



United to reverse the rise in chronic disease

European
chronic
disease
alliance



Green Paper on mHealth apps Input from the European Chronic Disease Alliance (ECDA) 2 July 2014

About ECDA

The European Chronic Disease Alliance ([ECDA](#)) is a Brussels-based alliance of 11 European health organizations representing major chronic diseases such as: liver disease, kidney disease, respiratory disease, COPD, allergic diseases, cardiovascular disease, hypertension, cancer, and diabetes. Together, we represent over millions patients and over 100,000 health professionals.

In 2010 the alliance's members joined forces to put the case for immediate political action to reverse the alarming rise in chronic diseases which affects more than a third of the population of Europe – over 100 million citizens. ECDA plays a leading role in the prevention and reduction of chronic diseases by providing policy recommendations based on contemporary evidence. Its main priorities are primary and secondary prevention related to chronic diseases and the common risk factors - tobacco use, poor nutrition, physical inactivity, alcohol consumption, and environmental factors.

For further information contact the Secretariat:

Laure Sonnier

E-Mail: info@alliancechronicdiseases.org

Tel.: + 32-2 213 13 12

Which specific security safeguards in mHealth solutions could help prevent unnecessary and unauthorised processing of health data in a mHealth context?

Encryption of data and patient authentication mechanisms are important measures that should be in place so as to improve the security safeguards in mHealth apps. Nevertheless, several other measures are noteworthy, such as a clear and easily understandable warning, at the log-in phase of every mHealth app, stating that the patient's data might be used by other parties. In addition to this, the introduction of a patient/user consent request on the use of his/her data, without detriment to the app's functions. Beyond the measures done at user/patient level, there should also be security measures at the level of Health Professionals, such as authentication mechanisms.

So as to reduce both the risks and the consequences of unauthorised and unnecessary processing of health data, it would be advisable to also introduce data masking and the

principle of minimisation of the data collected. In general, strong data protection rules are necessary so as to guarantee patient's privacy. Hence, app developers should not have the right to sell patient's data to third parties.

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?

A key point for the successful establishment of "data minimisation", "data protection by design, and "data protection by default" principles in mHealth apps is likely to be the establishment of regulation on which kind of information could be collected in mHealth apps, and how the collected information should be treated/processed. As a replacement to legally binding EU Law, The Commission could publish a set of recommendations on the above issues, together with a certification or rating scheme for mHealth apps. This would allow users to know which apps, and to what degree, comply with EU data protection recommendations.

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

The cross reference of different sources of data is crucial in big data analysis. Hence, collection of information by mHealth applications must be done in a way which allows gathered information from different apps to be used in conjunction. Therefore, a minimum level of standardization in the way information is gathered, stored, curated and shared is necessary.

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

("No" choice). Currently, there are no legally binding rules which clearly identify what constitutes a lifestyle and wellbeing app. In addition, there is no indication of which legislation applies to these applications. Consequently, mHealth applications currently fall into a legal vacuum. In other words, app developers that market such applications have currently no clear legal obligations.

Such legal uncertainty leads to serious questions on the safety and performance of mHealth apps. This is due to the fact that, at present, mHealth apps do not go through any kind of quality control before entering the market. Such a situation is in stark contrast with other areas of healthcare delivery, where safety and performance concerns entail a formal, and costly, procedure. Therefore it is of paramount importance to establish EU-wide standards for mHealth applications.

Is there a need to strengthen the enforcement of EU legislation applicable to mHealth by competent authorities and courts?

(“Yes”). Yes, together with the new update on legislation. The importance of this enforcement is even greater when taking into consideration the current lack of binding EU Law in regards to what constitutes a lifestyle and wellbeing app. This is due to the fact that, at present, there are different legal requirements between lifestyle and wellbeing apps, and medical and in vitro diagnostic medical devices.

What good practice exists to better inform end-users about the quality and safety of mHealth solutions e.g. certification schemes?

