SUMMARY REPORT ON THE PUBLIC CONSULTATION ON THE GREEN PAPER ON MOBILE HEALTH

Contents

1. PURPOSE OF THE GREEN PAPER AND NATURE OF THE PUBLIC CONSULTATION

On 10 April 2014, the European Commission launched a public consultation on mobile health (hereafter "mHealth") in the form of a Green Paper in which it requested stakeholders' views on 11 identified issues related to the uptake of mHealth in the EU.

Stakeholders had 13 weeks to respond to 23 questions on a wide range of themes: data protection, legal framework, patient safety and transparency of information, mHealth role in healthcare systems and equal access, interoperability, reimbursement models, liability, research & innovation, international cooperation and web entrepreneurs' market access.

The Commission has received 211 responses in the context of this consultation.

As regards the methodology, the report provides the total number of responses given per question and reflects the actions and comments most commonly made, specifying where possible the number of supporters for those actions. The report does not provide an exhaustive overview of all the individual responses given. Nevertheless, all responses are published along with this report on our website, except when anonymity was requested.

The purpose of this summary report is to provide an accurate overview of the actions suggested by stakeholders. It does not constitute in any way the views of the European Commission and therefore does not bind the Commission in acting accordingly.

2. EXECUTIVE SUMMARY

Data protection: A strong majority of respondents were in favour of strong privacy and security principles in place in order to build users' trust. The most popular security safeguards put forward were data encryption and authentication mechanisms, while responses acknowledged that health data are sensitive and should be encrypted both “in transit” and “at rest". App developers should only collect, process and store the personal data that is absolutely necessary for the purpose of the collection and take into account privacy concerns from conception of the software and throughout its lifetime. To guide them, they should follow the organisational and technical recommendations of the Article 29 Working Party opinion on apps on smart devices[1]. It could also be very beneficial to draw-up a code of conduct or guidelines covering a series of issues such as privacy, security and user safety.

Big data: Interoperability and the need for standards (e.g. on the way information is processed) were most often cited by respondents as a necessary precondition to fully realise the potential of mHealth generated "Big Data". Clear governance structures to promote the trust of the public in the use of big data were deemed as being key, as well as the necessity to share data from mHealth apps with electronic health records. Nevertheless, anonymisation should always be the preferred option to mitigate risks to citizens' privacy, while there is a need for accountability and control measures.

Legal framework: A majority of respondents thought that safety and performance requirements of lifestyle and wellbeing apps are not adequately covered by the current EU legal framework while calling for a strengthened enforcement of data protection and medical devices rules. In this context, a series of respondents either called for a specific legislation on lifestyle and

[1] Article 29 Working Party opinion 02/2013 on apps on smart devices of 27 February 2013

wellbeing apps, guidance (soft-law) or certification schemes to ensure the safety and performance of lifestyle and wellbeing apps. The need for quality standards or certification schemes was a recurrent issue under different topics of the public consultation (such as patient safety, equal access to healthcare, market access to web entrepreneurs).

Patient safety and transparency of information: Certification of mHealth applications was most often mentioned as a measure to ensure patient safety. Nevertheless, some respondents warned against the risk to 'over regulate', arguing that mHealth apps that qualify as medical devices already need to bear the CE marking. Most respondents also underlined the difficulty to prove the efficacy of mHealth solutions as the latter require long-term studies with health impact assessments.

mHealth role in healthcare systems and equal access: Respondents provided some concrete examples on the uptake of mHealth solutions in healthcare systems of different countries. Tele-monitoring services for chronic heart failure patients and management of diabetes were the most often cited examples. The limited number of responses received on this issue illustrates that good practice examples to support the use of mHealth for higher quality care are scarce and clinical guidelines for the use of mHealth are currently lacking. Many respondents also pointed out that the evidence of economic benefits of mHealth is limited due to the lack of large scale deployments. The most frequently mentioned policy measures at EU and national level to support equal access to healthcare via mHealth were funding and reimbursement, education and awareness raising and ensuring the quality of the products.

Interoperability: While a majority of respondents deemed the actions of the eHealth Action Plan as regards interoperability to still be valid (e.g. by setting-up an EU eHealth interoperability framework), a series of additional actions were put forward such as promoting the establishment of open standards for interoperability. There was also a clear consensus among respondents that EU and national actions should seek to ensure interoperability of mHealth solutions with Electronic Health Records (EHRs) as this would be beneficial for enhancing continuity of care, patient empowerment and research.

Reimbursement models: With the exception of some examples from a few countries, mHealth services are not reimbursed and there is no specific budget earmarked for telemedicine in most of the EU countries. Some respondents noted that there are no incentives for the adoption of mHealth solutions and called for the modernisation of reimbursement systems, while others considered that there is no need to single out mHealth services as they should be made available and funded as part of standard healthcare services provision.

Liability: The compliance with the existing legal framework applicable to mHealth was naturally highlighted as being important in the mitigation of risks. The need for app developers to have a clear understanding of their liability when designing mHealth solutions was considered to be crucial. One solution proposed was the drafting of guidelines or a code of conduct to which they could voluntarily abide. Other solutions put forward were risk mitigation strategies and reporting mechanisms in the case of problems.

Research & Innovation: The vast majority of respondents called on the EU to support further evidence gathering on the role of mHealth, its use and impact, including common methodological approaches to compare the collected evidence. Research & innovation should

also continue on mHealth in disease management (covering patient safety aspects) and innovative care pathways, while agreeing on the significant potential of location-based services in mHealth.

International cooperation: The EU should focus on supporting the adoption of international standards covering the development of adequate security and privacy mechanisms for mHealth, while more should be done on exchange of best practices in the field with third countries. In this context, various examples of good practices in other markets, e.g. in the USA, China, Africa were mentioned. In addition, the need to strive for international convergence of regulations related to mHealth was cited.

Market access to web entrepreneurs: A majority of respondents considered that web entrepreneurs faced problems when accessing the market, whilst one quarter thought that market access is not a problem, arguing that it is a flourishing market dominated by SMEs and web entrepreneurs. The most often cited barriers to accessing the market were: the lack of a clear regulatory framework and the complexity of legislation; difficulties in providing scientific evidence; lack of interoperability and common quality criteria and standards; knowledge barriers between entrepreneurs and users. Respondents also mentioned as barriers the difficulties in accessing medical expertise as well as EU funding, such as under Horizon 2020. Building a platform for exchanging experiences and enhancing cooperation between different stakeholders were seen as important tools at EU level to stimulate the involvement of industry and entrepreneurs in mHealth.

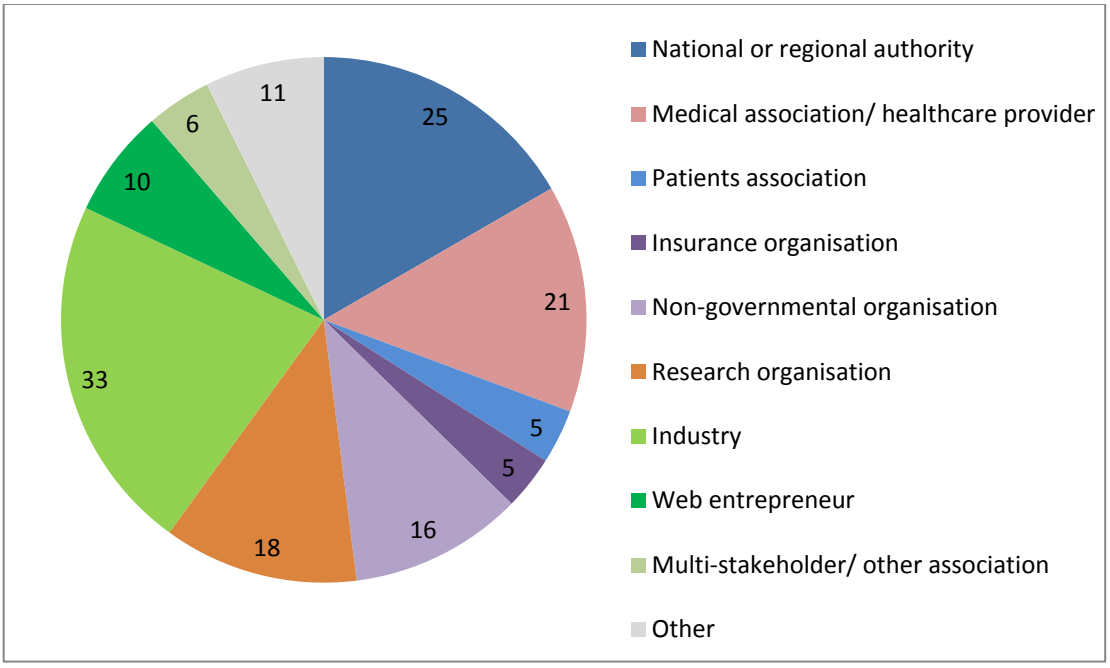
3. PROFILE OF THE RESPONDENTS

3.1. Number and type of respondents

A total of 211 responses were received with 71% of the responses coming from organisations and 29% from individuals[2]. The distribution of the contributions from organisations across sectors is as follows: 29% were received from businesses (including manufacturing industry (13), web entrepreneurs (10), pharmaceuticals industry (9), telecommunication companies (4) and industry associations (7)), 17% from national (18) and regional authorities (7), 14% from medical associations (18) and health care providers (3), 12% from research organisations, 11% from non-governmental organisations, 4% from multi-stakeholder and other associations, 3% from patients associations and 3% from insurance organisations. Figure 1 illustrates the distribution of respondents by sector and type of the organisation.

