th>The collector or processor of personal data:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Must process the data in a lawful and fair manner (95/46/EC Article 6 1 a)</td>
</tr>
<tr>
<td>• Must ensure that the data is accurate and, if appropriate, up-to-date (95/46/EC Article 6 1 d)</td>
</tr>
<tr>
<td>• Must ensure that the data collection is adequate, relevant and not excessive for the purpose of the collection (95/46/EC Article 6 1 c and 9)</td>
</tr>
<tr>
<td>• Must inform the subject of the collection and allow access to data collected (95/46/EC Articles 10-12)</td>
</tr>
<tr>
<td>• May only process data by informed consent, contractual or legal obligation, for the vital interests of the subject or for legitimate interests of the controller (95/46/EC Article 8)</td>
</tr>
</tbody>
</table>

4.2 Data collection

Data collection in the PRECIOUS service will be proportional, as described in Directive EC/95/46 [5]. PRECIOUS service will collect data for the purpose of customising the service and of providing the users with relevant information about their progress. Data may also be collected for research purposes in the field studies, which are described in detail in annual ethical reports. PRECIOUS will also adhere to the principles of fair information practices, presented in Textbox 2 [15].
Textbox 2. (reproduced from Langheinrich, 2001) [15].

1. **Openness and transparency:** There will be no secret record keeping. This includes both the publication of the existence of such collections, as well as their contents.
2. **Individual participation:** The subject of a record should be able to see and correct the record.
3. **Collection limitation:** Data collection should be proportional and not excessive compared to the purpose of the collection.
4. **Data quality:** Data should be relevant to the purposes for which they are collected and should be kept up to date.
5. **Use limitation:** Data should only be used for their specific purpose by authorized personnel.
6. **Reasonable security:** Adequate security safeguards should be put in place, according to the sensitivity of the data collected.
7. **Accountability:** Record keepers must be accountable for compliance with the other principles.

4.3 User Data Management

The underlying principle for data management in the PRECIOUS system is that the users’ data should only be available in the physical locations where it is required by the algorithms and services. Further, the collected and synthesised data is owned and controlled exclusively by the user. This is in direct contrast with centralized data architectures that many existing systems employ, where all the data is stored and accessed in one central location and owned by an operator. This principle is derived from the highly sensitive nature of the data collected and processed by the system, which calls for strong user controls of the data dissemination.

The following goals are set for the data management:

1. The user must have access to all data collected by the sensors.
2. The user must have access to all data synthesised by applications and services based on the collected sensor data.
3. The user must have the ability to delete any collected data, as well as data generated by the applications and services (e.g., health goals and personal programs).
4. The data must be stored by default only within devices owned and controlled by the user.
5. When data is required by external operators (e.g., sent to the “cloud” for further analysis), the user must be in full control of which data the operator is given access to, and must be able to provide the access anonymously or pseudonymously.

6. When data is required by local applications, the applications must get explicit permission from the user to access the data. The permission control must be fine-grained and partially revocable (i.e., the user should not have to either grant all permissions or not use the system at all).

There are multiple reasons to prefer the distributed model: 1) physically limiting the access to the data, 2) limiting the amount of data aggregation visible to third parties, 3) more fine grained trust model.

By physically limiting the spread of users’ data, the system makes it very difficult for unauthorized parties to access the data. While centralized data repositories are subject to massive scale leaking of private information through bugs, mismanagement and attacks, restricting the data only to the users’ own devices means that any data leak will be limited in scope and mass scale leaks are much less likely.

Limiting unauthorised third party data aggregation is important, because aggregated data can be more easily used for types of analysis not authorized by the user (e.g., de-anonymizing pseudonymous data). The user should be able to provide only the data required for the particular service without exposing the link between that data and other data (e.g., for heart rate based analysis service, the user shouldn’t have to expose any other data than the heart rate).