As stated in the paper, there is a considerable number of mHealth apps (97,000). Still, out of these, only a fraction (200) are part of the European Directory of Health Apps, and only a small percentage is labelled as a medical device – thus going through a regulated control procedure. The sheer number of mHealth applications entering the global market, and the cost involved in their assessment, makes it highly unlikely that any European or National authority will be able to properly test and control all apps on their safety and reliability.

Unless European and National authorities control and evaluate the efficacy and safety of the growing numbers of mHealth apps and app developers, the burden is placed on the end-user, who in general does not possess the required medical expertise to make a correct assessment of the mHealth app. Therefore, an emphasis should be placed in giving the end user as much relevant information possible on the mHealth app. Information on the developer, scope of the app, its functionality, etc., would improve the ability of the end user to make a more trustworthy assessment.

Initiatives such as the European Directory of Health Apps have been instrumental in some respect in providing information on mHealth apps recommended by patients groups and empowered consumers in Europe. However the private nature of such an initiative inherently limits its value in the long-run. Furthermore, non-Governmental Organizations - such as Patient, Consumer, and Medical Organizations – have the potential to contribute considerably to the safety of users in the EU, by identifying safe and recommended mHealth apps.

The European Commission could hence consider setting up an EU platform on mHealth to strategically gather the collective input of key EU stakeholders on relevant apps and to support users in making a more informed decision, thus helping to address the existing shortcomings when it comes to mHealth app safety control.

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

The Commission should ensure that authorisation for commercialisation as a ‘mhealth app’ is dependent on the verification of the app by a competent Health Authority so as to ensure that mHealth apps are in line with current health recommendations and are thus not health/life threatening.

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

One of the greatest considerations for the safe use of mHealth solutions by all citizens is likely to be the disparate levels of e-literacy and health literacy of different population groups, together with cultural, linguistic, age, literacy and social factors. Hence, it is of paramount importance that mHealth apps are developed in a way that is clear and accessible to all, so as to guarantee their usefulness and safety, independently of the user.

To address the above factors it would be advisable to set information standards for app developers for communicating use of data to users. Additionally, a recommendation to reduce the amount of inputs required by the end user to use the app could be established so as to reduce the possibility for errors to occur. So as to address issues that could arise after the launch of the mHealth apps, an EU report centre could be established thus enabling users to report any safety concern.

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

(“No”)

What good practice exists in the organisation of healthcare to maximise the use of mHealth for higher quality care e.g. clinical guidelines for the use of mHealth?

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

(“No”)

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

mHealth apps are designed to be used by smart devices and often require high speed mobile internet connections (3G, 4G). Additionally, the increase in mobile internet speeds is opening new opportunities for new types of mHealth apps. This entails that internet speed requirements of future apps, will be increasingly higher.

The present high cost of purchasing a smart phone - with enough processing power to effectively run the application, the capability of using high speed mobile internet connections, as well as the possession of an acceptable level of future proofing -, together with the current high cost of high speed mobile internet subscriptions, makes current mHealth applications accessible only to the social strata with higher purchasing power. The current economic situation of many European citizens, especially the high unemployment rate among young adults, is likely to lead to a maintenance in the unequal access to mHealth apps in the foreseeable future.

Also, it is necessary to recognise that the availability of high speed mobile internet is highly disparate between European Countries – i.e.: Sweden 63%, Bulgaria 13% - and also between regions of the same country (with a much higher availability in high population density regions).

Hence, although mHealth apps have a considerable potential for health improvement, there is a risk that only the populations with the lowest need for mHealth apps have an access to these same apps - those with close availability of Health Services (populations in urban centres), and enough purchasing power to access specialised high quality Health services.

Therefore, any policy actions should be taken with the goal of:

- decreasing the costs of smartphones so as to make them affordable to the lowest income people
- decrease the cost of high speed mobile internet subscriptions so as to make them affordable to all citizens
- Addressing the existing disparities on the availability of high speed internet connections

For that purpose, it would be advisable that the EC implements a process for effective stakeholder engagement in the policy-making process in order to identify best practises and develop EU wide solutions. An EU platform on mHealth, with all relevant stakeholders, could again be a key tool for the development of sound policy recommendations.