[2] 34% of the individuals expressly requested to remain anonymous and thus will not be published on our website. Organisations were not provided with this possibility.

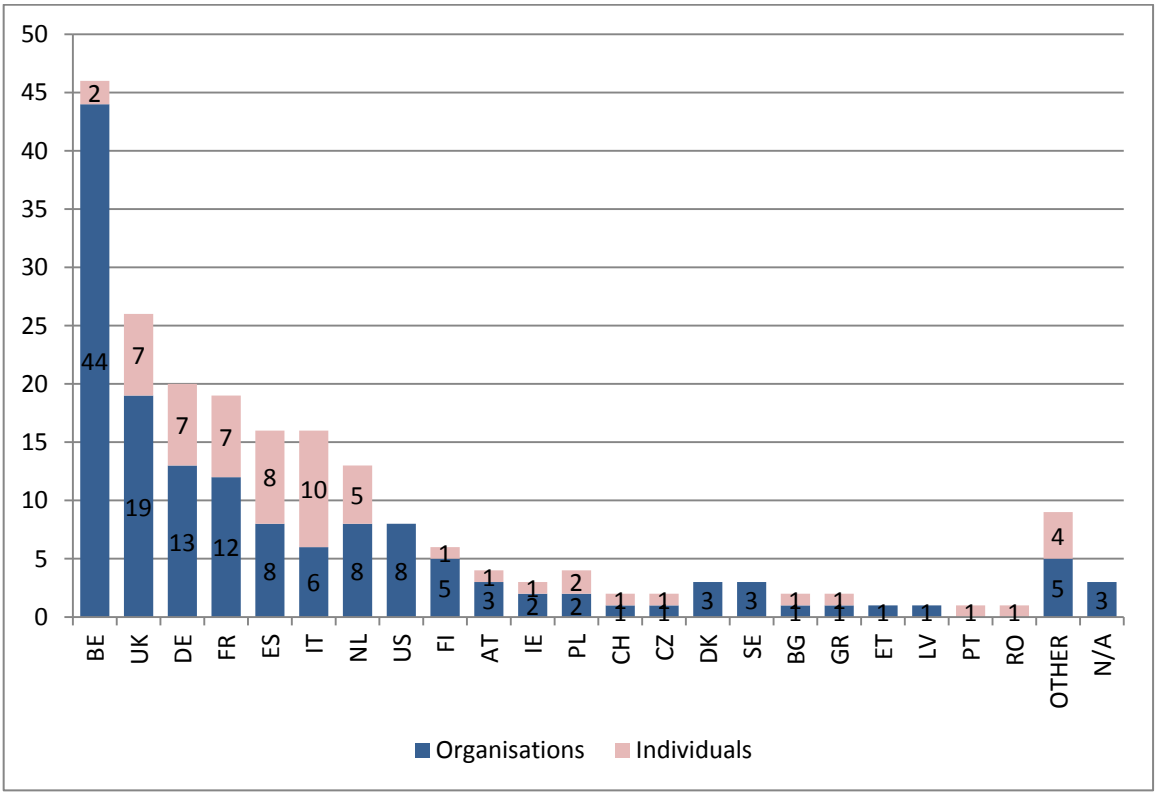
Figure 1: Distribution of responses by sector and type of the organisation



3.2. Geographical distribution of respondents

Figure 2 shows the distribution of the responses across the EU according to the countries (number of responses), with the largest number of responses coming from Belgium (47), United Kingdom (26), Germany (20) and France (19). We received 19 replies from outside the EU coming from the United States (8), Switzerland (2) and other countries (9).

Figure 2: Country distribution of responses



4. SUMMARY OF THE RESPONDENTS' CONTRIBUTIONS BY ISSUE

4.1. Data protection, including security of health data

1. Which specific security safeguards in mHealth solutions could help to prevent unnecessary and unauthorised processing of health data in an mHealth context?

Out of the 128 responses received, a strong majority were **in favour of strong privacy and security principles (97)** to build users' trust. As regards security safeguards, several respondents underlined the need to draw **a distinction according to the purpose of the mHealth solution**, whether to be used for healthcare intervention or for a purely consumer nature to assess the degree of security needed (21).

Solutions & actions proposed

Several respondents drew attention to the necessity for developers to **draw well-designed mHealth workflows** that address users' needs and prevent unwanted third party access. Many respondents also emphasised the **importance of users' awareness campaigns** on the security aspects of these solutions.

Interestingly, respondents were **divided on whether or not it is more secure to keep data** generated by mHealth solutions **on the device (15) or on the cloud (17);** the latter argued that data storage on the device is currently unsafe, with back doors allowing toolkit developers to capture data.

The most popular solutions put forward were **data encryption** (26) and **authentication mechanisms** (18). Regarding encryption, responses acknowledge that health data are sensitive and should be **encrypted both "in transit"**, while being communicated– **and "at rest"**, when the data are saved at its final destination.

Similarly, 31 responses emphasise the **importance of secured networks settings**[3] to prevent data interception, with specific security safeguards for mobile networks. In that respect, some responses drew attention to a series of initiatives from the mobile industry to protect mobile networks and users in case of theft or loss of their mobile devices[4].

On authentication mechanisms, many respondents promoted the use of digital certificates, biometric parameters, tokens or log-tracking techniques, authentication of the access by providing a password; authentication of the device and authentication of the person that logged in. They also suggested **using similar techniques as in the banking sector**, which is quite advanced in ensuring a safe access (digipass, sms authentication etc).

[3] Several respondents recall the upcoming Directive on Network and Information Security will further harmonise requirements for all operators of critical infrastructure, such as healthcare, to adopt appropriate steps to manage security risks and report serious incidents.

[4] Lost and stolen handset reporting policies and mechanisms already exist so that mobile customers can report and bar access to services and lock down lost or stolen devices and prevent unauthorised tampering of unique device identifiers.

Other security safeguards to be followed by mHealth developers **according to the risk and sensitivity of the data processed** were anti-theft protection of the software; safe protocols of the data transfer (SSL), deletion of the data in case of loss of the device, fireware and firewalls on the servers as well as anonymisation of the data processed.

To avoid any unauthorised access to personal data (e.g. mobile phone theft), upon request of the owner, the mHealth provider should be able to delete the app and any related data on the stolen device. A few respondents (3) warned that security measures should not prevent the use of assistive technologies by users with disabilities.

Several respondents (18) considered that **security and privacy standards are crucial** in this field, while 4 responses even considered that policy action could be focused at **mandating such standards**.

Interestingly, responses showed that the issue of adequate security safeguards is also closely linked with the **need to have clear access controls in place** and to obtain **user's consent (32)**. This requires for instance that **access to data is tracked** and documented by the system. Unauthorised access attempts should thus be recorded and reported immediately to the data controller.

While some respondents (8) considered important to **exclude technology-specific security requirements**, others (9) were in favour of **mandating certification of mHealth solutions as regards data storage**[5]. Some respondents considered that cloud services should be provided by trusted providers, while some supported the idea of dedicated clouds to store encrypted health data.

2. How could app developers best implement the principles of "data minimisation" and of "data protection by design", and "data protection by default" in mHealth apps?

The success of manufacturers of mHealth products and services **relies on their capacity to build trust** from a wide range of users. Nevertheless, the current app business model seems widely based on the re-use of personal data, which is particularly problematic when dealing with information that relates to the health status of individuals.

The key principles of "data minimisation", "data protection by design", and "data protection by default" **will become central requirements to be complied with** once the proposed data protection regulation is adopted[6]. 110 people provided a response to this question.

Data minimisation

The principle of data minimisation means that **app developers should only collect, process and store the personal data that is absolutely necessary** for the purpose of the collection.

[5] The specific example of France was given where it is provided by law that cloud providers can only store health data after having been certified by a national public authority (ASIP Santé), due to the sensitive nature of those data.

[6] Commission proposal for a regulation on the protection of individuals with regard to the processing personal data and on the free movement of such data, COM 2012/0011, 25.01.2012

A strong majority of respondents favoured this principle and recommended a transparent communication on the need to collect more information than necessary. Several respondents recognised the need for **app developers to be more specific about what data** is collected (12), arguing that many user agreements are left open to provide the possibility to extend data collection.

Some suggested to use a third party, as "trust provider", to ensure that data collection is kept to the minimum needed (3), while **privacy impact assessments** were also suggested as a key tool to determine which data are required and which not.

Data protection by design and by default

Data protection by design includes features such as anonymity, explicit consent, minimisation of disclosed data as well as secure transfer and storage of data.