Whenever a user shares data with another party, a trust relationship is required. In other words, the user must establish trust in the other party to handle the data according to the user’s wishes and to not expose it to third parties. Most centralized systems require the user to fully trust one provider with all their data. In a distributed design, the user can have more fine-grained control over the trust relationships, and limit the amount of data each other party has access to. On the flip side, this does make maintaining the trust relationships more complex for the user.

There are two main obstacles faced by a distributed data management approach: 1) the operators’ profit motives, and 2) technical complexity.

The former, profit motive, is due to the fact that aggregated personal information is seen as having high value by many businesses. Large, detailed datasets of personal information are difficult to obtain and can be used for various types of analysis. This makes it viable to sell access to the data or to analysis results obtained from the data. Often end user agreements that users are forced to sign, grant the operator unlimited rights to leverage the users’ data beyond simply providing the user the service they have signed up to receive. This may be acceptable in a scenario where the user explicitly provides the data to the service operator (e.g., posts to social networking sites), but not in the PRECIOUS scenario where sensors continuously collect data about the user and their environment, and synthesize new data based on it without direct interaction from the user.

The latter obstacle to the distributed approach, technical complexity, is due to the inherent complexity of designing distributed systems when compared to centralized data repositories.
Many ready solutions exist for collecting data from numerous sources and transmitting it to a centralised database for storage, as well as providing applications and services access to the stored data [16]–[19]. In contrast, distributing and managing data directly between the various sources poses a number of difficult technical challenges. In this area the PRECIOUS system will advance the state-of-the-art in distributed client side data management, by leveraging the existing SCAMPI opportunistic networking middleware that provides the basis for data distribution in such scenarios [20].

The PRECIOUS data management leverages three techniques for this: 1) physically limiting the spread of the data, 2) employing strong cryptography based access restrictions to the data, and 3) building user controls into the applications and services.

The best way to limit the risks related to data management is to physically limit the spread of the data itself. In the PRECIOUS system this is achieved by the use of the SCAMPI opportunistic networking middleware, which distributes data directly between the user’s devices rather than sending everything to the cloud. This means that all of the user’s data is by default only stored in devices owned by the user, putting them in full control. When the user wishes to share the data with other parties, it has to be done with explicit permission from the user. [20]

While physical control of the message spreading is the strongest form of control, it may be desirable to use centralized data stores in the “cloud” in some scenarios. The goals of the data management system dictate that such storage must not expose the data to other parties. To solve this, data access restrictions can be employed. In simple terms this means that the data is encrypted with keys only the user knows. The user can then control access to the data by controlling access to the keys. Different keys can be used to grant access to different data stored centrally.

Finally, all these mechanisms must be exposed to user control. This includes control of the distribution of the data to other parties, and access to the data by locally running applications.

4.4 Data management during field testing

During the reporting of studies carried out during the development of PRECIOUS, the individual identities must not be revealed and data must also be stored in anonymised form. Ethical and privacy issues relating to specific development work and testing will be addressed in annual reports (due for release in November 2014, 2015 and 2016), which will be made publically available.
4.5 Data storage considerations

For certain applications\(^1\), it might be useful to store user-related data such as physical activity and nutrition data over a longer period of time for the purpose of later evaluation which we refer to as Big Data \[^1\].

Analysing this data offers new possibilities for research. For example, large-scale behavioural patterns and environmental factors may be analysed together in order to detect and prevent certain types of diseases. Furthermore, other, as yet unknown, evaluations can be performed. Longer term data storage – assumed the developed platform will remain active over a longer time period – is also extremely valuable in the sense that historical data can be applied to newly developed algorithms and the result of the algorithm can be verified with the current status quo. Subsequently, with this verified algorithm, educated predictions for the future can be made.

The storage of big amount of data (i.e. Big Data) from the users would usually be handled by cloud technologies or by utilising cloud services from 3\(^{rd}\) party providers. However, these technologies, and especially the use of 3\(^{rd}\) party cloud services, where even the physical location of the data is unclear, are a controversial issue.

