Grant Agreement No: 611366

PREventive Care Infrastructure based on Ubiquitous Sensing

Instrument: Collaborative Project

Seventh Framework Programme (FP7) Call FP7-2013-10

D2.5 Report on Legislative Investigations

Due date of deliverable: 29/02/2016

Actual submission date: 29/02/2016

Start date of project: November 1st 2013
Duration: 36 months
Project Manager: Dr. Edward Mutafungwa
Revision: V0.4

Abstract

This document represents an overview of the legal considerations of particular relevance to the PRECIOUS project and the impact they may have on its development and deployment. Particular attention is given to European laws as these provide a focus, being applicable in many member states, and act to harmonise national law. Legislation relating to data protection, medical devices and consumer protection is considered. These areas of legislation however are currently undergoing revision to reflect the rapid advancements in technology that have occurred since original legislation was introduced, and will therefore need to be reviewed when the system is finalised.

Nature:	R (R: Report, P: Prototype, O: Other)
Dissemination Level:	PU (CO: Confidential, PU: Public)
Version:	1
Date:	29th February 2016
WP number and title:	WP2: Requirements identification and socio-economics
Deliverable leader	Campden BRI
Authors	Sue Keenan
Status:	Final

Document History

Date	Version	Status	Change
26/03/2015	0.1	Draft	1st draft
12/10/2015	0.2	Draft	2nd draft
12/02/2016	0.3	Draft	3rd draft
29/02/2016	0.4	Final	Final report

Peer Review History

Date	Version	Reviewed By
13/05/2015	0.1	Phillippe Tanguy
15/05/2015	0.1	Edward Aalto
01/12/2015	0.2	Consortium
12/02/2016	0.3	QEG review
25/02/2016	0.4	Campden BRI internal review

Contents

List of acronyms

CRD	Consumers' Rights Directive
EC	European Commission
EDPS	European Data Protection Supervisor
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EHRs	Electronic Health Records
EIF	Europe-wide 'eHealth' Interoperability Framework
EU	European Union
FDA	Food and Drug Administration
GDPR	General Data Protection Regulation
ICO	Information Commissioner's office
ICT	Information and Communication Technologies
IoT	Internet of Things
ISS	Information Society Service
MEDDEV	Medical device
mHealth	Mobile health
MHRA	Medical Health Regulatory Authority
NHS	National Health Service
OS	Operational software

1. Executive summary

The objective of the PRECIOUS project is to create a state-of-the-art, evidence based service that is accessible from a mobile phone or other computing platform, and motivates and supports healthy lifestyles so helping to prevent lifestyle and related disorders.

The PRECIOUS project aims to utilise the new technologies available via mobile phones and similar devices, along with motivational techniques to help support healthy lifestyles. Such technology is developing quickly and offering previously unforeseen opportunities and possibilities. It also however offers considerable challenges, particularly in the areas of data protection, standards, efficacy and consumer protection. Legislation in these areas was first introduced a number of years ago (the existing Data Protection Directive 95/46/EC [1] has been in place since 1995) and, as such, was not necessarily designed to meet the challenges presented by the new technologies and applications available currently, or potentially in the future.

Due to the proliferation of mobile apps the distinction between what is a medical device and what is a 'health and well-being' app that does not come under the same regulatory controls, is a grey area. There are reported to be over 150,000 health apps available in Europe and they all vary greatly as to the service they offer, how they function and claims made. There is however reported to be little guidance for doctors or patients on quality, safety or efficacy. The majority of apps are downloaded from 'app stores' available from various internet sites such as iTunes and Google Play for example, [2, 3].

The European Commission (EC) has reviewed the existing legal framework and also outlined the main areas of which app developers are aware. These included the areas of data protection, medical device regulation and how this applies to apps and of consumer protection regulation. Consumers themselves have also highlighted concerns over privacy of their data, where it is stored and who has access as well as how to assess the quality of the many apps available.

This document provides an overview of the legal considerations of relevance to the PRECIOUS project so as to inform its development and deployment. Particular areas include the requirements relating to data protection, medical devices, interoperability and consumer protection and recent developments in this area. Developments in relation to the standards for mobile apps are also highlighted.

The extent and applicability of the different items of legislation however will ultimately depend upon the individual components, final configuration, operability and stated claims of the PRECIOUS system.

2. Introduction

2.1. Purpose, context and scope of this deliverable

The aim of this deliverable is to provide an overview of the legal considerations of particular relevance to the PRECIOUS project and the impact they may have on its development and deployment. Particular attention is given to European laws as these provide a focus, being applicable in many member states, and act to harmonise national law.

Within the above context this document therefore describes:

- The PRECIOUS service and the elements within it
- Mobile health (mHealth)
- The current legislative landscape and proposed amendments that may impact on the PRECIOUS system
- National considerations

2.2. Description of the PRECIOUS service

The PRECIOUS system is still under development and the description of how it will operate given below is that envisaged by the project team.

The objective of the PRECIOUS project 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 disease. The service, is intended to be accessible from a mobile phone or other computing platforms, and 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. In order 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.

The PRECIOUS service is a combination of modern technology and motivational techniques that are used to promote and support well-being and healthy lifestyles. Thus sensors deliver an overall profile of the user's 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. The service cannot be used for clinical diagnoses, but rather it is designed to indicate potential risky behaviours and motivates the user to make changes.

The intention is that the service is provided using mobile phone or other smart device platforms (such as tablet PC, smart TV etc). Figure 1 below depicts the PRECIOUS concept:

Figure 1 PRECIOUS concept

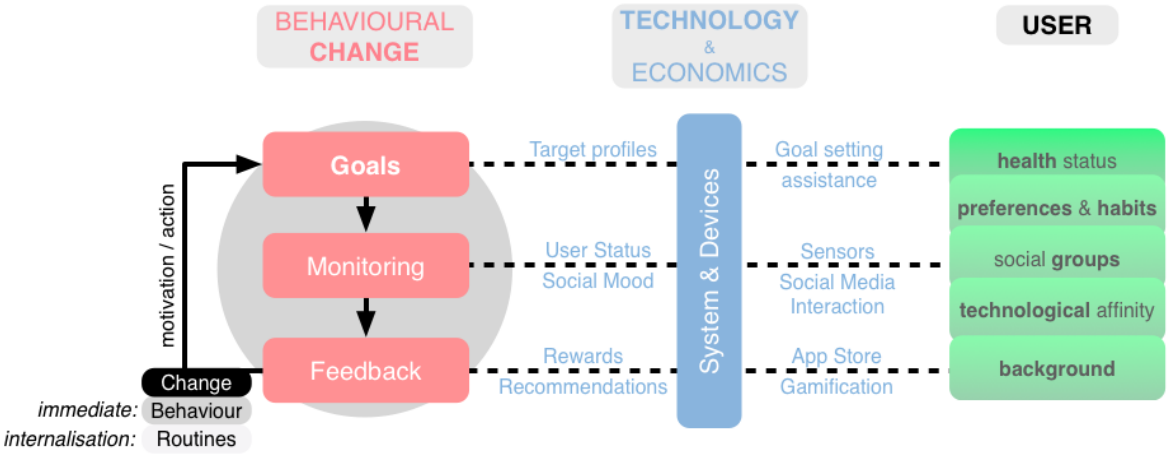
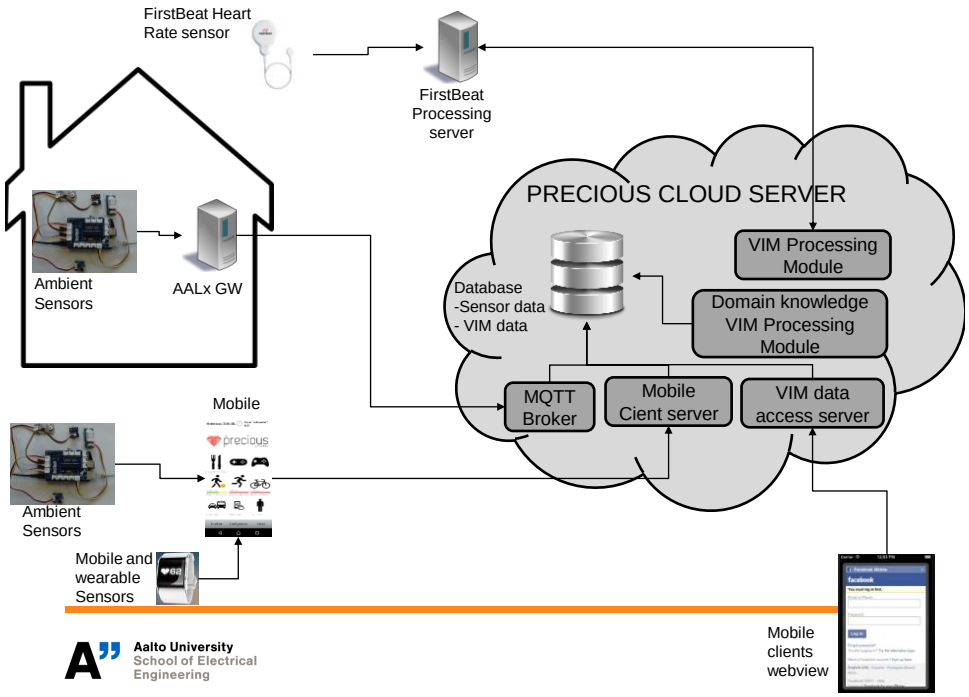


Figure 2 below depicts the PRECIOUS system:



2.2.1. PRECIOUS System Interactions

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 sight or light 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 the user's home such as home gateway servers or the data can be transferred to data centres (ie cloud) for further processing.

User-service interaction:

Users interact actively with PRECIOUS by entering personal data via mobile devices, personal computers or other smart devices.

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 an existing social media (Facebook, Twitter etc.).

Gamification:

The PRECIOUS project also incorporates a gamification aspect to encourage participation.

Table 1 Summary of the role of the individual elements within the PRECIOUS system

Location	Component	Role of individual elements within PRECIOUS
	PRECIOUS system	Preventative care for those at risk of developing diabetes or cardiovascular disease. Home and individual sensors provide an overall profile of user's health status.
Home	Ambient sensors • Air quality • Temperature • Humidity • Light levels	Connected sensors automatically monitor ambient conditions and sends alerts via TV / mobile / lighting if these need to be changed.
	Connected scales	Connected scales automatically record weight
	Learning module (library)	Modules of information / Library containing on relevant topics e.g. Reference Intakes and guidance on healthy eating, exercise.
	Challenge module – Tailored feedback	Based on the information provided by the user and analysed by the system sets individual challenges e.g. Increase consumption of fruit and vegetables, with rewards to encourage progress.
Individual	Wearable sensors incorporating: • Gyroscope • GPS • Activity tracker	Monitor activity inside and outside the home
	Food intake monitor / diary	Manual logging or via barcode scanner. Photo diary: Photo log of food; To visualise what has been eaten during the day / Record for later logging
	FirstBeat Heart rate sensor	Measures stress levels
Smart devices (phone, laptop, TV) Cloud server	Personal data	When signing up to the system (via mobile phone app or website) users are requested to give certain basic personal information: Email address; Height, Weight plus details of their drinking and smoking habits In addition they will be required to accept the Terms and Conditions of Use of the system as assigned by the project team.
	Data analysis (Cloud server)	Central server analyses all input data (manual or collected automatically via the sensors) to identify any behaviours or data that indicate an increased risk, if continued, of developing diabetes or cardiovascular disease. The system thus provides tailored feedback to the user and challenges them to change their behaviour and provides guidance / advice as to how. This is provided via mobile app, website or smart TV.
Communication	Access	The user accesses the system via smart devices (mobile phone, laptops, computer, TV)
	Support	Use of social media services for additional support.

2.3. Ethical considerations

As indicated above 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. The system also involves a gamification aspect.

Aspects associated with all of these factors involved in the PRECIOUS system need to be considered. Ethical and data protection considerations associated with the implementation of the PRECIOUS system have been discussed in the report D2.4 Ethical and privacy guidelines for PRECIOUS system implementation [4].

This report indicated that there is an abundance of health related mobile applications. Since PRECIOUS cannot guarantee the personal data is adequately protected by individual service providers they are currently evaluating whether the service will recommend the use of existing applications, or if a new application will be developed for the service.

Whilst there may be some overlap with the above report under work package 2.4, the current report reviews the legislative situation associated with the design, implementation and use of mhealth applications and considers how these may affect the development of PRECIOUS. Only the courts however are able to give a definitive interpretation of the associated legislation.

2.4. Mobile Health

Research programmes on e-Health have been undertaken in the European Community since the early 1990s. e-Health is described as *"the application of information and communications technologies across the whole range of functions that affect the health sector* [5].

e-Health tools or solutions include products, systems and services that go beyond simply internet-based applications. They include tools for health authorities and professionals as well as personalised health systems for patients and citizens. Examples include health information networks, electronic health records, telemedicine services, personal wearable and portable communicable systems, health portals, and many other information and communication technology-based tools assisting prevention, diagnosis, treatment, health monitoring, and lifestyle management[6].

More recently, and with the rapid technological developments in information technology and network availability, the area of mHealth (an area of e-Health) has been considered. mHealth includes "*medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and other wireless devices*" [6,7] It also includes applications ("apps") such as lifestyle and well beings apps, as well as personal guidance systems, health information, medication reminders, fitness and dietary recommendations.

Depending on the particular app the extent and type of information collected is variable but potentially considerable including medical, physiological, lifestyle, daily activity and environmental data.

Similarly the way in which apps operate can also vary. Apps are software applications which can be downloaded onto a variety of mobile devices including smartphones, laptops, tablets and e-readers. Apps can also be accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software.

Thus some will have been developed specifically to reside on a mobile device platform and may also be designed to utilise other mobile phone features, such as camera or GPS radios. Others utilise the browser function through the mobile device to provide the end user with information and require that the relevant browser or appropriate interface is enabled. Some are a combination of both approaches.

Apps can also be made available in a number of ways such as via medical professionals or via an appropriate app store and may be available free of charge of as a chargeable or subscription service.

Mobile app developers need to consider how the app will be supplied and the compatibility with the operating systems of the mobile systems (platform) on which they are intended to operate. These will in turn affect the route to market and who owns the app.

The quality of some of the apps available however has been questioned with respect to how they have been calibrated and their efficacy demonstrated [2, 3].

It can be seen that the concept of eHealth / mHealth encompasses a wide variety of services, supplied and made available in an equally wide variety of ways and potentially involving a range of data types of varying levels of confidentiality.