Many responses underlined the need for app developers to take into account **privacy concerns from the software conception throughout the lifetime** of the software. They also stressed that due to the sensitive nature of the data collected, developers must **ensure by default** that personal data **cannot be accessed by third parties** without data subject consent.

Several respondents recommended that mHealth app developers ensure the anonymisation or pseudonymisation of the data collected (16), while many underlined the need to prevent the developed software from accessing any other data stored on the mobile device (12).

According to a number of respondents (8), privacy by design also requires that citizens and mHealth users have a **good understanding of privacy issues,** for instance by making users aware of privacy default settings or ensuring that important information is not hidden to mislead them.

Several respondents suggested app developers follow the organisational and technical **recommendations** of the **Article 29 Working Party opinion on smart devices** (8)[7]. Other relevant documents mentioned included **ENISA smartphone secure development guidelines**[8].

Nevertheless, some argued that specific requirements could **dramatically increase the cost** of designing and producing ICT products, thus having a negative impact on innovation and SME access to this emerging market (3).

One solution put forward by several respondents lies within **standards**, eHealth standardisation profiles coverage should be extended to answer the market and the patient/citizen expectations in terms of data protection.

These principles should be built-in to any robust system, using standards that promote safety in the context of innovation. Some respondents expressly mentioned the benefits of Privacy-Enhancing Technologies (4), which the EU should support by funding projects to develop such technologies in the mHealth domain.

---

7 Article 29 Working Party opinion 02/2013 on apps on smart devices of 27 February 2013

8 ENISA Smartphone Secure Development Guidelines of 25 November 2011

Furthermore, while the harmonisation of data protection rules at EU level was welcomed by several respondents; some nevertheless called on a **shift of data protection rules towards a risk-based approach** (6).

Some responses recalled the importance of guaranteeing that collected personal data will not provide discriminatory effects against the individuals concerned (3). Several respondents (9) supported the development of a **code of conduct or guidelines** for mHealth, covering a series of issues such as privacy, security, user safety. Several respondents recalled that **personal data** processing by apps or mHealth solutions **cannot be "owned" by the developers**, the host provider etc.

Finally, some responses invited the Commission to invest in projects to develop and share best practices on data protection by design. Other respondents encouraged the Commission to draw guidelines on data protection for mHealth manufacturers to include the principles of privacy by design and by default.

4.2. Big data

3. What measures are needed to fully realise the potential of mHealth generated "Big Data" in the EU whilst complying with legal and ethical requirements?

The responses to this question (106 responses in total) can be divided in two parts. The first type of responses focused on general elements promoting the use of big data in the EU. The second type of comments focused on specific measures concerning patients, such as the need to ensure patient control over data, anonymisation, misuse, (legal) protection of individuals, etc.

General measures

The general line is that **transparency is necessary to increase trust** of the public in the use of big data. Currently, citizens do not feel they are appropriately informed about the use of their personal data.. It should be **clear what kind of data is gathered, who is using it and what it will be used for.** Specifically the concept of an **open registry** or registration was mentioned several times for tracking information about health related "big data" projects. But it is equally important to ensure citizens are made aware of the great potential of big data for better healthcare outcomes so that they can take informed decisions about their data.

Strongly related to the transparency and trust issue is the need for **clear governance structures** to promote the trust of the public in big data. It was suggested that the governance structures should include an approval process by an independent research ethics committee.

Interoperability (12) and the **need for standards** (29) were most often cited by respondents as a necessary precondition to fully realise the potential of mHealth generated big data. Secondary data linkage should be facilitated for researchers, health care providers and authorized persons (via consent), according to some respondents. This requires **standardizing the way information is collected, stored and shared**. With adequate standards it will be easier to share and make use of data generated by different systems and improve their quality and reliability. Standards should be open, focused on data-management and the way information is encrypted and de-identified. Standards are also often referred to as necessary items to make sure systems are not unnecessarily closed.

Whereas there seems to be consensus that without supporting infrastructure and methodology it will be difficult to create a safe big data sector for health, the question remains as to how much standardization is possible or needed.

Many respondents stated that there is a **need for a legal framework, focusing mainly on protecting patients** (22), to provide clear rules on processing and data usage, but also on what is legally and ethically acceptable in the use of big data. Existing bodies (e.g. Article 29 Working Party, eHealth Network) were referred to, to play a role and facilitate the creation of a legal and ethical framework to ensure big data can address important cross-border health challenges.

Some respondents also considered that to achieve the full potential of big data, it is **necessary to connect the mHealth applications to the data within Electronic Health records**.

Specific measures to protect patients/citizens

Concerning specific measures to protect the public from negative effects of the use of big data, respondents suggested ensuring anonymisation or pseudonymisation of personal data (49). These measures are often seen as a prerequisite to make proper use of big data in health research. There should be EU **agreement/guidelines on how anonymisation is done in a reliable and safe way**. It was however also mentioned that sometimes anonymisation can make a data-set useless for specific types of research. A middle way must be found where the data contains enough personalized data to be useful, but that it does not create negative personal effects for the data subject.

The importance of giving control to patients over their data was also often referred to (11). **It should be the patient who decides what kind of information he/she wants to share**, while keeping the right not to share. It must also be possible for the patient to see who is using the data and for what purposes. Current models for notice and consent on privacy are not working in the new area of big data. New models should be developed which simplify the patient's choice and control.

It was pointed out that besides the opportunities of big data in health, the possibility to misuse the information is also significant. Misuse needs to be prevented as much as possible, by developing secure techniques and infrastructures. Tracking devices to make sure that the ones who are misusing the data can be held accountable could increase trust. In general **more attention should be paid to the implementation of accountability and control measures by the EU**.

Some patients are more vulnerable than others. It was recommended that these sub-populations (e.g. patients with rare diseases) are included in the debate.

4.3. State of play on the applicable EU legal framework

4. Are safety and performance requirements of lifestyle and wellbeing apps adequately covered by the current EU legal framework?

Safety and performance requirements of lifestyle and wellbeing apps are not adequately covered by the current EU legal framework, according to a clear majority of respondents (71 out of 121), while only 29 considered they are adequately covered.

To tackle the current legal vacuum, a notable number of respondents pointed out **a need for a specific regulation** on lifestyle and wellbeing apps (26). A remarkable number of respondents (18) mentioned that **guidance (soft-law) would be needed**. In addition, introducing **quality labels** or **certification schemes** to ensure the safety and performance of lifestyle and wellbeing apps was cited several times (10).

A few respondents (3) pointed out the need for **a progressive and flexible legal framework**, not stifling innovation and taking into account developments in technology, as the majority of app developers are individuals or small companies.

Many respondents (17) stated the need to clarify the borderline between apps which are medical devices and those which are lifestyle and wellbeing apps. Setting up guidelines, such as the **EU MEDDEV guidelines**[9], providing clear rules and examples, was often supported. Some respondents thought that the Directives on general product safety and liability for defective products should apply to lifestyle and wellbeing apps (5). A few respondents also underlined the **issue of apps that disguise their real intended purpose** in order to fall out of the scope of the Medical Devices Directives.

A lack of adequate data protection rules and a lack of measures to ensure the security and privacy of the data collected by lifestyle and wellbeing apps were mentioned several times (7). Some respondents (5) underlined the importance of clarifying the legal nature of data collected by lifestyle and wellbeing apps –**which of these data fall under the definition of "health data"** and which do not (for instance data on your weight and height or data revealing information on your lifestyle, such as nutrition intake, smoking habits or your activity level).

The following remarks were made by individual respondents:

A simple self-declaration by manufacturers – e.g. for medical devices of risk category I – is not sufficient for mHealth apps. The **post-market intended use should be monitored** in real-time and corrected, whenever needed. App stores should have some legal responsibility to vet lifestyle and wellbeing apps against published safety and advertising criteria. One respondent specifically suggested that a specific regulation of lifestyle and well-being apps should be either based on product claims to ensure any claim can be qualified by a manufacturer when asked (soft approach); or based on minimum performance and safety criteria (stronger approach).

5. Is there a need to strengthen the enforcement of EU legislation applicable to mHealth by competent authorities and courts; if yes, why and how?

Half of the respondents (55 out of the 102 responses provided) consider that **enforcement should be strengthened**, as opposed to 17 respondents who were of the opinion that there is no need to strengthen enforcement.

Several respondents (13) mentioned the **need of quality standards or certification schemes** to ensure the quality of mHealth apps. A number of respondents suggested to set-up monitoring (including monitoring of the practical intended use) and alert mechanisms throughout the lifecycle of apps as well as randomized controls of apps to verify their compliance. The need for

[9] MEDDEV 2.1/6 January 2012 Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices

efficient breach management and adequate penalties in case of non-compliance was mentioned a number of times.

A few respondents saw in the proposal for a **Medical Device Regulation a good tool for better enforcement**. The issue of lack of clarity as to whether or not the medical devices directives apply to health-related apps was raised several times. This lead to the request of clearer guidelines with a series of mHealth examples. Some respondents suggested that the European Commission should have a coordinating role to support authorities and courts to decide what is appropriate.