In order to address this issue, PRECIOUS will create a security strategy, which will address all security-, and privacy related issues and prevent the problem of the “untrusted 3\(^{rd}\) party” to the highest extent possible for the server side data of the PRECIOUS core. The user should be made aware of if any data will be shared with 3\(^{rd}\) party applications. Thus, user has the possibility to limit the data sharing since PRECIOUS cannot guarantee that 3\(^{rd}\) party applications fulfil the required privacy standards.

The PRECIOUS security strategy\(^2\) is based on a number of security layers, which shall also be mapped to the hardware in order to eliminate data breach threats triggered by virtual environments. Security levels shall be separated from each other on an organisational, connectivity, and physical level.

This separation of security layers is achieved by applying state-of-the-art data centre/cloud security mechanisms, such as:

- On an organizational level, different people, with their own access codes, shall be responsible for the various security layers and strict password rules shall be applied.
- On the connectivity level, established mechanisms like DMZ\(^3\), Firewalls, Proxies and usage of encryption shall be applied.
- On the physical level, components of different security layers shall be physically separated and physical access shall be restricted.

\(^1\) “application” in this respect refers to the evaluation of data, not the “App” which is executed e.g. on a smartphone
\(^2\) Please note that this high-level description of the security concept is only an initial outline of proposed security and privacy mechanisms as the concept is still under development and is not the subject of this deliverable
\(^3\) Demilitarised Zone – physically and logically separated part of the network where the access of lower security network zones (like the Internet) is handled
In this security strategy, the highest security level is called the *secure core*, which is also eligible for highly critical processes such as payments and storage of critical user data. Data within the secure core is always processed in this core. Furthermore, data shall never leak to a lower security layer unless it has been processed and transformed to protect secure information. Access is only possible from one security layer to the next higher one and is protected by using *secure APIs*.

Concerning *Big Data* in the overall security strategy:

- User-related Big Data is split into categories, e.g. location data is never stored together with related health data, in order to make it impossible to find the identity of a user by analysing one category (e.g. position data) and correlating it with another category (e.g. health related data).
- The real identity of the user is hidden by removing any reference to the user from the data set and tagging the data set. The relationship between the tag and the user is stored in a high security layer.
- 3rd party cloud providers should only be used after data is anonymised.
5. How the possible risks of the PRECIOUS service have been addressed

Computer based applications and portable devices have been found to be effective for improving learning in many environments [21]. An advantage is that they are more accessible than personal health care services and thus they increase the availability of the service for a higher number of users. Internet-based applications are also low-threshold services that can be joined easily without extensive resources.

It is not anticipated that the PRECIOUS service will have any negative impacts on the user's health. Nevertheless, as with any programme that targets health related behaviours, the PRECIOUS service may have its risks. This document presents the risks that will be taken into consideration when planning the service and offers solutions to prevent them. The service will be designed so that these risks are limited. The PRECIOUS service will also offer tutorials that guide the use and warn of unhealthy use patterns.

PRECIOUS will offer tools for monitoring of behaviour. In some individuals, self-monitoring may escalate into compulsive behaviour, whereby users act in an excessive manner. The PRECIOUS service will be planned so that it supports users in self-awareness, and thus aims to prevent disproportionate behaviours.

In the following sections, we present specific features of the service, possible ethical and privacy consequences for the users and discuss how these have been addressed.

5.1 Gamification

Games and gamification that will potentially be used within the PRECIOUS ecosystem are centred on a global reward system that is still to be specified. Even though the major emphasis of the system will not be placed on extrinsic or tangible rewards, obsessive passion with regards to game-like elements have sometimes been found to foster negative effects in terms of emotional and social status, as well as the satisfaction of basic psychological needs. Thus, we will explore the possibility of using the PRECIOUS system to identify users who are predisposed towards obsessive behaviours and secondly, automatically investigate cases where obsessive and subsequently unhealthy usage of the system has occurred in order to prevent psychological harm to the user.