The consideration of how the PRECIOUS system is made available and the choice of operating system is not addressed here. The applicable legislation however may affect this choice for the project team.

3. Legislative Considerations

As the area of mHealth has developed, so the variety and number of health apps has grown along with the associated technology and ways of access. Similarly the regulatory environment has been adapted accordingly and is currently undergoing change. In addition since healthcare systems' organisation is a national or regional competence, there is the potential for cross-border barriers to trade and the need for EU-wide co-ordination.

A recent Green Paper and associated staff working document [6, 7] has reviewed the existing EU legal framework applicable to lifestyle and well being apps. The key areas identified by the consultation document relating to the uptake of mHealth in the EU included [8]:

- Data protection, including security of health data
- Big data
- State of play of the applicable EU legal framework
- Patient safety and transparency of information
- mHealth role in healthcare systems and equal access
- Interoperability
- Reimbursement models
- Liability
- Research and innovation
- International cooperation
- Access of web entrepreneurs to the mHealth market

Responses to the EC public consultation document indicated that privacy and security, patient safety, a clear legal framework and better evidence on cost-effectiveness are all required to help mHealth care flourish in Europe. Respondents also suggested that EU and national actions should ensure interoperability of mHealth solutions with Electronic Health Records (EHRs) for continuity of care and for research purposes and that greater emphasis should be put on actions to promote open standards and the use of the common open architecture or open Application Programming Interfaces.

The above Green Paper was also accompanied by a staff working document [7] that outlined the main legislative areas of which app developers need to be aware. These were:

- Data protection
- Medical devices and whether or not such legislation applies to their apps
- Consumer directives

Similarly, due to the impact the development of mHealth may have on individuals' rights to privacy and personal protection the European Data Protection Supervisor issued an Opinion 1/2015 [9] on reconciling technological innovation with data protection which recommended that the EU legislator should:

- Foster accountability and allocation of responsibility of those involved in the design, supply and functioning of apps

- Enhance data security by encouraging privacy by default and privacy by design principles
- Ensure that the sensitive nature of health data should be taken into account by app designers
- Increase transparency and the level of information provided to users about the processing of their data
- Privacy and data protection settings should be embedded in the design and applicable by default
- 'Big Data' should be used for purposes that are beneficial to individuals, such as medical research, and not for practices that could cause them harm, such as discriminatory profiling for employment or insurance purposes

All of these various aspects are of potential relevance to the development of PRECIOUS and should be considered by the project development team.

3.1. Data protection:

Although mHealth [10] is relatively new both the Data Protection Directive 95/46/EC as amended (1) and the ePrivacy Directive 2002/58/EC as amended [11] have provisions that protect the users' rights but these need to be implemented correctly. As indicated above the European Data Protection Supervisor (EDPS) has issued an opinion [9] that addresses the issue of data protection implications on m-Health as well as the ethical and practical implications of the application of data protection principles [12].

3.1.1. Data Protection Directive 95/46/EEC

The issue of data protection has been considered in the report under Task 2.4 Ethical and privacy guidelines (4) for PRECIOUS system implementation and so will not be considered in detail here. In addition a wider discussion concerning data protection in the context of a remote accessibility system and the processing of health information, as well as a consideration of individual country requirements within the European Community is given in relation to the REACTION project [13].

Data and app security need to be considered in the design and development of any app. The particular data concerns will depend on the final format including the amount of personal data input and whether it is a stand alone device or intended to interact with other devices across computer networks and national boundaries. Therefore such factors as whether, and what, information will be stored on the app, encryption of such data and how the app interacts with the wider network will all need to be considered.

In general systems and security should be proportionate and relevant.

The principle item of legislation is the Data Protection Directive 95/46/EC. This is however currently being revised to reflect development in new technologies and globalisation (General Data Protection Regulation (GDPR) COM (2012) 11 Final) [14]. These revisions are discussed below. Currently however this directive prohibits the processing of sensitive data, including that relating to health, although processing can be authorised in strictly limited circumstances:

- Performance preventive medicine; Medical diagnostics; Provision of care or treatment or the management of healthcare services and where the processing of such data is however to be by health professional or one bound by requirement of secrecy
- Requires consent which is to be freely given, informed and specific
- The data can not be further processed for commercial purposes unless duly informed, specifically and explicitly consented

Other principles of data quality also apply. It is also possible for other Member States to have exemptions eg due to reasons of substantial public interest. It can be expected that users of apps in a country other than that where the app was developed would expect the app to comply with the data privacy requirements of that country of use.

In the UK the Information Commissioner's office (ICO) published guidance for app developers – Privacy in mobile apps: guidance for app developers [15]. The guidance is not specific to mHealth apps but is intended to assist with compliance with the main relevant item of legislation ie the Data Protection Act 1998 and ensuring users' privacy. It lists main areas for consideration as:

- Will the app deal with personal data?
- Who will control the personal data?
    - Where and how will data flow when the app is used?
    - Who is the data controller?
- Will data be transferred outside the European Economic Area?
    - Additional privacy requirements apply
- What data will be collected?
    - Privacy impact assessment required?
- How will users be informed and consent obtained?
- How will users give feedback
- How will data be kept secure?
- How will the app be tested and maintained?

Article 29 of the Data Protection Directive 95/46/EC established a Working party on the Protection of Individuals with regard to the Processing of Personal Data [16] which has an advisory status relating to various aspects placed before it. As such it was asked to consider the processing of personal data relating to health in electronic records. This includes a definition of health data. It has also issued opinions on *Apps on smart devices* (17) whereby the relevant legal framework is identified as the Data Protection Directive 95/46/EC, in combination with the specific consent - requirement contained in Article 5 [3] of the ePrivacy directive 2002/58/EC. These rules apply to any app targeted to app users within the EU,

regardless of the location of the app developer or app store. Most conclusions and recommendations in this opinion are aimed at app developers *(in that they have the greatest control over the precise manner in which the processing is undertaken or information presented within the app), but often, in order for them to achieve the highest standards of privacy and data protection, they have to collaborate with other parties in the app ecosystem, such as the OS and device manufacturers, the app stores and third parties, such as analytics providers and advertising networks. Recommendations are given for the responsibility of each within this development chain.* The Article 29 Working party has also considered the use of cloud computing [18].

More recently the Article 29 Working Party has issued an opinion [19] related to the 'Internet of Things' (IoT) [20] particularly in relation to the vulnerability of devices and associated concerns about security and privacy challenges, which provides additional guidance to that provided in previous documents provided by the Working Party, such as that on smart devices as identified above. As such the working party designed a comprehensive set of practical recommendations addressed to the different stakeholders concerned (device manufacturers, application developers, social platforms, further data recipients, data platforms and standardisation bodies) to help them implement privacy and data protection in their products and services. If use of such devices is uncontrolled then it could be considered to be some form of surveillance and this might be considered unlawful under EU law.

According to this opinion paper the PRECIOUS system may potentially be considered to incorporate all aspects addressed in this position paper ie:

- 'Wearable computing' eg watches, glasses
- 'Quantified self' system eg activity trackers, heart rate monitors - which is considered challenging since the data collected can be health-related, hence potentially sensitive, as well as collecting extensive data
- Home automation ("domotics") eg motion sensors, thermostats

What is 'Health' data?

The processing of health data is prohibited under Article 8 of the Data Protection Directive 95/46/EC, unless exemptions apply.