A number of respondents stated that **privacy and data protection should be strengthened** as well as better enforced, including enforcement of quality, privacy and security guidelines for app-generated big data. **Guidelines in the area of cloud computing** were requested several times. In this context, it was mentioned twice that data exchanged between the patient and the health professional could not be property of a third party, such as a social network, a cloud computing programme or software.

The main remarks made by individual respondents were the following:

There is a **need for harmonised standards** and for consistency of the application of EU legislation to mHealth. App stores should remove apps not complying with medical devices legislation from their platforms.

There should be an **EU wide portal of registration for apps** including a comprehensive documentation for each app. A lack of staff to enforce legislation on medical devices was mentioned.

4.4. Patient safety and transparency of information

6. What good practices exist to better inform end-users about the quality and safety of mHealth solutions (e.g. certification schemes)?

The respondents (96 responses in total) focused on the use of certification schemes to assess mHealth applications, the need to share best practices, education and training, and the need to have standards.

General measures

The certification of mHealth applications was most often mentioned in the responses concerning patient safety (more than 40). Respondents expect **certification to guarantee the quality and independency of the information**. It is a tool that will increase trust in the mHealth applications and also gives providers a better understanding of which applications to trust. In this respect, the NHS Choices health apps library[10] in England was mentioned a few times. Health apps are reviewed by the NHS to ensure they are clinically safe. This increases trust and usability. Some respondents (3) mentioned IEC 62304 Certification as a good certification scheme.

[10] http://apps.nhs.uk/

Even though the examples mentioned concerning certification are mainly national, there were several requests to create **a European wide certification/labelling system**. Thus, without discouraging national initiatives; it was suggested that the EC could define over-arching certification principles and leave each country to implement the certification process associated with mutual recognition mechanisms. As an example the STORK project[11] was mentioned. A certification/label scheme could be implemented based on existing standards such as STORK that defines four Quality Authentication Assurance levels ranging from 1 (minimal) to 4 (highest).

A few respondents warned against the risk to 'over regulate'. They were of the opinion that there are already enough certification possibilities in place. As mHealth apps that qualify as medical devices bear the CE mark, any extra practice would hardly have an added value on top of the CE mark regarding safety and quality.

Some respondents emphasized the importance of exchanging best practices about the possibilities to increase safety and quality of mHealth applications. It was stressed that there is no unique mHealth model that can be imposed across Europe, but that **successful models and experiences should be better shared and transferred**. Specifically, it was suggested that a mapping of good practices, or the development of a code on best practices, should be done within the EU.

Information literacy and the need for both patients and providers to understand mHealth use remain an area of interest according to respondents. **Clear guidance and education of potential users** is required to ensure that people are aware of the possible dangers of the applications.

According to many respondents (20+), standards play a key role in terms of patient safety, and transparency of information. It is necessary to have at least national rules, or even EU-level or global rules about how systems such as health data archives should be working together and sharing the data. Therefore, the **development of standards, protocols and guidelines for the deployment of mHealth applications** is urgently required. However, private organizations already have developed standards-based interoperability guidelines. These guidelines have been accepted and published by the ITU-T (Telecommunication Standardisation Sector of the International Telecommunications Union) as official standards (like H.810).

Other remarks concerning quality and safety

<u>The following remarks were made by individual respondents:</u>

One respondent noted that there is still a **lack of a scientific evidence base**. All aspects of mHealth products should be **made accessible to blind and partially sighted people**. The level of quality and safety necessary is different per mHealth application. It should be clear for end users whether and to what extent the solution has been tested, which organization has certified it, where data is stored, and which legal framework applies in the case of conflict.

7. Which policy action should be taken, if any, to ensure/verify the efficacy of mHealth solutions?

[11] https://www.eid-stork.eu/

Out of the 128 people who provided an answer to this question, most of the respondents noted the **difficulty to prove the efficacy of mHealth solutions** as the latter require long-term studies with health impact assessments.

Respondents were **split as to whether or not policy action is needed** to support the development of safer mHealth solutions. Six respondents expressly supported a "do nothing approach" emphasising that the current legal framework is adequate as it already imposes safety requirements on mHealth solutions that can pose a risk to user's safety, i.e. those with a medical purpose. They acknowledged that **most mHealth apps available on the market today do not meet the definition of a medical device**. In their views, those solutions should not be subject to Union action, as **only products that are of higher risk should be required to demonstrate efficacy**. They also underlined that the product cycle of the mobile solution is much faster than that of a traditional medical device, thus the clinical study may not fit the nature of the mobile device development.

On the contrary, several respondents (13) considered that **all mHealth solutions should be submitted to safety requirements** with some expressly requesting legislation to be enacted or binding policy actions. A few respondents expressed the view that **app stores' role is crucial in ensuring compliance with safety requirements**. Six respondents also emphasised the importance to impose an **obligation to verify the medical contents** of apps by healthcare professionals.

Solutions & actions

Out of the actions put forward the most popular one was the **development of certification schemes** (27 out of 121). According to respondents, such schemes would ensure the quality and safety of mHealth solutions that are not already covered by mandatory schemes like medical devices.

Some respondents **supported a government-led certification** (8) either by the national health authority or the consumer agency or existing independent evaluation bodies. The latter is deemed appropriate given that non-medical device solutions are consumer oriented.

Some respondents preferred, however, **a more flexible approach where the certification or the quality labelling is done on a voluntary basis** (20). These responses considered that there is a role to play from the private sector; either from a private entity in the field of certification and testing, from organisations representing health professionals and patients, or from developers themselves, to endorse apps in order to increase their credibility and quality. Some respondents were in favour of the **adoption of codes of conduct** (6) or guidelines to help developers. Along this line, a series of respondents (11) expressed the **important role that standards can play** to increase credibility of mHealth solutions, especially as regards their effectiveness. A few respondents were in favour of **a graduated approach in the policy response**: the support of self-regulation in a first stage, while not disregarding the option of legislating in case self-regulation remains ineffective.

Other suggested actions related to the setting-up of **national bodies to review mHealth solutions**, **such as the NHS health apps library** in the United Kingdom; or the creation of rating schemes targeted at effectiveness, involving users and health professionals. Also, development of **"testbeds" or "ecosystems" throughout the EU** was suggested as they could act as testing,

developing, living lab environments for new solutions and provide for the right framework for evaluating health economics and outcomes of mHealth solutions (to support more evidence on efficacy).

Finally, some respondents (5) expressly mentioned that the Commission could be in charge of **setting-up an EU platform for experts to draft recommendations on efficacy** of mHealth solutions.

8. How to ensure the safe use of mHealth solutions for citizens assessing their health and wellbeing?

The 154 responses to this question were focusing on two different aspects. Some responses focused on quality, security and safety issues, and a general need to create some kind of regulation (mandatory or voluntary) for the mHealth market. Other responses focused on the user's need for transparency and user-friendly products.

Quality of mHealth solutions, certification and labelling of products

Many respondents stressed the importance of keeping a clear distinction between medical and lifestyle (wellbeing) mHealth solutions; they also underlined the need to impose **certified and labelled products** used in situations where patients' health could be at risk (30).

Many responses considered that more should be done on **certification**, but although many consider that such task should be undertaken by regulatory authorities; some respondents preferred a private or research-based certification process. General measures were often mentioned, such as the development of **common criteria** and **standardisation** that will allow evaluation, certification and recommendation of mHealth apps. The need for **standards** (e.g. for quality, safety, usability and communication) was often mentioned (19). Some of the respondents were in favour of mandatory or voluntary **labelling** schemes. Some of the respondents also expressed a need for easing the reporting of safety issues.

The risk of **entering wrong data** and receiving inaccurate results was mentioned as well. Correct and high quality information is likely to lead to safer mHealth solutions. This could be achieved for example by making it obligatory to publish the professional medical bibliography on which the application is based.

Research or evaluation was mentioned in some of the responses as means for securing the quality of the products as well as for providing instruction on **how to use the app appropriately**.

Information and knowledge, usability

Another aspect that was often mentioned with regard to ensuring safe use of mHealth solutions was the need of transparent **information for both** patients and healthcare professionals (8). Patients should be advised to seek medical advice in case of doubt.

Many respondents emphasised the **usability aspect** (10). Accessible information must be available to e.g. blind and partially sighted people, elderly people or people in poor health condition, or to users with low level of literacy. Remote monitoring devices need to have a user-friendly design.

4.5. mHealth role in healthcare systems and equal access

9. Do you have evidence on the uptake of mHealth solutions within EU's healthcare systems?

A number of respondents (53) cited **different sources of evidence and provided concrete examples on mHealth uptake** in different countries. The majority of respondents did not provide an answer (110) or considered that **there was no or not enough evidence on the uptake of mHealth** (13).

Telemonitoring services for **chronic heart failure patients** (remote ECG and high blood pressure monitoring, remote monitoring of cardiovascular implantable electronic devices etc.) have been implemented in a number of countries (e.g. Spain, France, Czech Republic, Austria). mHealth is also increasingly used for the **management of diabetes** (e.g. France, Czech Republic, United Kingdom, Austria). Other domains of use in clinical practice include follow-up of chronic dermatologic pathologies and sleep apnea remote monitoring (in France), remote monitoring of patients treated with anticoagulants (in Czech Republic), ophthalmologic treatment (in the Netherlands) and mental health.