In addition, the gamification approach within PRECIOUS will fully be user-centric rather than trying to fulfil the goals of developers. Thus, the goals of the PRECIOUS team are fully aligned with the goals of the individual using the system. Gamification is presented in greater detail in the Deliverable 3.3 Interim Motivation Service Design Document.
5.2 HealthCOIN

As part of the project, we will investigate the possibility to introduce the so-called HealthCOIN concept in the PRECIOUS service. HealthCOIN, which will be described in the Deliverable 2.2 Interim report on socio-economic factors and business models, would target the creation of an ecosystem around applications and services that facilitate healthy lifestyles, based on a new virtual currency. Thus, HealthCOIN should only be used as a virtual currency for activities within the PRECIOUS platform and not for arbitrary and potentially unhealthy business cases. It should be possible to transfer HealthCOIN into a payout, which is given in the currency preferred by the user. The concept must also limit opportunities to cheat and therefore misuse the platform due to monetary motivations. As a result, the usage of extrinsic motivation techniques via HealthCOIN should be limited. Further activity and progress indicators or metrics will be necessary to support the internalisation of behavioural change. It is not the intention of PRECIOUS to make newly adopted healthy practices subject to continuous extrinsic stimuli, but to provide continuous support to strengthen the intrinsic motivation in the longer term.

5.3 Sensors and actuators

There are two types of sensors in the PRECIOUS system; sensors collecting physiological data and sensors collecting environment data.

Heartbeat sensors (called bodyguard2; Firstbeat) detect minor changes in heart rate variability and thus provide information on levels of stress and recovery. More specifically, these heartbeat sensors measure R-R intervals of the heart, i.e. the time intervals between each heartbeat, as well as 3D accelerometer data. The data can thereafter be used for physiological modelling of the user by utilising analysis of heart rate variability and body movements, and to provide information on the levels of stress, recovery, and physical activity. The bodyguard2 sensor is generally safe for the user, who is provided with, and encouraged to follow, the instructions of use at any time when dealing with sensors.

When performing a measurement, standard, disposable electrodes are used. The glue or electrode paste of the electrodes can irritate the users’ skin, and therefore the users are instructed to clean and dry their skin after removing the electrodes. It is also possible to slightly alter the electrode location between different measurement days. Other aspects of safety and comfort of use include that the device should not be charged while it is attached to a person’s body, the sensor should be removed while going through airport security and/or metal detectors, and that the use should be discontinued immediately, and the skin should be cleaned carefully, if the electrodes start giving the user a rash or an obvious allergic reaction. Furthermore, a doctor should be consulted if needed.

There are several factors in a home environment that are associated with an individual’s health, such as temperature, humidity, etc. Ambient sensors will be used by the PRECIOUS system to collect data such as indoor temperature, humidity, air quality, light intensity, sound
level, etc. Furthermore, the users habits can be monitored by algorithms that work on a dataset of home sensor data (e.g. open/close door, on/off TV, up/down roller shutters, etc.).

Feedback and actuation loops are envisioned for managing environmental risk factors. It will be partially realized by home automation actuators or multimedia devices, for instance; automated programmes could be used to regulate the bedroom temperature during night to improve the users sleep quality according PRECIOUS recommendations, or, the system could trigger an alarm concerning the home air quality or simply notify the user with a message on multimedia devices, such as a connected TV, smartphone or personal computer.

PRECIOUS will provide a transparent sensors/actuators layer to manage interoperability issues between heterogeneous devices and communication protocols. Indeed, all sensors/actuators use communication protocols to exchange data. A number of different protocols exist, e.g. Bluetooth or WiFi for smartphone devices, as well Zwave, Knx or EnOcean for home automation sensors/actuators. Unfortunately, the main issue is in seamlessly managing several sensors/actuators that use several communication protocols. One of the objectives within PRECIOUS is to propose a solution in order to share information in such a way that it is transparent for the user.