The Article 29 Working Party [16] discusses the wide scope of health data, concluding that personal data are health data when the data are:

- inherently medical data
- are raw sensor data that can be used alone, or, in combination with other data, to draw a conclusion about someone's health status or health risk[1]; or conclusions are drawn about health status or health risk (regardless of accuracy, legitimacy or adequacy)

Sensitive data has special protection and in practice, in the context of IoT requires that data controllers obtain the user's explicit consent, unless the data subject has himself made the data public. Such a situation is likely to arise in the context of the Quantified self devices, which are mostly registering data relating to the well-being of the individual. This data does not necessarily constitute health data as such. However as the data is registered then in time it may provide information on the individual's health thus making it possible to derive inferences from its variability over time. Data controllers are recommended to take account of this change over time and take adequate measures accordingly.

The Article 29 Working Party opinion provides recommendations [19] common to all stakeholders, to operational support (OS) and device manufacturers, Application developers, Social platforms, IoT device owners and additional recipients, standardisation and data platforms. The recommendations for all stakeholders and application developers are reproduced here as being perhaps of most relevance to PRECIOUS, although the full document should be consulted for further detail.

[1] 'Health risk' is discussed in further detail in Work package 3, Report D3.4, section 3.4 which states that "*For the PRECIOUS field studies, we will take into account user characteristics and health risks that may affect the use of the service. This risk score may be calculated from previous medical examinations, and other factors will be assessed with simple questions. The list of variables to be included is as follows: gender, age, weight, height, body mass index (BMI), blood pressure, cholesterol, current physical activity level, current nutrition, current stress, tobacco use, alcohol use, presence of health conditions (arthritis/arthrosis, respiratory problems, heart problems, depression, anxiety, diabetes, digestive problems, pain and others)"*

Recommendations applicable to stakeholders and application developers

Summary:

"In particular, app developers and device manufacturers should provide an adequate level of information to end users, offer simple opt-outs and/or granular consent, when applicable. Furthermore when consent has not been obtained, the data controller should anonymise the data before reporting it or sharing them with other parties".

Recommendations common to all stakeholders

- "*Privacy Impact Assessments (PIAs) should be performed before any new applications are launched in the IoT. The methodology to be followed for such PIAs can be based on the Privacy and Data Impact Assessment Framework which the WP29 has adopted on 12 January 2011 for RFID Applications. Where appropriate/feasible, stakeholders should consider making the relevant PIA available to the public at large. Specific PIA frameworks could be developed for particular IoT ecosystems (eg smart cities)*
- *Many IoT stakeholders only need aggregated data and have no need of the raw data collected by IoT devices. Stakeholders must delete raw data as soon as they have extracted the data required for their data processing. As a principle, deletion should take place at the nearest point of data collection of raw data (eg on the same device after processing).*
- *Every stakeholder in the IoT should apply the principles of Privacy by Design and Privacy by Default.*
- *User empowerment is essential in the context of the IoT. Data subjects and users must be able to exercise their rights and thus be "in control" of the data at any time according to the principle of self-determination of data.*
- *The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. In particular, information and consent policies must focus on information which is understandable by the user and should not be confined to a general privacy policy on the controller's website.*
- *Devices and applications should also be designed so as to inform users and non-user data subjects, for instance via the device physical interface or by broadcasting a signal on a wireless channel"*

Application developers

- *"Notices or warnings should be designed to frequently remind users that sensors are collecting data. When the application developer does not have direct access to the device, the app should periodically send a notification to the user to let him know that it is still recording data.*
- *Applications should facilitate the exercise of data subject rights of access, modification and deletion of personal information collected by the IoT device*
- *Application developers should provide tools so that data-subjects can export both raw and/or aggregated data in a standard and useable format*
- *Developers should pay special attention to the types of data being processed and to the possibility of inferring sensitive personal data from them*
- *Application developers should apply a data minimisation principle. When the purpose can be achieved using aggregated data, developers should not access the raw data. More generally, developers should follow a Privacy by Design approach and minimise the amount of collected data to that required to provide the service".*

Source: Article 29 Working Party: Opinion 8/2014 on the Recent Developments on the Internet of Things Adopted 16 September 2014

3.1.2. Revision of the General Data Protection Directive 95/46/EC

On January 25, 2012, the EC released its data protection legislative framework proposal ("Draft Regulation"), intended to replace Directive 95/46/EC: Proposal General Data Protection Regulation (GDPR) COM (2012) 11[14] final to repeal Data Protection Directive and to provide consistency of data protection implementation across the European Economic Area and provide legal certainty and high level protection of individuals.
Agreement of the “Draft Regulation” was published on 15th December 2015. The final texts were to be formally adopted by the European Parliament and Council at the beginning 2016 and the new rules will then become applicable two years thereafter. The GDPR aims to strengthen the rights of data subjects and also introduces the guiding principles of privacy by design and default as becoming a legal obligation rather than best practice. The legislation will be introduced as a Regulation rather than a Directive to ensure consistent application across the EU.

The Regulation will have a significant and wide-ranging impact on businesses, imposing new compliance obligations and promising significant sanctions for non-compliance. The Article 29 Working Party will be replaced by the European Data Protection Board.

The draft regulation defines health data as:

data concerning health’ means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

3.1.3. ePrivacy Directive

The Directive on Data Protection is complemented by the ePrivacy Directive 2002/58/EC Privacy and electronic communications [11] which specifically addresses the requirements of new digital technologies. In particular, the subject of the Directive is the “right to privacy in the electronic communication sector” and free movement of data, communication equipment and services. This Directive was amended in 2009 by Directive 2009/136/EC [21]. This included a requirement for consent for storage or access to information stored on a subscriber or users terminal equipment – i.e. a requirement to obtain consent for cookies and similar technologies. In addition there is a requirement to advise users of any particular risk / data security breach.

3.1.4. Network and Information Security (NIS) Directive

The aim of the proposed directive concerning the measures to ensure a high common level of network and information security across the Union (COM (2012 238 final) [22] is to improve the security of the Internet and of private networks and information systems. The proposal requires national competent authorities to establish national strategies and cooperation plans to counter NIS threats and incidents. Companies in specific critical sectors

(including health and internet providers) and public administrations will be required to assess the risks they face and adopt appropriate and proportionate measures to ensure NIS.
As apps are used via electronic products which themselves are supplied with embedded software a consideration of required standards applies not only to the app software but to that of the reliability of the device software and associated risks at all levels of usage. EN/IEC 62304 [23] standard is a new global benchmark for the management of the software development cycle. Designing to this standard ensures that quality software is produced by means of a defined and controlled process of software development. Software developed according to IEC 62304 should meet the essential requirements contained in the Medical Devices Directive 93/42/EC, amended 2007/47/EC as related to software development.

3.1.5. Interoperability

In general mobile networks operate to different standards and use different technologies leading to problems with interoperability.
As part of the eHealth Action Plan 2012 [24] published by the EC focus was placed on developing common standards to enhance interoperable healthcare systems among member states so as to be able to make use of Information and Communication Technologies (ICT) to improve healthcare in Europe.

A recent study (published 2013), defines a vision of a Europe-wide 'eHealth' Interoperability Framework (EIF) [25] which consists of four levels of operability: technical, semantic, organisational and legal. These results will be used to specify the deployment of cross-border eHealth services in the framework of the Connection Europe Facility (CEF) [26], but they will also potentially be used for national, regional or project based deployments.