The "3 millionlives programme" in England has set a target of 3 million patients for telecare and telehealth targeting medical conditions such as chronic obstructive pulmonary disease, type 2 diabetes, blood pressure, body mass index, cardiac arrhythmia and medication reminder systems.

There is also well-established evidence in the 9 European regions which participated in the EU-funded project **Renewing Health**[12]; service solutions are already operational at local level for tele-monitoring and the treatment of chronic patients suffering from diabetes, chronic obstructive pulmonary or cardiovascular diseases. **ENS4CARE**[13] is another EU-funded project, gathering evidence on good nursing and social care practices to develop Evidence Based Guidelines for Nurses and Social Care Workers for the deployment of eHealth services.

Other examples of mHealth applications mentioned include patient health portals and access to personal medical records, secure messaging between health professionals, applications providing information and support to cancer patients and reminder applications for treatment compliance and appointments.

10. What good practices exist in the organisation of healthcare to maximise the use of mHealth for higher quality care (e.g. clinical guidelines for use of mHealth)?

The limited number of responses received to this question (58) illustrates that existing good practices in healthcare organisations to maximise use of mHealth for higher quality care are scarce.

Some respondents (6) explicitly pointed out that **good practice examples** and clinical guidelines for the use of mHealth are currently lacking since there is no consensus on the clinical evidence supporting mHealth. At the same time, it was acknowledged by respondents (7) that **national**

[12] http://www.renewinghealth.eu/

[13] http://www.ens4care.eu/

strategies and guidelines are needed to support mHealth development while implementation of verified and efficient mHealth solutions as part of **clinical guidelines** would be useful.

Some **examples of good practices**, that were highlighted, included: guidelines for the medico-economic evaluation of mHealth solutions (in France); "telemedicine ethical guidelines" and special qualification for eHealth (in Finland); standardized operational protocols to introduce tele-monitoring services in routinely practice (in the Veneto region in Italy); providing training to patients and developing recommendations for the design of mHealth solutions (in Andalusia); guidelines for use in implementing eHealth in long-term care and a dedicated website where patients and experts both review and publish applications (in the Netherlands); the integration of mobile health devices into the guidelines for the management of diabetes published by the United Kingdom National Institute of Health and Clinical Excellence (NICE).

A few respondents reported that there is a dedicated app for clinical guidelines in their country, such as *GuíaSalud* [HealthGuide] app in Spain and NICE guidelines for healthcare professionals in the United Kingdom available in the app format.

11. Do you have evidence of the contribution that mHealth could make to constrain or curb healthcare costs in the EU?

Out of 94 responses received to this question, 25 respondents stated they do not have such evidence and 15 were of the opinion that there is **no real evidence yet or that the evidence is limited as regards economic benefits** due to lack of large scale deployments. It was noted that limited evidence from telemedicine trials show good results for clinical outcomes (reduced mortality) and health care delivery processes (fewer emergency admissions, hospitalisations and bed days); nevertheless these results are not conclusive as to the cost-effectiveness of such solutions. Some emphasised that a series of projects (such as United Kingdom Whole Systems Demonstrator[14] and Renewing Health project[15]) have shown that costs may even increase if implementation of telemedicine solutions is not accompanied by a change in the organisation and daily clinical practice.

A few respondents (2) suggested that the European Commission should **facilitate and centralise the further collection of evidence** on mHealth impact on healthcare costs in the EU. It should also create a robust methodology to be systematically followed for assessing the large scale implementation of mHealth.

Many respondents (21) referred to specific studies and projects which have demonstrated efficiency gains. For example, according to one study,[16] trials in the Nordic countries show that mHealth could generate a **50-60% reduction in hospital nights and re-hospitalization for patients with COPD**. According to the same study, based on data collected from pilots and projects in Scotland and Norway, it is estimated that mHealth could **reduce overall elderly care**

[14] Steventon et al. (2013), 'Cost effectiveness of telehealth for patients with long term conditions (Whole Systems Demonstrator telehealth questionnaire study): nested economic evaluation in a pragmatic, cluster randomised controlled trial', BMJ 346:f1035.

[15] Kidholm et al. (2014), REgioNs of Europe WorkINg together for HEALTH Final Report, Version 1.3.

[16] The Boston Consulting Group and Telenor Group, The Socio-Economic Impact of Mobile Health, April 2012.

expenditure by 25%. Another example is a review[17] on the **effectiveness of electronic reminders** to improve adherence to chronic medication carried out by the Netherlands Institute for Health Services Research; the latter concluded that SMS and e-reminders can be effective in improving patients' adherence in the short run. A number of respondents referred to the PwC report on the socio-economic impact of mHealth[18] according to which mHealth could save 99 billion EUR in healthcare costs in the European Union (EU) by 2017 if its adoption is encouraged.

Several respondents (14) stated, without providing concrete evidence, that mHealth could help reducing costs by decreasing the number of routine visits and hospitalisations; by shortening waiting lists; by initiating treatment at an earlier stage; by leading to better adherence to therapies, hence improving patient outcomes and by contributing to the prevention of diseases and supporting healthier lifestyles.

12. What policy action could be appropriate at EU, as well as at national, level to support equal access and accessibility to healthcare via mHealth?

A number of policy actions at both EU and national levels, were supported by the respondents (111 responded to the question). The most frequently mentioned policy measures were **funding and reimbursement** (31); **education and awareness raising** (30); and **ensuring the quality of the products** (29 responses). Overall, it was acknowledged that mHealth has significant potential to support equal access and accessibility to healthcare.

Funding and reimbursement schemes were considered to be very important policy tools by many respondents. At the EU level, **EU structural funds** and the **Connecting Europe Facility** were highlighted as appropriate tools to deliver interoperable mHealth services. At the national level, **reimbursement schemes** that reward health outcomes and efficiency improvements to stimulate the integration of mHealth in healthcare provision were considered to be crucial. Covering costs by **mandatory health insurance** was mentioned by a number of respondents.

Some respondents (13) underlined the importance of tackling **access to technologies** by disadvantaged population groups. **Subsidies**, **grants or tax relief** for purchasing smartphones, **to support** self-management to prevent hospital admissions were suggested as a possible policy response.

Education and awareness raising of both healthcare professionals and end-users and enhanced digital literacy were considered as an important area for policy action by many respondents, mentioning public education programmes and information campaigns as well as training of health professionals. It was emphasised that end-users should be made aware of mHealth benefits and use; while health professionals would need to be better involved to integrate mHealth into daily practice.

[17] Vervloet, M., Linn, A.J., Weert, J.C.M. van, Bakker, D.H. de, Bouvy, M.L., Dijk, L. van The effectiveness of interventions using electronic reminders to improve adherence to chronic medication: a systematic review of the literature. Journal of the American Medical Informatics Association, vol. 19, 2012, nr. 5.

[18] PricewaterhouseCoopers, Socio-economic Impact of mHealth – An assessment Report for the European Union, 2013.

To increase confidence in mHealth, **ensuring quality of the products and services** was considered to be essential. Provision of clear instructions and user-friendly solutions, in particular taking into account the needs of people with lower digital literacy, of people with physical and mental impairments was emphasised by many respondents. Establishing appropriate **standards, guidelines and recommendations** on data, terminology, interoperability, connectivity, design etc., were mentioned most frequently.

Easy-to-understand **quality labels** were seen as a useful tool by some respondents to ensure more transparency and to increase confidence in mHealth. Fewer respondents called for **a stricter approach**, e.g. requiring rigorous testing and continuous monitoring or establishing Europe-wide certification.

In general, **access to broadband internet and mobile network coverage** were seen as prerequisites for ensuring that everyone can benefit from mHealth solutions (21). Ensuring broadband access (especially in remote and rural areas), availability and affordability of (mobile) internet access were mentioned in this regard by many respondents supporting, for instance, the **Connected Continent proposal** as well as the necessity to have a more coordinated approach to **radio spectrum authorisation** in the EU.

A number of respondents (14) emphasised that further **research and monitoring** would be necessary to have a better overview of mHealth services, e.g. their safety while mapping the obstacles for their adoption. It was also felt by some respondents that stronger evidence-based studies on the usefulness of mHealth solutions are required to demonstrate their cost-effectiveness and added value.

Policy actions to **promote the exchange of good practices** between Member States, involving **relevant stakeholders**, e.g. through the use of existing platforms, such as the European Innovation Partnership for Active and Healthy Ageing, were emphasised by many respondents (14).

In addition, a number of respondents emphasised the importance of **embedding mHealth into overall health system policies**, promoting the innovative care concepts and strengthening the role of the citizen in healthcare systems. Introduction of the electronic health record and online access to health information was also mentioned in this regard.

4.6. Interoperability

13. What, if anything, do you think should be done, in addition to the proposed actions of the eHealth Action Plan 2012-2020, in order to increase interoperability of mHealth solutions?

A majority of the 110 respondents to this question **supported the actions proposed in the eHealth Action Plan**. In particular, the need to foster the use of international standards was quoted by at least 18 respondents. The main standard development organisations named were Continua/ ITU-T (18), IHE profiles (9), HL7 (11), IEEE (7) and SNOMED CT (4).