As shown previously, several datasets will be collected in the home environment, which provide information on user context and habits. Concerning ethics & privacy, some issues have been identified in relation to home automation sensors:

- Home automation security & privacy protocols
- Home automation data access
- Home automation data storage
- Home automation external access from internet
- Home automation user and/or service identification
- Home automation scenarios
- Malware in home network

Basically, PRECIOUS will provide, at home, a transparent sensors/actuators layer thanks to a new communication protocol named xAAL (presented on the web page http://recherche.telecom-bretagne.eu/xaal/) [22]. The xAAL protocol will be designed to deal with all the security & privacy issues listed previously. The xAAL protocol is still in a specification and development stage. However, several proposals have been considered and we choose to use encryption mechanisms to guarantee the user privacy & security in the home environment. Obviously, external access by user or service from internet to the sensors/actuators layer will be protected with password and a protocol called Transport Layer Security (TLS). Finally, home automation scenarios (e.g. start coffee at 7 a.m.) could be a problem from an ethics point of view that can be avoided by informing and giving control to the user (i.e., the system needs to offer a total transparency to the users).

Otherwise, as described previously, the system can send feedback (e.g. notifications) and modify the home environment with automated scenarios (e.g. light on when it is morning) or
provide the user with notifications (e.g. message, sound, flashing light). The following ethics & privacy issues should be considered:

- PRECIOUS will have access to home automation actuators (e.g. lights, roller shutters, thermostat, etc.)
- External services used by PRECIOUS (e.g. IFTTT) or external mobile Apps may have access to home automation actuators

Finally, the sensors/actuators layer could present a problem because it is transparent. Indeed, the user is not aware of all the data collected and this may lead to concerns about losing control of their own data. To avoid this, PRECIOUS must give the user access/control of data that is collected, as well as to the automated scenarios and actuators used. Moreover, access to raw data is also necessary to give the user the opportunity to verify the quality of data used by the system.

5.4 Context monitoring

One of the most significant developments with mobile apps is the use of contextual information to make them more relevant to the user. The PRECIOUS service rely on similar approach by combining multiple context values of an individual to generate a more powerful understanding of their health risk levels and make timely and informed preventive care interventions. The context may include traditional categories [23], namely: the actual user context (user profile, location, mood, etc.), computing context (user devices, network connection type, etc.), physical or environmental context (temperature, noise etc.) and time context (time of day, day, season etc.). Recently, the emergence of social media platforms has also increased the importance of monitoring the user’s social context [24].

However, gathering and mining of user contextual information also poses some critical concerns in relation to privacy and potential inappropriate exploitation of the information (e.g. for push marketing, impersonation etc.) or information disclosure with malicious intent. These privacy concerns are even more amplified in the health and wellness application scenarios. Therefore, the PRECIOUS system implementation targets a privacy-aware context sharing environment that provides privacy preservation according to existing data protection regulations and user privacy preferences, such as, hiding or revealing certain context information, preserve anonymity to certain services and so on [25].

5.5 Concerns associated to monitoring food intake

As PRECIOUS is an automatic service that functions without human reflection, there is a risk that the recommendations might not be suitable for every person and every situation. For example, an individual with food allergies will need to keep these in mind in case the service provides unsuitable suggestions which are based on generic national recommendations. It is also possible that if a psychological vulnerability for eating disorders pre-exists, the use of a tool for monitoring eating behaviours may trigger unhealthy behaviour patterns.
The abovementioned risks will be addressed by consulting nutritionists and psychologists during the design of the service and by conveying only scientifically acknowledged nutritional facts. PRECIOUS will also use the best available nutrition composition data, provided by EUROFIR, to analyse the energy and nutrient content of the users’ diet.