3.2. Medical devices

Although medical apps are not mentioned specifically, the revision of the Medical Devices Directive (Directive 93/42/EEC) which came into force in 2010 [28, 29, 30] amended the definition of a medical device to include the reference to standalone software used for diagnostic and therapeutic purposes.

Under the Medical Devices Directive manufacturers who wish to place a medical device on the market must first register the device with their competent authority and label the device with a CE mark.

As discussed previously there has been a significant increase in recent years in the availability of health and lifestyle applications available through smartphones and wearable technology. Such technology is referred to as eHealth, mHealth or Mobile Health. These vary considerably. In general eHealth covers the interaction between patients and health-service providers, institution-to-institution transmission of data, or peer-to-peer communication between patients and/or health professionals. Health information networks, electronic health records, telemedicine services, wearable and portable personal health systems and other information and communication technology based tools assisting disease

prevention, diagnosis, treatment and follow-up are all examples of eHealth. Similarly such systems vary according to the particular information collected and how, where and how this is stored, the confidentiality of this information, how they are supplied and by whom [31].

In the development of such apps for use in eHealth/mHealth it has been commented that appropriate measures should be put in place to check for clinical risk, security, information governance integration with existing infrastructure and also that the app is fit for purpose [32].

Subsequently the EC has held a stakeholder meeting on the quality and reliability of mobile health applications (6th July 2015) [33]. The meeting was a follow up to the Green paper on mobile health. As a result of the outcome of the public consultation the Commission has started preparations to develop a pro-innovation legal framework aiming to clarify the legal status of health and wellness apps as consumer products. As such and to clarify the borderline between medical and lifestyle and wellness apps work is ongoing to review and update the MEDDEV guidelines. The revision of the MEDDEV guidelines "Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices" [34] includes a specific reference to apps and for example the classification of the software based on location rather than function. Adoption is expected to take place in 2016.

The EC has begun work on an industry-led code of conduct for mobile health apps to address privacy and security issues. It is anticipated that the new code will enable developers to have a clear understanding of their responsibilities and liabilities.

3.2.1. Standardisation

The Commission also announced the intention of developing a European standard on quality criteria for the development of health and wellness apps. It intends to use the UK draft standard PAS:277 Health and wellness apps – Quality criteria across the life cycle – Code of Practice as the basis [35]. This standard is intended to establish the main principles and specify the aspects that app developers would need to consider from the outset so ensuring the robustness of the app development process with an emphasis that the apps are fit for purpose and meet the public need. Such aspects include for example:

- Legislative compliance
- Usability
- Measuring outcomes
- Updating and maintenance of the app
- Sustainability
- Risk assessment

The standard does not address clinical evidence and the guidelines needed for doctors to be able to recommend apps. Nor does it cover requirements for apps that are classed as

medical devices as defined in the Medical Devices Directive or whether an app falls under these requirements

It defines:

a "health and wellness app" as an app that contributes to any aspect of the physical, mental or social wellbeing of the user or any other subject of care or wellbeing

and

"personal data" as any information relating to an identified or identifiable natural person

ISO 13485:2003 [36] specifies requirements for a quality management system where an organization needs to demonstrate its ability to provide medical devices and related services that consistently meet customer requirements and regulatory requirements applicable to medical devices and related services.

Other items of possible interest include:

ENISA - Smartphone secure development guidelines [37]:

This document was written for developers of smartphone apps as a guide to the steps required in developing secure apps.

IPEN – Internet Privacy Engineering Network [38] brings together developers and data protection experts from regulators, business, civil society and academia to work together on privacy respecting solutions for practical problems

3.2.2. Definitions

- Software and medical devices

Applicable legislation [28, 29, 30], which has been amended a number of times, includes:

- Directive 93/42/EC concerning medical devices
- Directive 90/385/EC active implantable medical devices
- Amended by Directive 2007/47/EC which states that:

"It is necessary to clarify that software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, is a medical device. Software for general purposes when used in a healthcare setting is not a medical device".

The Medical Device Directive 93/42/ EC defines a medical device as "*any instrument, apparatus, appliance, software, material or other article, whether used alone of in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used by human beings for the purpose of:*

- *Diagnosis, prevention, monitoring, treatment or alleviation of disease*
- *Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap*
- *Investigation, replacement or modification of the anatomy or of a physiological process*
- *Control of conception*

And which does not achieve its principle intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in is function by such means.

Lifestyle and well-being apps potentially fall within the scope of a medical device or an in vitro diagnostic medical device and as such may be required to comply with the safety and performance requirements of Directive 93/42/EC concerning medical devices or Directive 98/79/EC on in-vitro medical devices respectively. In part whether or not such apps fall within the medical device category depends on what is being claimed for the product.

A manufacturer is therefore advised to contact the relevant national regulatory agency to check whether or not the proposed app would be classed as a medical device, prior to placing on the market.

- Placing on the market is defined as:

"the first making available in return for payment of free of charge of a new or fully refurbished device other than a device intended for clinical investigation, with a view to distribution, use, or both, on the Community market"

- Manufacturer

"the person who is responsible for the design, manufacture, packaging and labelling of a device before it is placed on the market under his own name, regardless of whether these operations are carried out by that person himself or on his behalf by a third party".

The EC has adopted two proposals on medical devices and on in vitro diagnostic medical devices which, once adopted, will replace the existing legal framework applicable to medical devices in the European Union [39].

There are no specific rules defining a lifestyle and well being app from a medical device or in vitro medical device. Guidance has been has been provided by the Commission services (MEDDEV 2.1/6 January 2012 [34] – which includes a decision tree to decide whether a product is a medical device) and also, for example, from the Medical and Healthcare Products Regulatory Agency (MHRA) [40] in the UK. Apps, which are used on smart phones and computers, can be considered as a medical device in their own right if they have a medical purpose. These are referred to as stand-alone software or stand-alone medical devices (as compared with software that is part of an existing medical device eg software that controls a CT scanner).

Thus stand-alone software is that with a medical purpose, which is not incorporated into a medical device at the time of being placed on the market. However software that has a medical purpose could be a medical device.

Combinations of elements or systems are not defined in the directive but there are specific requirements for products placed on the market that combine CE marked devices and non-CE marked devices. For example a combination of a laptop (not a medical device), software that analyses data (a medical device) and heart monitoring hardware (an accessory) is considered to be a system if placed on the market together.

Note: CE marked - Signifies that products sold in the European Economic Area (EEA) have been assessed to meet high safety, health, and environmental protection requirements.

- Software apps:

Such apps are used via mobile devices such as phones, laptops and tablets. These mobile devices can store personal information, tend to be always switched on. Certain key words are more likely to contribute to an app being determined as a medical device including: amplify, analysis, interpret, alarms, calculates, controls, converts, detects, diagnose, measures, monitors [40].

Examples of software apps include:

- Apps acting as accessories to medical devices, such as the measurement of temperature, heart-rate, blood pressure and blood sugars could be a medical device;

- Apps with software that monitors a patient and collects information entered by the user, measured automatically by the app or collected by a point of care device may qualify as a medical device if the output affects the treatment of the individual;

- Apps with software that provides general information but does not provide personalised advice, although it may be targeted to a particular user group, is unlikely to be considered a medical device;

- Apps with software that is used to book an appointment, request a prescription or have a virtual consultation is also unlikely to be considered a medical device if it only has an administrative function.