A **specific approach to procurers**, especially public procurers, e.g. like in the Antilope project, was also supported (11). This means the need to identify de facto interoperability specifications through the **ICT standards multi-stakeholders platform**, which is needed for public procurers to legally refer to those "de facto" standards in their call for tenders.

There was a consensus on the need to develop an **EU eHealth Interoperability framework** (21) (see eHealth Action Plan), and an mHealth subset of it, where the use of selected standards would be fostered. Respondents were divided however on whether it should be made mandatory by EU legislation, or not. Many respondents expressed the view that **those standards should be preferably open** (21) or implemented through a common open architecture, or an open Application Programming Interface that each electronic Health Record (eHR) vendor would publish in order for mHealth applications to access them. Some respondents considered that the EU should play a role in ensuring compliance to this interoperability framework (7).

A **specific approach to vendors** was mentioned (8). Together with the interoperability framework, there is a need to promote and further develop testing and certification schemes in order to enable suppliers to test the interoperability of their solution with others.

A few respondents emphasised the importance to **continue or reinforce international cooperation in the field** (EU-US MoU, Japan, WHO). The necessity to involve the eHealth Network or the Member States to further progress was mentioned as well.

A few respondents (5) stated, however, that there is no need for action regarding interoperability or that it should not be the first priority, because it would have a negative effect on the market.

Furthermore, a series of innovative actions were proposed:

- launching national or EU (or combined) incentive programs to influence local choices (7), ensuring vendor compliance (2) and giving access to open data only to compliant apps (1); developing an EU approach or policies on quality of data was supported by 8 respondents, unfortunately without any concrete proposal on how to progress in that area;

- setting-up an independent body, or institute, or independent governance panel for interoperability (5) or some aspects of it.

14. Do you think there is a need to work on ensuring interoperability of mHealth applications with Electronic Health Records? And if yes, by whom and how?

Out of the 112 responses provided to this question, only 3 were against the idea of ensuring interoperability of mHealth applications with Electronic Health Records. This shows that there is a **clear consensus that interoperability** of such solutions **with EHRs could be of benefit**, in particular when they are medical devices. Respondents provided a series of examples of these potential benefits:

- ensuring continuity of healthcare (e.g. emergency) by broadening knowledge on the patient's health status and becoming a source of information for doctors;

- supporting patient empowerment by giving them the effective way to take control of their data;

- providing access to researchers to this very useful amount of data, provided privacy safeguards are in place.

Several responses pointed out the need to ensure the standardisation of the transfer of these data along with a common methodology, and semantic interoperability (20). Requiring the EHR vendors to **publish (open) Application Programming Interfaces**, preferably based on open standards, so that mHealth apps can access patients' data, was also largely supported (21).

Some responses emphasised the fact that this would require **strict rules on how to integrate mHealth data into EHRs** (only clinically relevant data), who can access it, who may alter it, and under what circumstances. Confidentiality should also be guaranteed, for instance through the use of specific authentication requirements such as “digipass”. One respondent even supported an EU Directive regulating electronic health records.

Several responses (10) considered that the **government should have a leading role** to ensure that interoperability is made with all the necessary safeguards. Some respondents considered that this problem is linked to the necessity of reviewing the efficacy of mHealth solutions, so that data collected are reliable (5).

4.7. Reimbursement models

15. Which mHealth services are reimbursed in the EU Member States you operate in and to what extent?

Out of 81 responses received to this question, 33 stated that mHealth services are not reimbursed in their country. Furthermore, the **lack of long-term reimbursement mechanisms** was specifically noted by some respondents (8). Respondents criticized the fact that there are no incentives for the adoption of mHealth solutions and called for the modernisation of the reimbursement systems. A few respondents suggested that the European Commission could support an initiative to **collect good practices in the area of reimbursement and develop recommendations** for appropriate innovative incentive structures, including funding mechanisms based on health outcomes.

In most cases there is **no specific budget earmarked for telemedicine** in the Member States and funds are allocated on a case-by-case basis to project implementations or publicly funded research projects (e.g. Mobile 50+ in **Germany**). Some of the respondents also considered that there is no need to single out mHealth services, as they are provided as part of standard healthcare provision (e.g. **Denmark, Norway, Czech Republic, Netherlands, United Kingdom**). This is especially the case in tax-funded healthcare systems where there is no reimbursement of healthcare services as opposed to insurance based systems.

However, some interesting examples from a few countries are worth noting. In **Germany,** the first health app addressing eye disorder amblyopia has been reimbursed since March 2014, allowing ophthalmologists in **Germany** to prescribe the vision therapy app. In **Denmark,** there are seven different telemedicine services that are reimbursed and at least two of them (e.g. photos of diabetic wounds and data from measuring devices in the patients’ home) may involve the use of mHealth devices. A study is currently carried out to assess the cost-effectiveness of these services in that country.

In **France**, pilots of telehealth solutions are being implemented in nine regions. Implementation of mHealth solutions could also be supported through procurement processes run by payers to support health management programmes involving amongst others patient support services

and mHealth technologies. For example, the MGEN (Mutualité Générale de l'Education Nationale), covering 3.5 million people, is on its way to implement such a programme in the cardiovascular sector in 2015 in two regions of **France**.

Another example from **France** is the reimbursement for CPAP (Continuous Positive Airway Pressure), where the payment for a service is linked to evidence that the CPAP is being used by the patient on a regular basis. In **the United Kingdom and Italy,** a full or partial reimbursement is provided to cover the cost of a blood glucose monitor for diabetic patients that plugs directly into smartphones, where data can then be uploaded to an accompanying app. In the **Czech Republic,** remote monitoring of implantable devices (pacemakers and ICDs) could be the first type of operation during 2014 to be reimbursed by public health insurance. In **the Netherlands,** mHealth services are made widely accessible. Examples include: internet consultations, self-management programmes, e-mail consultations, telemonitoring, remote healthcare by means of on-screen care and electronic assistance with the supply of medicines. In **Belgium, the "**My Diabetes Link Online" platform is reimbursed and in **Estonia** the "e-ambulance mobile workplace" is state-funded.

Some responses referred to specific examples from the work-place wellness environment where reward systems are established such as mobile tracking of weekly activity & exercise goals, monitoring of body metrics (e.g. weight, BMI), monitoring of vital signs and health conditions, monitoring of nutrition behaviour and healthy eating adherence.

It was also noted that different business models exist for the wellness and medical sectors, whereby **90% of apps for the wellness sector are for free**. In the medical sector, where the app can be prescribed or recommended to the patient by healthcare professionals, the effectiveness of eHealth and mHealth still has to be demonstrated to generate innovative financial models. Establishing the effectiveness of mHealth solutions with a medical purpose would require an agreed evaluation methodology according to some respondents.

16. What good practice do you know of that supports refund of mHealth services (e.g. payer-reimbursement model, fee-for-a service model, other)? Please give evidence.

Responses (47) were split on that question and no trend emerged. Many respondents agreed that as mHealth is a new way of offering health services in a more efficient and cost-effective way, **new refund models are needed** that focus on "**keeping people well and healthy**". It was also noted that most business models in mHealth are still in the development stage.

Some respondents considered that mHealth services that can be classified as medical interventions and thus as integral elements of healthcare delivery should be subject to the same reimbursement conditions as other medical interventions (e.g. home monitoring solutions, sensors, apps classified as medical devices, etc.).

It was suggested that the strongest case for providing funding for mHealth solutions is to **demonstrate the savings to national health systems**, not just in relation to the cost of primary care, but also in the improved health of the population. It was suggested that mHealth developers should also develop solutions for administrative tasks (e.g. reminder notifications, booking of appointments etc.) with the view to replace or improve existing processes and generating savings and that those should thus be provided to patients free of charge. On the

other hand, apps to monitor health conditions and early disease detection associated to ageing are beneficial for patients who may be willing to pay for the service.

Examples were provided of statutory health insurance funds offering apps providing information and counselling on various health topics for free to insured persons as well as mHealth solutions providing monitoring services: e.g. apps covering early diagnosis check-ups; dental prophylaxis; vaccination; prenatal care; checkups for children; lists of physicians and medical specialists, hospitals and clinics in the surrounding area; accident and first aid tips and information about complementary benefits. In **Finland** service vouchers (also **e-Vouchers**) are a common option to get reimbursement, for example to buy health or wellbeing services from various service providers. Multi-provider models (**public-private-partnership, PPP**) are also being tested to provide better services (also e-Services) to citizens via an e-Services portal where they can find information on services related to health and wellbeing from different providers. In **the United Kingdom**, suppliers of telehealth services have offered some customers a payment-by-results contract, whereby payment is dependent on the success of the service, typically in reducing unplanned hospitalisations.