Users will be provided with dietary guidance information developed by organisations such as the World Health Organization, the European Union and European member state government bodies. Also, users will be made aware that the PRECIOUS platform is an automatic tool and, as with all technical programmes, it may have deficiencies. Users will be altered to the fact that they have the responsibility to compare choices proposed by PRECIOUS with other publicly available health guidelines and information. The PRECIOUS service will provide links to some external sources of dietary information. The user will be advised to consult a medical professional before making any major dietary changes.

5.6 Concerns associated to physical activity

Inappropriate use of the PRECIOUS service, as with any tracking service, might lead the user to adopt harmful behaviours. For example, following numeric information with a competitive attitude might lead to over-exertion and ignoring of bodily signals. This will be avoided by designing the service to emphasize the user experience instead of external achievements. The users will be advised to consult a medical professional before making any major changes to their physical activity routine.

The use of a mobile device outdoors might increase the risk of accidents if the device requires attention from the user (accidents may occur in the event that the user does not pay attention to the traffic or to their general surroundings). We will investigate the possibility that the features that are necessary in outdoor sports might be conducted with voice commands and consider the possibility to perform all setup before embarking on the activity. Users are not encouraged to operate their mobile device during physical activity.

All physical activity may predispose the individual to accidents or injuries. A motivational service may increase the risk, especially if the user is absorbed by a virtual world. Furthermore, a training programme might misleadingly encourage individuals to continue training when sick or injured.

The aim for developing an interactive nature in the PRECIOUS service is that the user would not be passively following a training programme proposed by the service, but that PRECIOUS would track the user’s well-being and adapt its suggestions to changes in it. This is a goal for the system design but it should be remembered that PRECIOUS relies on the data received from the users and thus the data will vary according to the willingness of the users to provide information, and the sensors that are being used.

The service does not encourage risk behaviours but aims to enhance the basic fitness of the user in the safest possible way. For instance, tracking all activities (with an activity wristband or other constantly wearable sensors) can encourage users to stay moderately active e.g. reduce sedentary behaviours.
5.7 Concerns associated to measurement and analysis of heartbeat data

PRECIOUS can utilise heartbeat data collected with sensors, and analyse heart rate and heart rate variability information from this data in order to produce descriptive results of the user’s lifestyles, stress, recovery, sleep, and physical activity. As such, the system can be used to identify increased risk for type 2 diabetes and cardiovascular diseases, where individual’s lifestyle plays a significant role. However, with technology, there is always a risk of a service failure or malfunction that may provide incorrect or inappropriate results. The misinterpretation of results from heartbeat measurements due to service failures or other reasons such as data quality, medications used by the user, inappropriate use of the sensors etc. might cause anxiety about the user’s health.

Therefore, the users of PRECIOUS need to acknowledge and agree that the results of sensor-based assessments (e.g. heartbeat related assessment) created or delivered by the system may induce inaccurate or faulty results or results, which are open to various interpretations. PRECIOUS, or a service supplier for the PRECIOUS system, therefore does not warrant that the system fits for the intended purpose of its end-users and is not liable for any costs and damages incurred as a consequence of use of the system. Moreover, the terms and conditions of any external services used alone or in connection with PRECIOUS need to be accepted by the users of these services or the overall system. The services, software and accompanying materials are provided “as is” and thus specifically disclaim all other warranties, whether expressly stated or implied. The users are encouraged to follow any instructions provided with the system or its sub-services.

5.8 Psychological risks to be addressed

The PRECIOUS service will encourage the user to set behavioural goals in order to attain a healthier life style. Goal setting, together with self-monitoring, is a widely used and effective behavioural change technique [26], [27]. However, there is a risk that poorly evaluated or over-ambitious targets that are not achieved might lead the user to experience failure and this can weaken self-efficacy. Many people do not reach the national or international recommendations for physical activity or healthy eating [28], [29]. Constant awareness of unmet standards may induce negative feelings towards the service or the self. For this reason, the PRECIOUS service should be based on personal, realistic targets that can be achieved and thus the user can gain experience of success and competence.