Software intended to carry out further calculations, enhancements or interpretations of patients images or data, is a medical device. It is also a medical device if it carries out initial complex calculations, which replaces the clinicians own calculations.

Decision support software is usually considered to be a medical device.

In the UK the MHRA regulates medical devices according to the intended purpose as stated by the manufacturer, including claims given in promotional materials for the device such as brochures and web pages.

Medical devices are categorised according to the degree of risk inherent in the device, medical action of the device, duration of use, invasive nature and if the device is powered. Thus the specific class to which a given mobile app is assigned is dependent on the functionality of the app and the manner in which it interacts with or poses a potential risk to the patient.

Should the app be classed as a medical device it will need to meet the essential requirements for its design and manufacture as listed in Annex 1 of the Medical Devices Directive 94/42/EEC (28) and the manufacturers are required to be able to demonstrate that these requirements have been met via a technical file.

In summary requirements for medical devices include:

To be CE marked;

- Effective post market surveillance to be in place (including a registration or activation system to be able to track those sold by third parties)
- Instructions for use – may be required
- Validation
- Adverse incident reporting

Suppliers / Distributors also need to be aware of their responsibilities.

Whether or not the PRECIOUS outcome would fall within the requirements of the Medical Devices Directive 93/42/EC would need to be verified with the relevant national bodies. The outcome of this decision, and thus which aspect of the regulation applies to PRECIOUS, will ultimately depend on its particular functionality, how it is described and claims made and how it is supplied to the consumers as discussed in section 2.3.

For comparison, in America the Food and Drug Administration (FDA) [41] has issued guidance concerning medical devices and health and well being apps: Mobile device applications: Guidance for industry and Food & Drug Administration staff whereby:

'Many mobile apps are not medical devices (meaning such mobile apps do not meet the definition of a device under section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act)), and FDA does not regulate them. Some mobile apps may meet the definition of a medical device but because they pose a lower risk to the public, FDA intends to exercise enforcement discretion over these devices (meaning it will not enforce requirements under the FD&C Act). The majority of mobile apps on the market at this time fit into these two categories. Consistent with the FDA's existing oversight approach that considers functionality rather than platform, the FDA intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended. This subset of mobile apps the FDA refers to as mobile medical apps'.

Some of these new mobile apps are specifically targeted to assisting individuals in their own health and wellness management. Other mobile apps are targeted to healthcare providers as tools to improve and facilitate the delivery of patient care.

FDA intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended.

The FDA strongly recommends that manufacturers of all mobile apps that may meet the definition of a device follow the Quality System regulation (which includes good manufacturing practices) in the design and development of their mobile medical apps and initiate prompt corrections to their mobile medical apps, when appropriate, to prevent patient and user harm.

Mobile apps that are intended for individuals to log, record, track, evaluate, or make decisions or behavioural suggestions related to developing or maintaining general fitness, health or wellness, such as those that:

- *Provide tools to promote or encourage healthy eating, exercise, weight loss or other activities generally related to a healthy lifestyle or wellness;*
- *Provide dietary logs, calorie counters or make dietary suggestions;*
- *Provide meal planners and recipes;*
- *Track general daily activities or make exercise or posture suggestions;*
- *Track a normal baby's sleeping and feeding habits*
- *Actively monitor and trend exercise activity;*
- *Help healthy people track the quantity or quality of their normal sleep patterns*
- *Provide and track scores from mind challenging games or generic "brain age" tests;*
- *Provide daily motivational tips (e.g., via text or other types of messaging) to reduce stress and promote a positive mental outlook;*
- *Use social gaming to encourage healthy lifestyle habits;*
- *Calculate calories burned in a workout.*
- *Mobile apps that allow a user to, collect, log, track and trend data, such as blood glucose, blood pressure, heart rate, weight or other data from a device to eventually share with a heath care provider, or upload it to an online (cloud) database, personal or electronic health record.*
- *Mobile apps that use video and video games to motivate patients to do their physical therapy exercises at home;*
- *Mobile apps that provide pre-diabetes patients with guidance or tools to help them develop better eating habits or increase physical activity*

When these items are not marketed, promoted or intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, or do not otherwise meet the definition of medical device, FDA does not regulate them. When

they are marketed, promoted or intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, or otherwise meet the definition of medical device, FDA intends to exercise enforcement discretion

In the US the FDA has approved over 100 mobile medical applications. It also however takes legal action against those placed on the market illegally.

In the UK the National Information Board [42] has an ongoing project to improve digital services and enable the public to access health and care information, including access to a set of health and care digital apps that will have been endorsed by the NHS. Currently interactive tools, apps and podcasts are available via the NHS Choices tools library [43, 44].

As a follow up to the previous Green paper [6] the EC has recently established a new working group which will develop guidelines, to be published later in 2016, for assessing the validity and reliability of the data that health apps collect and process. The group will build on existing initiatives and best practice and develop guidelines in order to provide common quality criteria and assessment methodologies that could help different stakeholders (users, developers, vendors of electronic health record systems, payers etc.) in assessing the validity and reliability of mobile health applications. In addition, in order to be able to recommend apps to their patients and take apps' data into consideration in a treatment/monitoring process, health professionals need reassurance about the reliability of the apps.

3.3. Other consumer based legislation

3.3.1. Safety requirements

Safety requirements apply to all manufactured products and are defined by

- Directive on general products safety 2001/95/EC [45]
- Directive on liability for defective products 1985/374/EC [46]

However it is not yet clear if and to what extent these apply to lifestyle and wellbeing apps i.e. those not classed as medical devices.

If the lifestyle / wellbeing app is classed and approved as a medical device it is assigned a CE mark. This denotes safety and not effectiveness of the product.

Patient safety is another important consideration. If the product is classed as a medical device then a technical dossier will have been required. The previous ethics report considered clinical risk and hence that aspect will not be considered in detail here.

Information standards underpin the basic requirements re Information Standards Board and have been considered in section 2.1.3.

3.3.2. Product utility and validation

A large number of apps now exist and concern has been expressed that these can be of varying quality for example with respect to the sources of information used and whether these are reliable / trusted.
As indicated above in the UK interactive tools, apps and podcasts are available via the NHS Choices tools library [43]. In addition the NHS mental health apps library was launched in 2015 and details online mental health services that have all been approved for use by the NHS (44).The PRECIOUS project team contains a wide range of specialists including nutrionalists and software developers. This breadth of expertise and discussion with potential users, including the running of focus groups, should ensure a reliable and relevant end product for the consumer.

3.3.3. Consumer Rights

The Directive on Consumers' Rights (CRD) (2011/83/EC repealing 97/7/EC) came into force in all EU member states in 2014 [47]. It applies to traders selling goods, services or digital content to a consumer and aims to simplify consumer rights in certain important areas, mostly relating to buying and selling and maintaining a high level of consumer protection. The Directive provides uniform EU protection.
Although contracts for healthcare are expressly excluded, the directive is considered to cover lifestyle and wellbeing apps [6,7].

The trader is considered to be either the app store (when the consumer downloads the app from an app store) or the app developers (in cases where the consumer buys the app directly from them). The trader has obligations under the CRD to provide the consumer with a series of information in a clear and understandable language and in a way appropriate to the means of distance communication.