Some **challenges were also mentioned** related to new funding models. For example, it was pointed out that savings from applying m-solutions are not immediately obvious or appear in some other related area, not directly where the investment was made. It was thought to be useful to develop international metrics and methodology for feasibility studies. It was also suggested that the EU could share best practices and conduct pilot projects to find new ways of incorporating private capital as eHealth requires investment upfront to bring savings later. Some initiatives were mentioned for developing mechanisms to enable business cases that extend beyond the boundaries of a single reimbursement entity (e.g. hospital) to benefit from inputs external to that entity, so that downstream (e.g. social services) savings can be financially attributed to improved hospital care.

Concerns were also expressed by a few respondents about the pharmaceutical industry having direct access to consumers through the medium of sponsored apps. It was emphasised that as it is not always clear who is behind an app, the identity of the sponsor should be part of the standard label on health related apps.

4.8. Liability

17. What recommendations should be made to mHealth manufacturers and healthcare professionals to help them mitigate the risks posed by the use and prescription of mHealth solutions?

Out of the 128 responses provided, a general observation that was made by many respondents was that medical solutions typically pose a **greater risk to patient safety** and health than lifestyle solutions. The logical conclusion is that medical interventions should be more strictly regulated, and this is currently the case[19].

Several respondents were concerned by the serious risks posed by medical apps that are not empirically tested. Nevertheless, they also acknowledged that risks to health and safety may

[19] Mobile solutions, which have a medical purpose, fall within the scope of the medical devices directives, currently under review. See SWD accompanying the Green Paper on mHealth.

arise throughout the entire product lifecycle. Different stakeholders (users, developers, health professionals etc.) can be the source of such risks and be held liable when damage occurs.

Actions focused at developers

Several respondents underlined the need for mHealth manufacturers and developers to **comply with applicable rules**, such as on medical device (CE marking) or data protection (data minimisation, privacy by design, adequate security safeguards) in order to prevent or mitigate liability risks.

In that respect, manufacturers need to have a **clear understanding of their liability** when designing mHealth solutions. This requires a clear legal framework **with adequate guidelines** to help manufacturers and developers assess easily with what rules they have to comply (12). Abiding to rules set-out in a **code of conduct** was also supported by 3 respondents.

While **independent testing** was supported by 15 responses, the specific involvement of users and healthcare professionals in such testing was also mentioned as one possible option (7), along with the importance of the user-friendliness of these solutions (7).

Regarding **solutions that provide medical information**, respondents expressed the necessity to make mandatory that such information **be checked by a healthcare professional** (6). In France, websites with a medical content are certified by a non-for-profit organisation chosen by the public authority "Haute autorité de Santé".

Other respondents considered that one key pre-requisite would be that mHealth solutions should in any case provide **adequate information on its functioning**, reliability and the best way to use it – **taking into account the skills and abilities of users**.

Several respondents considered that all mHealth solutions should carry out evaluation studies to study the impact of solutions, as well as a risk analysis accompanied by measures to mitigate risks to users. **11 respondents were in favour of certification**, which is already mandatory for mHealth solutions that are medical devices.

The implementation of recognised security standards was also suggested. Some respondents considered necessary to provide for a **reporting mechanism in case of problems** (13) for instance that would warn a doctor by email in case of abnormal results, while unfair disclaimers should be banned.

Actions focused at healthcare professionals

Some respondents emphasised the importance for healthcare professionals to **receive adequate training** to use mHealth (6), while such training should be given throughout their professional career or be **part of their curriculum** (5).

Professionals should ensure that patients understand how to use mHealth (10), while these solutions should only be seen as supplementary tools, and not replace doctors' diagnosis.

Several respondents suggested the **adoption of clinical guidelines** to help health professionals use mHealth adequately. 11 respondents considered that health professionals can **only recommend or prescribe apps that are certified**, while they should provide the adequate level

of information to users while prescribing them. Not doing so, may be a cause of exclusion of insurance coverage.

A few respondents expressed the view that national laws on liability provide sufficient guarantee to health professionals and that there was no need for further action (3).

Some respondents considered that mHealth solutions put an **unreasonable weight on doctors** who may become overwhelmed with the big amount of data received and bear most of the liability risks due to the fact they are the ones to "take the final decision". The latter will lead to a continuous monitoring of their patients, while doctors may be held liable in case they do not react swiftly to an alert sent from an mHealth solution.

Finally, 4 respondents recommended **taking out insurance** that would cover liability risks arising from the use or prescription of ICT solutions to patients.

4.9. Research & innovation

18. Could you provide specific topics for EU level research & innovation and deployment priorities for mHealth?

A fifth of the respondents (22 out of 108) expressly highlighted the urgent **need for research to demonstrate concrete evidence** on mHealth role, use and impact.

It was pointed out that there is a need for **methodological approaches** to obtain and measure evidence on whether mHealth is producing better health outcomes (5); to analyse the barriers and enhancing factors for the up-take of mHealth solutions from the perspective of practitioners and patients; and to assess the safety, privacy and reliability.

Many responses highlighted the need to take into account issues around **security, privacy, data protection** and data handling in general. Developing further interoperability and standards was considered necessary. Exploring the potentials of big data and research on big data analytics trends were also supported by some respondents. How to **balance security/privacy and usability** especially for big data is to be explored. Integration of heterogeneous data sources is considered to have significant innovative potential.

Evidence on cost-benefits, health economics, business models and bottlenecks in integration in healthcare is needed. It was stressed that research is needed on new ways to measure clinical efficacy and cost-effectiveness (e.g. substitutes for randomised clinical trials as they are not appropriate to mHealth solutions).

The necessity to **assess behavioural impact** as well as the impact on workforce and workforce skills at the interface of health and social care was also emphasised. Anthropological research and sociological research could help in this regard. Many respondents emphasised that evidence should be analysed especially as to **mHealth impact on vulnerable individuals** and groups such as the elderly, people with disabilities or with lower health literacy.

A lot of interest was expressed on more research on **innovative healthcare models (11)**, as well as on reimbursement schemes. Another focus of research should be to adapt and re-structure healthcare systems and services, to create new care pathways that integrate mHealth solutions for marginalised populations.

Key healthcare areas where mHealth brings an added value should be identified to help EU and national policymakers to create European guidelines and best practices.

Collaborative research was proposed recurrently by the respondents in innovative mHealth interventions for vulnerable or hard-to-reach populations, taking into account cultural differences.

Many respondents expressed an interest to **continue research in the area of mHealth for patient-centred care**, self-management, patient engagement and empowerment, tailoring personalised interventions that improve adherence, compliance and disease management.

As a new area for research, it was proposed **to move from patient-centred to relations-centred solutions**, to improve data flows and create extended networks of care (patient, caregiver, doctor, general practitioner, hospital).

Many respondents stressed the importance of **promoting digital and health literacy** and motivating people to use mHealth solutions while informing them about risks.

Improving patient safety was another important area for research. Clinical areas of interventions that were mentioned included chronic diseases, mental health, multi-morbidity, improving quality of life, compliance and adherence to treatment, even more specific areas such as eye health. **Additional domains of innovations in mHealth** that were mentioned included: multidisciplinary solutions e.g. combining mHealth/eHealth/health technology with games for health; research in novel sensors; intelligent sensor networks; IoT research and measurements systems. Research for technological support on communications machine-machine, human-machine, storage, visualisation, or serious games should accompany the development of mHealth solutions.

Other ideas of research that were mentioned included, for example, the development of real time mHealth participatory tracking systems for epidemics, emergency or tracking behaviours; apps for professional training, education and inter-professional communications; and use of mobile solutions in clinical trials.

Respondents also mentioned the need for collaborative research to adequately involve professionals, care-givers, users to **co-design mHealth solutions**, while usability was a strong concern. This requires for instance multi-disciplinary research (social science, medical informatics etc.).

Different instruments were proposed such as promoting partnerships between healthcare industry and start-ups, smart procurement and pre-commercial procurement. A need for **creating scientific boards/bodies for accreditation/certification of solutions** was indicated, as well as self-certification as a solution along with automated testing (as developed by ETSI, for instance).

19. How do you think satellite applications based on EU navigation systems (EGNOS and Galileo) can help the deployment of innovative mHealth solutions?

A clear majority of respondents **agreed on the significant potential of location-based services** in mHealth (41 out of 56). However, some of them said they could not see an added value of

basing mHealth solutions on the EU navigation systems because alternative satellite navigation systems and mobile networks are already used and provide much of what is needed.

Innovative mHealth solutions can be developed in the following areas:

The most useful solutions spotted by the majority of respondents (35) are those tracing people in **emergency situations**, those helping people find local services (hospitals, specialists, drug stores and specific medicines stocks, first-aid points, wellbeing and fitness services) and those helping people with disabilities (e.g. sight loss, loss of memory-Alzheimer), the elderly or people living in rural areas. Especially for the emergencies, respondents found that these services can provide a major added value.

Other situations can be: solutions utilising additional location data offering a **context awareness** (e.g. quality of environment, climate, that could be used in prevention); tracking activity; tracking behaviours; monitoring diseases; guiding (streets); tracking patients at high risk (including mental illness or alcoholism involving self-harm), and tracking expensive health devices. For these other areas, the privacy issue is however highlighted as well as the fact that unauthorised tracking is prohibited. These solutions need to comply with existing data protection rules.