We take into account that repeated negative feedback, either from the service or from peers, might decrease self-esteem [30]. Therefore, the service will be designed to provide feedback in a positive manner. Behavioural choices will be framed positively and the principles of motivational interview (presented in Deliverable 3.3 Interim Motivation Service Design Document) as well as the self-determination theory will guide the design so that individual values, choices and goals are supported. [9], [27], [28]

Social support is an effective strategy in health behaviour change and it may be a strong positive power of change [11], [32]. Peers and significant others can provide significant support for the life goals of the user [33]. Social support may also be offered in online groups that are formed around a common health concern [34]. However, social networking and
information sharing might also be experienced negatively. User-user interactions may be experienced negatively if impolite language is used, achievements are understated, the user receives negative feedback, does not receive positive feedback, or experiences shame for not reaching targets. Another risk of social support groups is that the user may compare oneself to others in a negative manner. The user should have the possibility to comment on or justify their performance while publishing data to others, for instance giving reasons for exercising little, slowly or below their skill level. Additionally, they must always have the choice to choose what will be published, which may minimise the risks of negative interactions. Social media may include challenges in privacy and group dynamics that must be taken into account in the implementation of PRECIOUS.

In applications where achievements are awarded with scores or other rewards, there is a risk that service failures or network problems may cause participants to loose these scores. For instance, if the service fails to track location information for physical activity, the user may not earn associated points. This may cause frustration for the user. For this reason, the service should not be too strongly focused on collecting points or rewards; instead they should only be used as additional encouragement. Additionally, the user should have the option to add manually achievements or points that the service had ignored. In the design of the service, a balance will be sought between external rewards, such as points or rewards, and more autonomous motivations, which are associated with sustained health behaviour changes.

The PRECIOUS service may give health behaviour related reminders and advice to the user. In order to make the service user-friendly, it is necessary to plan their implementation carefully so that the service does not become intrusive for the user. In the service design it will be taken into account that the reminders should function in an encouraging manner e.g. by offering options for adjusting the feedback frequency so that the users can customise the service for their personal use.

The possible use of a graphical representation of the user (avatar) in PRECIOUS related apps might be experienced adversely by the user, if for instance the avatar gains weight or loses fitness. The graphical representation of the user is intended as a visual aid for understanding changes in behaviour or physiology and for increasing self-awareness. Research into the use of an avatar will be carried out to understand how this might support the user and to conclude whether an avatar will be included in the service.

Continuity and availability of the service may also be important from psychological point of view: Will the user face negative emotions if the service is not maintained in the long run? Will there be negative consequences if the users have been used to relying on the service? May the users overuse the service?

6. Ethics and privacy from the viewpoint of PRECIOUS usage scenarios

A set of usage scenarios have been described in Deliverable 2.1 List of usage scenarios and user requirements. These usage scenarios are used to describe four potential user groups of
PRECIOUS (family, retired couple, student and young single professional) and to indicate how individuals within these groups may use PRECIOUS to accomplish particular goals or tasks. Whilst many issues overlap, there will also be some key ethical and privacy issues that are particularly relevant to these distinct user groups. These key issues are discussed below by user group.

6.1 Family

Use of the PRECIOUS service in a family brings about questions of privacy, for example, will an individuals’ personal data be open to everybody in the family? Any multiple user access must be created in a way that makes the service sufficiently private for all the members but also enables shared goal-setting and monitoring of progress. The service should be customisable for different family needs so that the level of privacy and sharing can be easily adjusted.

6.2 Retired couple

Questions of privacy and multiple user access may also be relevant for a retired couple. Additionally, as older generations are typically less familiar with modern technology, the user interface should be simple and privacy settings should be easy to control and understand. For example, it should not be possible for the user to unintentionally publish personal information on social networks.