3.3.4. eCommerce Directive 2000/31/EC

The eCommerce Directive 2000/31/EC [44] contains information requirements to be provided by service providers, being legal or natural persons, providing information society services.
An Information Society Service (ISS) is any service normally provided for remuneration, at a distance, by electronic means and at an individual request of a recipient of services. 'Free apps' are also covered by this directive which covers any economic activity, including cases in which the remuneration is received from other sources, such as advertising.

ISS service providers must comply with the law of the Member States in which they are established with respect to the setting up and exercise of ISS activities

The directive states the information requirements a service provider (eg apps store) has to provide to the recipient before an order is placed.

The directive also provides a framework for liability for intermediary ISS providers which may be applicable to app stores depending on their activities and whether they are regarded as hosting service providers (providing storage for information provided by the app developer or owner where the information is the app itself).

3.3.5. Unfair Commercial Practices

The Directive on Unfair Commercial Practices 2005/29/EC [49] applies to all business-to-consumer commercial practices, including the selling of lifestyle and well being apps and intends to maintain a consumer's freedom of choice by prohibiting unfair commercial practices by traders.

A commercial practice is considered unfair if it does not comply with the principle of professional diligence and is likely to distort the economic behaviour of the average consumer. In particular commercial practices are unfair if they are misleading or aggressive.

Thus when promoting or selling their products, traders (app stores or app developers) have to avoid any practices which could mislead a consumer or which could compromise his freedom of choice.

Examples related to lifestyle and well being apps are given as:

- False claim of being signatory to a code of conduct or on the approval of the product by a public or private body (eg EC conformity marking)
- Using trust or quality marks without the necessary authorisation
- False claims that a product is able to cure illness, dysfunction or malfunction.

4. Activities in different EU member states

EU legislation is enacted in a number of ways

Regulations

A "regulation" is a binding legislative act. It must be applied in its entirety across the EU.

Directives

A "directive" is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to each individual countries to decide how to do this and to devise its own laws on how to implement this.

Decisions

A "decision" is binding on those to whom it is addressed (e.g. an EU country or an individual company) and is directly applicable.

Recommendations

A "recommendation" is not binding. A recommendation allows the institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed.

Opinions

An "opinion" is an instrument that allows the institutions to make a statement in a non-binding fashion, in other words without imposing any legal obligation on those to whom it is addressed. An opinion is not binding. It can be issued by the main EU institutions (Commission, Council, Parliament), the Committee of the Regions and the European Economic and Social Committee. While laws are being made, the committees give opinions from their specific regional or economic and social viewpoint.

Each member state has implemented the Directives referred to in this document. Directive 95/46/EC as amended on the protection of individuals with regard to the processing of personal data and on the free movement of such data has been identified as the main element of the European legal framework on data protection, and also encompasses health data. As a Directive individual countries have been able to introduce their own national provisions. As indicated previously these national provisions have been discussed in the report of the REACTION [13] project and are well recognised. Since the EC proposal to amend this Directive and to introduce provisions as a Regulation will apply across all of the

European Community member states, it is not now the intention to consider such national provisions further.

Since information collected as part of the PRECIOUS system may potentially become part of a patient's medical record the following table summarises aspects of the national provisions of the member states with respect to electronic health records (50), as this aspect may be a consideration for the project team.

A report [51] of a benchmarking study analysis of the EU member countries about their readiness for mHealth business reported that Germany (19%) and France (17%), whilst offering business potential due to the potential market size, were seen, by mHealth practioners, as having legal barriers such as the prohibition of remote patient treatment and a reluctance to adopt digitilsation of healthcare. Denmark, Finland, the Netherlands, Sweden and the UK were reported to be countries offering the best market conditions for mobile health app companies in Europe.

Summary of particular aspects of national laws on electronic health records in EU Member State

Criteria		Country																												
		AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Data Protection for EHR	General data protection	✓	✓	✓	✓		✓	✓		✓						✓		✓			✓					✓				
	Specific law					✓			✓		✓	✓	✓	✓	✓		✓		✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
Specific rules on hosting and processing of EHRs		✓				✓			✓	✓	✓	✓	✓	✓				✓		✓			✓	✓				✓	✓	✓
Legal obligation to encrypt data		✓															✓						✓	✓						
Secondary use foreseen in law	General research / scientific purpose	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
	Epidemiology				✓						✓	✓			✓		✓		✓	✓							✓			✓
	Statistics	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓				✓	✓	✓	✓	✓
	Other		✓	✓	✓						✓	✓	✓				✓			✓						✓			✓	✓
Safeguards for secondary use	Anonymisation	✓	✓	✓		✓		✓	✓		✓	✓	✓		✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓
	Patient consent		✓						✓				✓					✓					✓						✓	✓
Specific rules on inter-operability		✓	✓						✓			✓	✓				✓	✓		✓			✓	✓	✓			✓	✓	

Source: Milieu Ltd, Time-lex Overview of the national laws on electronic health records in the EU Member Sates and their interaction with the provision of cross-borer eHealth services. Contract 2013 63 02, 23 **July 2014**

5. Summary

This report has outlined the various items of legislation that potentially apply to the PRECIOUS system, a number of which are themselves undergoing amendment to reflect current and future technological developments.
In order for the PRECIOUS system to be placed on the market there are many aspects to be considered including the required appliance and operability standards to be met, data protection requirements (including security, informed consent the handling of health data), whether or not the system falls within the scope of a medical device as well as general consumer protection legislation.

Those items of legislation identified to be of particular initial interest include:

- The Data Protection Directive (as currently revised GDPR) which places requirements for privacy by design and that of informed consent.

- The Medical Devices Directive. The PRECIOUS system consists of appliances (which in themselves may / may not be medical devices) and associated software. Although it is not intended to diagnose disease or provide clinical services, it is however intended to monitor users with the aim of alleviating / preventing those behaviours which could contribute to the development of diabetes or cardiovascular disease. Terms such as prevention, monitoring and alleviation of disease come within the scope of a medical device. The system will also undertake calculations.

  The authority within the UK (MHRA) responsible for medical devices has been consulted for their opinion as to whether the PRECIOUS system falls within the scope of a medical device. Their reply is summarised below:

  As it is still somewhat unclear how the system will be intended to be used, on whom and in what setting they state that they are only able to give very general comments. It does very much depend upon the claims made for the product and whether or not these fall within the scope of a medical device (see Section 3.2.2). The system is currently described as being intended to be used as a preventative care system, in/on patients who are at risk or subject to type II diabetes and/or cardiovascular disease. On this basis it is foreseeable, given the aforementioned claims that the system would qualify as medical device and would need to be regulated as such. If no specific medical claims regarding prevention of disease are made for the product and the product is merely intended to help individual's live healthier lives or make healthier choices then the system would likely not fall within the remit of the Medical Devices regulations. Ultimately a definitive judgement could only be made by the Courts.

This report has outlined those items of legislation of particular relevance and that could potentially impact and inform the development of the PRECIOUS system.

5.1. Overview of the PRECIOUS system and potentially applicable directives

Table 2 below indicates the main legislative elements to be considered with respect to the individual components of the PRECIOUS system and the system as a whole.

If any individual item requires personal individual information which is transmitted and/or stored (connected) then the requirements of the Data Protection and ePrivacy Directives apply. Consumer legislation applies to all products supplied to the public. Standards also apply.