What 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?

Which mHealth services are reimbursed in the EU Member State(s) you operate in and to what extent?

What good practice do you know of that supports the refund of mHealth services e.g. payer-reimbursement model, fee-for-a service model, other?

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?

Risks posed by the use and prescription of mHealth solutions can be found throughout the entire product lifecycle. This entails that different stakeholders (app developers, users, and healthcare professionals) can be the source of risks, and liable for the consequences, related with mHealth app use. Consequently measures should be taken at all levels to address any possible issues. App developers should be made aware of the consequences that might arise from any errors in app programming, and encouraged to keep the highest control standards in mHealth app development. As for healthcare professionals, it is vital that mHealth apps are only seen as a supplementary tool for diagnosis/treatment and not as replacement for current methods. Furthermore, healthcare professionals should ensure that the use of any prescribed mHealth application is only made by a fully informed, capable and motivated user.

What specific topics would you provide for EU level research, innovation and deployment priorities for mHealth?

Misuse and/or development errors - both in programming and in the information used by the app - of mHealth apps, might have a considerable negative impact in the health of app users. Hence, future research should address the above mentioned risks associated with mHealth app use, making them a safer, more reliable and more effective tool.

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

The introduction of EU positioning and navigation systems in the development of mHealth applications, can bring considerable advantages as it allows for the correlation between the position of the user/patient with his/hers health status and/or needs. Such application is valid for both preventive actions, as well as emergent/urgent situations.

An example of applications in the field of emergent/urgent care that make use of navigation systems, these could be designed for example, to inform authorities of the exact location and health status of patient's suffering from life-threatening events (e.g.: diabetic patients with a severe hypoglycaemic event).

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

Considering the current legal uncertainty within the EU, in clearly defining what constitutes a wellness and lifestyle app, it would be helpful to generate a common understanding of what is meant by "mHealth app" and create a prerequisite list. Also, so as to address the risk of a possible increase in healthcare access disparities within Europe, measures should be taken to: guarantee equal availability to high speed mobile internet connections in the whole EU; improve the affordability of smart devices, high speed mobile internet subscriptions and mHealth apps; establish interoperability (EU-wide) of apps and Health related government services; and guarantee security so as to prevent misuse of information.

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

Is it a problem for web entrepreneurs to access the mHealth market?

If needed, how could the European 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?

The potential marketing success of European based apps, is directly related to the number of people to whom this app might be useful. This highlights the need to adapt/reform several areas. Firstly, there is the issue of interoperability. Apps that attempt to centralize patient's information must be able to operate with the different health systems in the EU.

Only by establishing such parameters of interoperability at the EU level, can it be guaranteed that mHealth apps will stay functional, and thus contribute to the improvement of one's health, in all EU Member States.

Secondly, the disparities in terms of availability of mobile internet and affordability of devices should be addressed. As stated in the paper there are considerable differences in mobile internet availability between countries and between regions of the EU, with some countries having mobile internet availability below 20% (e.g.: Bulgaria 13%, Portugal 16%). This will have a direct impact on the number of EU citizens that have access to mHealth apps and therefore the number of potential customers for mHealth entrepreneurs.

Thirdly, it is advisable to clarify legal definition and requirements for mHealth apps. The current legal vacuum involving the definition of, and requirements for, wellness and wellbeing apps can have a detrimental effect in the number of entrepreneurs that invest in the development of mHealth apps. Such effect would likely be related to the risk of becoming involved in costly legal proceedings arising from the disparate interpretations that the current lack of legally binding EU Law on mHealth apps allows.

Lastly, there should be a streamlining of bureaucracy related to possible EU financial support. Considering that 30% of app developers are individuals and 34.3% small companies (2-9 individuals), the application for EU financial support can be costly, both in terms of money and time, which can prevent such small sized developers from seeking support.