Some respondents from the industry believed that **real-time location technologies** will create **new healthcare services** as the information obtained could be used for instance to observe behaviours in a region, tracking flu or other epidemics.

Satellites can be used for supporting interconnectivity, for instance for telemedicine purposes. Geo-localisation could also help users to communicate with specific communities as well as receiving their support.

Finally, some respondents emphasised that the developed applications can in fact also stimulate and help validate the EU navigation system.

4.10. International cooperation

20. Which issues should be tackled (as a priority) in the context of international cooperation to increase mHealth deployment and how?

Out of the 83 responses provided, several respondents (21) highlighted the need for the adoption of international standards covering the development of adequate security and privacy mechanisms for mHealth, and suggested that **good practice and experience on data protection,** user trust establishment and patient safety should be shared.

Several respondents called on the EU to strive for **convergence of regulations** related to mHealth (9). Some suggested to have internationally agreed regulations of data protection and information security (e.g. ISO 27001), taking the form of **standards**, common approaches to Privacy Impact Assessment or **Codes of Practice**. Several responses also suggested that convergence on medical devices in the IMRDF should continue.

A recent example given of progress on interoperability is a joint project between officials from the EU and APEC to map together the requirements for APEC's Cross Border Privacy Rules

(CBPRs) and the EU's Binding Corporate Rules (BCRs). This mapping project will help the EU and the APEC region protect data transferred across borders.

Increased cooperation with the US for mHealth certification requirements and standards was also mentioned in several responses. One respondent promoted the establishment of a framework for common recognition of mHealth apps certification systems in the EU, while another suggested that apps approved by the FDA should also be granted access to the EU market.

Interestingly, a respondent specifically referred to the EU-US MoU which should strive to agree on the regulatory framework governing regulation of mHealth apps (currently there is no reference to mHealth in the MoU Roadmap[20]). One respondent warned against the increased trend towards international and transatlantic agreements, such as **TTIP** which could impose **unfavourable regulatory conditions on European legislators**. Some respondents also argued that the impact of such an agreement still remains unclear for healthcare and data protection, while supporting the involvement of civil society in the ongoing discussions. Two respondents on the contrary suggested that eHealth be part of such an agreement.

Several respondents also valued the exchange of best practices on mHealth among countries around the world (8), while one respondent expressly called for engagement with the **WHO-ITU for a joint agreement on mHealth for non-communicable diseases**.

Overall, a significant number of respondents raised the **importance of tackling privacy and security of health data** in the area of mHealth. The need of developing and adopting international standards on interoperability to enhance innovation in mHealth was also highlighted by several respondents, as was proper regulation and timely, effective approval procedures for apps. A few responses also suggested tackling the **ethical issues** around mHealth and the need to have apps in the mother tongues of users at international level.

21. Which good practice in other major markets (e.g. US and Asia) could be implemented in the EU to boost mHealth deployment?

Out of the 54 responses provided, seven from both sides of the Atlantic emphasised the need to provide **incentives** for healthcare providers to **implement interoperable EHR systems** as a tool to stimulate mHealth uptake and to include mHealth into reimbursement mechanisms. The **US 'meaningful use**' regulations were cited as an example which the EU could learn from.

Regarding regulation of mHealth applications, the **US FDA Health IT Risk-based Framework** was highlighted as **a good example** to be considered as well as a similar approach in South Korea. Another issue raised was the relatively long time it can take to approve mHealth solutions and apps. It was indicated that the FDA approach to approval takes on average of four to eight weeks, although a stakeholder stated that the FDA had only cleared/approved 110 apps in the past 11 years.

The EU could learn valuable lessons on mHealth innovation **from low to medium income countries** such as **China**, as well as some **African countries** where the deployment of mHealth

[20] Transatlantic eHealth/health IT Cooperation Roadmap, February 2013

services are increasing access to healthcare for rural communities. A respondent urged the Commission to ensure that Europe maintains its lead in new mHealth technologies through dedicated funding streams in Horizon 2020.

A concern expressed by several respondents was the route to commercialisation of new mHealth technologies and ensuring the maximum impact for patients. The **FDA's Innovation Pathway 2.0'** was cited as a good example where approving authorities can engage with innovators much earlier and in a more collaborative way to reduce the time and cost of bringing the same and effective mHealth technologies to patients.

Interestingly, the **South African government** has recently adopted a ten year **nation health insurance plan** that decentralises primary healthcare to clinics and community care services with several pilots including the implementation of mHealth solutions. One European stakeholder organisation called for a **'mHealth Task Force'** that brings together telecommunications authorities and other actors in mHealth to be formed in the EU.

Overall, a significant number of respondents referred to US initiatives and programmes (such as 'meaningful use') which the EU could use and adapt as models for deployment of mHealth in healthcare systems. In addition, the EU could learn valuable lessons in the deployment of mHealth from emerging economies.

4.11. Access of web entrepreneurs to the mHealth market

22. Is it a problem for web entrepreneurs to access the mHealth market? If yes, what challenges do they face? How can these be tackled and by whom?

Out of the 91 respondents who addressed the question, a majority (69) considered that web entrepreneurs faced problems when accessing the market, whilst a quarter (22) thought that market access is not a problem.

Many respondents (19) mentioned the **lack of a clear regulatory framework and the complexity of legislation**, as well as the fragmentation of the healthcare systems and regulatory requirements, as the main challenges. Some respondents (7) also underlined the lack of common quality criteria and standards as a barrier.

Several respondents (13) cited the **lack of interoperability** and the complexity of health IT standards and data structures as an obstacle. Some interesting ideas were put forward on how to tackle the issue of interoperability. For example, it was suggested that member states should provide the central system and integrated infrastructure which would allow integrating all of the different solutions and ensuring interoperability. It was suggested that mHealth developers could benefit from the openness of data related to health IT. For example, by ensuring that Electronic Health Record systems have an open API and adhere to a standard data structure, small app developers could link to them without the need to set up and maintain multiple different interfaces.

Difficulties in providing scientific evidence were highlighted in many responses (12). It was noted that small-scale entrepreneurs are unlikely to have the skills, resources or time required to produce the sort of evidence that is needed for payers. Furthermore, in case of new technologies and very fast paced development, there might not be evidence available when

products come to market. Therefore, it was suggested that **mechanisms to do fast prototyping, testing and evaluating of new products** and also ways to roll them out in practice are needed. Another suggestion to overcome the obstacles was the development of evaluation and testing models for m-services (an incubation programme) that would involve relevant parties and experts and allow ideas to be tested in a controlled environment and help judge the utility of new solutions.

Knowledge barriers between entrepreneurs and users were another frequently mentioned barrier (11). It was noted that small entrepreneurs are facing **difficulties in accessing medical expertise**. The need for partnerships between developers, doctors and other stakeholders was highlighted in a number of responses. It was pointed out that on the one hand, there is lack of knowledge and skills among patients, healthcare providers and decision makers as regards the benefits of technology. On the other hand, the entrepreneurs do not understand sufficiently the needs of health systems and users.

23. If needed, how could the Commission stimulate industry and entrepreneurs involvement in mHealth, e.g. through initiatives such as "Startup Europe" or the European Innovation Partnership on Active and Healthy Ageing?

As regards the **Commission's role** in stimulating the involvement of industry and entrepreneurs in mHealth, many respondents (18 out of 73 responses) agreed that **EU funding,** including Horizon 2020 and funding opportunities under Startup Europe, is an important tool. It was however suggested by some respondents that the tender processes of EU funding mechanisms could be streamlined. As mHealth solutions are often developed in short timeframes, and the rapid evolution of technology makes it difficult to involve many partners working together over a number of years, it was suggested to consider creating calls for shorter term financing and microfinance initiatives.

An equally important area for Commission involvement mentioned by many respondents (19) was **building a platform for exchanging experiences and enhancing cooperation between different stakeholders**. Many respondents mentioned the European Innovation Partnership on Active and Healthy Aging in this regard. Also, the Knowledge and Innovation Community of Active Living and Healthy Ageing (EIT-KIC Health) set up by the European Institute of Innovation and Technology (EIT) under Horizon 2020, was mentioned as a useful mechanism in enhancing the cooperation between industry and researchers.

Finally, innovation centers providing test facilities for mHealth as well as living labs, user panels and ecosystem models were mentioned as a good practice for the development of mHealth solutions, as well as making data available to app developers through application programming interfaces (APIs) applied increasingly, for example, in US and United Kingdom.

5. NEXT STEPS

The Commission is going to assess the proposed actions and will come forward with a set of policy responses based on the results of the public consultation involving all the relevant stakeholders in the course of 2015. If needed, the Commission will carry out an impact assessment on future possible actions.

As mHealth is a fast developing field, the need to enable the market to develop to its full potential should be taken into account and the policy actions should not stifle innovation while striking the right balance to ensure reliability, safety and users' trust.

The Commission will work closely with the Member States to enable stronger policy alignment at EU and Member States level. It also intends to strengthen cooperation at international level, notably with relevant international organisations.

A series of follow-up actions to support mHealth deployment are already foreseen under Horizon 2020 and will be taken into account in future work programmes.