Table 2 PRECIOUS system and potentially applicable EU directives

Location	Component	Legislative consideration			
		Data Protection Directive	Medical Device Directive*	ePrivacy Directive	Consumer Protection Directives
Various	PRECIOUS system overall	YES	To be confirmed	YES	YES
Home	Ambient sensors • Air quality • Temperature • Humidity • Light levels	NO	NO	NO	YES
	Connected sensors	YES	To be confirmed*	YES	YES
	Scales	NO	NO	NO	YES
	Connected scales	YES	To be confirmed*	YES	YES
Individual	Wearable sensors incorp: Gyroscope GPS Activity tracker Food intake monitor / diary	NO	To be confirmed*	NO	YES
	Above individual devices connected	YES	To be confirmed*	YES	YES
	FirstBeat Heart rate sensor	NO	NO**	NO	YES
	Connected heart rate sensor	YES	NO**	YES	YES
Smart devices (phone, laptop, cloud server	Personal data	YES	NO	YES	YES
	Learning module (library)	NO	NO	NO	YES
	Challenge module	YES	To be confirmed*	YES	YES
	Data analysis	YES	To be confirmed*	YES	YES

* It is difficult to give a definitive comment without full details of the products and claims to be made. Once the system and associated claims are finalised it will be necessary to obtain a definitive opinion from the relevant authorities re the status as a medical device.

** As advised by manufacturer

6. References

1. 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 (ref EC1) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=1

2. Armstrong, S. (2015) What app should I use? British Medical Journal BMJ2015;351;h45997

3. PatientView (2014) What do patients and carers need in health apps – but are not getting?

4. Precious project (2014) D2.4 Ethical and privacy guidelines for PRECIOUS system implementation

5. European Commission, (2004) Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area COM (2004) 356 final http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0356&from=EN

6. European Commission, (2014) Green paper on mobile health ("mhealth") {SWD(2014) 135 final}, COM(2014) 219 final Brussels 14.4.2014 http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth

7. European Commission (EC1), 2014 Commission staff working document on the existing EU legal framework applicable to lifestyle and well being apps Accompanying the document Green Paper on mobile Health ("mHealth") SWD(2014) 135 final COM(2014) 219 final Brussels 10.4.2014 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5146

8. European Commission (2015) Summary Report on the Public Consultation on the Green Paper on Mobile Health http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=8382

9. European Data Protection Supervisor (2015) Opinion 1/2015 Mobile Health Reconciling technological innovation with data protection

10. mHealth http://ec.europa.eu/digital-agenda/en/mhealth

11. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&qid=1417002925491&from=EN

12. European Data Protection Supervisor (2015) Opinion 4/2015 Towards a digital ethics. Data, dignity and technology

13. REACTION (2012) Remote accessibility to diabetes management and therapy in operational healthcare networks (FP7 248590) D9-2 Regulatory framework and data protection including patient rights version 3

14. European Commission, (2012) Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – (GDPR) COM(2012) 11 final http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

15. Information Commissioner's Office, 2013 Privacy in mobile apps. Guidance for app developers https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf

16. Article 29 Working party Working document on the processing or personal data relating to health in electronic health records 15 February 2007 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf

17. Article 29 Working party on apps on smart devices 27 February 2013 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

18. Article 29 Working party on Cloud Computing 01 July 2012 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

19. Article 29 Working Party: Opinion 8/2014 on the Recent Developments on the Internet of Things Adopted 16 September 2014 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

20. European Commission - the Internet of Things http://ec.europa.eu/digital-agenda/en/internet-things

21. Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136&rid=1

22. Proposal for a directive concerning the measures to ensure a high common level of network and information security across the Union COM/2013/048 final - 2013/0027 (COD)http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013PC0048

23. EN IEC 62304:2006 Medical devices software – Software lifecycle processes https://www.iso.org/obp/ui/#iso:std:iec:62304:ed-1:v1:en

24. European Commission (2012) eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=4188

25. European Commission (2013) eHealth European interoperability framework (EIF) http://ec.europa.eu/digital-agenda/en/news/ehealth-interoperability-framework-study-0

26. European Commission (2013) EU activities in the field of eHealth: Interoperability and Standardisation: an overview http://ec.europa.eu/digital-agenda/en/news/eu-activities-field-ehealth-interoperability-and-standardisation-overview

27. European Commission Connecting Europe Facility (CEF) https://ec.europa.eu/digital-agenda/en/connecting-europe-facility

28. Directive 94/42/EEC concerning medical devices http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:01993L0042-20071011&rid=1

29. Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32007L0047

30. Amended by Directive 2007/47/EC amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market http://ec.europa.eu/consumers/sectors/medical-devices/files/revision_docs/2007-47-en_en.pdf

31. European Commission Public Health – eHealth http://ec.europa.eu/health/ehealth/policy/index_en.htm

32. European Commission – Medical devices http://ec.europa.eu/growth/sectors/medical-devices/index_en.htm

33. European Commission (2015) Summary of the meeting: Stakeholder meeting on the quality and reliability of mobile health applications 6th July 2015 CNECT.H1 http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=10256 see also Stakeholder meetings https://ec.europa.eu/digital-agenda/en/news/next-mhealth-stakeholder-meeting

34. European Commission (2012) MEDDEV Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices, MEDDV 2.1/6 January 2012 http://ec.europa.eu/DocsRoom/documents/10362/attachments/1/translations/en/renditions/native

35. British Standards Institute PAS:277 (2015) Health and wellness apps – Quality criteria across the lifecycle – Code of practice http://shop.bsigroup.com/ProductDetail/?pid=000000000030303880

36. ISO 13485:2003 Medical devices -- Quality management systems -- Requirements for regulatory purposes http://www.iso.org/iso/catalogue_detail?csnumber=36786

37. ENISA Smartphone secure development guidelines https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines

38. IPEN Internet Privacy Engineering Network https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines

39. European Commission Communication: Safe, effective and innovative medical devices and *in vitro* diagnostic medical devices for the benefit of patients, consumers and healthcare professionals, 2012 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012DC0540

40. Medical Health Regulatory Authority (MHRA) (UK) http://www.mhra.gov.uk/Howweregulate/Devices/Software/index.htm

41. Food and Drug Administration (FDA) Mobile device applications: Guidance for industry and Food & Drug Administration staff. http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm

42. National Information Board workstreams https://www.gov.uk/government/publications/national-information-boards-workstreams

43. NHS Choices : Tools library http://www.nhs.uk/tools/pages/toolslibrary.aspx

44. NHS Choices: Online mental health services http://www.nhs.uk/conditions/online-mental-health-services/Pages/introduction.aspx

45. Directive 2001/95/EC on general product safety (as amended) (GPSD) http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1444689388782&uri=CELEX:02001L0095-20100101 and also http://ec.europa.eu/consumers/consumers_safety/product_safety_legislation/general_product_safety_directive/index_en.htm

46. Directive 85/374/EC concerning liability for defective products http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:01985L0374-19990604&rid=1

47. Directive 2011/83/EU on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European

Parliament and of the Council http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1

48. eCommerce Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&rid=1

49. Unfair Commercial Practices Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Text with EEA relevance) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0029&qid=1417196148900&from=EN

50. European Commission - Overview of the national laws on electronic health records in the EU Member States http://ec.europa.eu/health/ehealth/projects/nationallaws_electronichealthrecords_en.htm

51. Research2guidance (2015) EU countries' mHealth app market ranking 2015