The service could also be developed with accessibility in mind, that is, specific features could make it more approachable for elder people. To offer an easy and accessible system such easy-to-use features could include audio recordings instead of text messages and the possibility to have a simple screen view with a larger font size. Improving skills of digital literacy for elderly is a measure of inclusion and a step for avoiding digital divide between generations [8].

6.3 Student

Student users often have a low income level and this must be taken into account if commercial services are included in the PRECIOUS. Low income may affect also nutritional choices, access to particular physical activities and ability to purchase state-of-the-art technology. This should be reflected in the options recommended by the service. It is noted that this issue will also be applicable for lower income households within the other user groups. PRECIOUS aims being an easily achievable and affordable well-being service, and thus contributing to social equality [1].

6.4 Young single professional

For the group of young single professionals, key ethical questions identified were data sharing and access while travelling, the use of a cloud service, and privacy related to profile sharing with friends. Advice will be given to only share one’s personal information with individuals who are friends in real world, not only in the virtual one. It is noted that these users are likely to travel regularly for work and social activities and may require support to continue healthy behaviour during such trips. In particular, the service should consider the users safety when recommending activities in new areas, for example advice to jog by the
river or in woodland in an unfamiliar city may carry unnecessary risks. Advice to use well lit paths and exercise during daylight hours where possible should be provided.

6.5 Accessibility

While creating PRECIOUS service, we also keep in mind that in a later stage the service must ensure accessibility for potentially disadvantaged groups, such as those on a low-income, people with a disability, the less-literate, and the elderly. The prototype may later on in the product phase be tailored to these user groups for instance by including voice messages or easy-to-use features.

The service should also be available for individuals with different socio-economic backgrounds. The service will therefore be designed with social inclusion in mind – it should be accessible with a standard smartphone, without purchasing expensive sensors [8].

7. Conclusion

The PRECIOUS service has been presented with respect to ethical and privacy considerations. The use of technology to promote well-being and health behaviours presents a number of ethical and privacy challenges. These have been discussed and solutions are offered to minimise risks. All project partners are committed to careful planning in order to avoid any harm for the user. Possible physical and psychological risks are minimised. The nature of the PRECIOUS service is to help the user to recognise unhealthy behaviours and choose healthy options. Thus, the service can help to avoid harms that might be related to for instance insufficient physical activity or unhealthy eating.

The interactive nature of the PRECIOUS service means that it actively monitors the user’s health and adapts its functioning with regard to changes. However, the users themselves have control over the service; the service does not enforce activities. Thus, the user has autonomy but also the final responsibility lies with the user. It is crucial to convey to the users that PRECIOUS is an unregulated, unsupervised service, and that by using PRECIOUS they accept the nature of the service. Furthermore, PRECIOUS will not provide any clinical diagnoses and the service will not be able to reliably take account of food allergies and other medical conditions. The PRECIOUS service only gives motivational recommendations, tips, and information on healthy living following evidence-based recommendations. PRECIOUS only receives the data that the user provides and is therefore not a comprehensive view of the user’s health. Users will be informed of the limitations of the system.

The risk of psychological harms related to the use of PRECIOUS are minimised through careful planning of the service. For instance, support messages are framed positively, negative feedback is avoided, and the users are guided to set appropriate goals. These measures are taken to increase the experience of autonomy for the users. The core of the service is the customisation; users can modify the privacy settings to decide which information is shared with others. All collected data is handled with great care and with appropriate data protection measures. It can be concluded that the risk for harm to be caused by the PRECIOUS service is small and may be further prevented through careful
design of the service. Despite the risks mentioned in this document, PRECIOUS is considered to be a low risk service. To decrease risks, the service will be designed to offer a tutorial, teaching the user how to use the service in an optimal way and how to take care of the users’ safety and privacy.

8. Next steps

Ethics will be considered continuously during the project in annual reports. All the trials will be reported and permission requested from national research ethics committees.

9. References


