European Commission Green Paper on mHealth – Consultation

1) Data Protection (including security of data)

The rapid development of the mHealth sector raises concerns about the appropriate processing of the data collected through apps or solutions by individuals, app developers, health professionals, advertising companies, public authorities etc[1].

4 types of data protection risks can be identified[2]:

- Lack of transparency: Many apps do not have a privacy policy or fail to inform their potential users in a meaningful way about the type of personal data the app may process and for what purposes.
- Lack of free and informed consent: Once the app is downloaded, consent is often reduced to a tick box indicating that the end user accepts the terms and conditions
- Poor security measures may lead to unauthorized processing of sensitive personal data.
- Purpose limitation: personal data may only be collected and processed for specific and legitimate purposes.

Questions:

Q1: Which specific security safeguards in mHealth solutions could help to prevent unnecessary and unauthorised processing of health data in a mHealth context?

EHN: Patients need to be ensured that sufficient measures are taken to avoid data being retrieved by third parties not involved in their medical treatment, included but not limited to health insurers.

The responsibility of securing the data should be of app developers as they determine the purposes and means of the processing of data on smart devices. They must then comply with the provisions on security enshrined in the Data Protection Directive[3] and the e-Privacy Directive[4].

Another aspect is the security of the networks used to transfer these data. Hospitals or medical centers must take all necessary measures to guarantee the security of the data sharing in the framework of

[1] European Commission Green Paper on mHealth, 2014/219

[2] Opinion 2/2013 of the Article 29 Working Party of 27 February 2013 on apps on smart devices

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

interaction with the health data available on the patients' smart devices, in order to prevent the hacking of such data[5].

One solution to data security might be to have it embedded with the app, for instance by encrypting the data and authenticate every device the data touches (sign the code and processes the information). The keys or certificates to read these encrypted data should only be available to healthcare professionals involved in the treatment of the patients and to the authorized data developer.

Q2: 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?

EHN: Apps are able to collect a large amount of data from the device (location data, any data stored on the device, contacts lists, calendar, and other data from the different sensors). App developers must then carefully consider which data are strictly necessary to perform the desired functionality (principle of data minimisation).

It should also be noted that different types of health-related applications exist with some apps (for example a decision-aid tool which does not store data) that would differ significantly from an app designed to store sensitive medical data. For those applications, privacy by design should be encouraged.

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. It is an essential tool in minimising privacy risks and building trust. It can lead to earlier identification of security problems and facilitate the compliance with data protection legislation[6]. App developers should be encouraged to follow a protection by design policy when starting a mHealth project.

2) Big Data

Big data is the capacity to analyse a variety of unstructured data sets from a wide range of sources (data mining).

These data can be a vital element of epidemiological research as they can enable researchers and scientists to improve patient treatment by looking for patterns on a larger scale or draw new conclusions, for instance on the relation between the development of a medical condition and environmental factors.

Question

Q3: What measures are needed to fully realise the potential of mHealth generated "Big Data" in the EU whilst complying with legal and ethical requirements?

EHN: The potential of big data for epidemiological research in cardiovascular diseases is considerable[7]. New prevention patterns or risk factors relationships can be established thanks to the analysis of these data. It is therefore crucial that legislation on data protection safeguard the possibility for researcher to use these data, while ensuring the security of patients' data. Informed

[5] More and more patients come at the hospital with their own device, in agreement with their healthcare professional (BYOD – Bring Your Own Device policies), which can lead to security leaks.

[6] Article 23 of the proposed EU General Data Protection Regulation addresses the issue of protection by design.

[7] A recent example is the Health eHeart Study of the University of California, San Francisco, that will analyse data from up to 1 million participants worldwide to find new prevention schemes for heart diseases.

consent is of course an important issue, but the potential of big data for research is so vast that it is sometimes difficult to predict to which aim and when the personal data will be used. A solution could be the pseudonymisation of such data, enabling researchers to analyse these data without being able to re-identify the patient him/herself. Further legal clarity on the use of data for research is crucial to enable the potential of big data in epidemiological research/studies.

3) EU legal framework

Both the Medical Devices and the In Vitro Diagnostics Medical Devices regulations have recently been adopted by the European Parliament so are still waiting to enter into force in the Member States. It exists then for the moment a lack of clarity whether the current Medical Devices Directive applies to apps and health-related apps. Such clarity is therefore required as to the rules with which they must comply.

Questions

Q4: Are safety and performance requirements of lifestyle and wellbeing apps adequately covered by the current EU legal framework?

EHN: While the Medical Devices and the In Vitro Diagnostics Medical Devices regulations still have to enter into force, and the General Data Protection regulation is still under discussion, health-related mobile applications are currently covered by three Directives.

Concerning the security and user's protection aspects, the main relevant EU legal framework is the Data Protection Directive (95/46/CE)[8]. This Directive says that the data controller (any party involved in the development, distribution and operation of an app) is responsible, alone or jointly with others, for ensuring compliance with all the requirements set forth in the Directive. Additionally to this Directive, the e-Privacy Directive (2002/58/EC, as revised by 2009/136/EC) sets a specific standard for all parties worldwide willing to store or access information stored in the devices of users in the European Economic Area[9].

For what concerns the safety and performance requirements, if the mobile application is to be considered as a medical device, then it must comply with the provisions of Directive 93/42/EEC[10] on medical devices, or of Directive 98/79/EC[11] on in vitro diagnostic medical devices, or of Directive 1999/5/EC[12] on Radio Equipment and Telecommunications Terminal Equipment (RTTE).

Technology is moving fast and all these texts are now out-of-date. This is why the European Commission decided to propose a revision of these Directives. The proposed Regulations does cover many of the current challenges of data protection and safety requirements. Improvements have been made regarding the safety and performance requirements (cf. Article 49 of the proposed Medical

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[9] Opinion 2/2013 of the Article 29 Working Party of 27 February 2013 on apps on smart devices
[10] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices
[11] Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices
[12] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity

Devices regulation on clinical evaluation[13]) however fine-tuning must still be done on some provisions regarding research data and pseudonymisation of personal data.

Q5: Is there a need to strengthen the enforcement of EU legislation applicable to mHealth by competent authorities and courts; if yes, why and how?

EHN: The proposed General Data Protection Regulation and Medical Devices Regulation go into the right direction regarding safety and privacy, notwithstanding the need to safeguard access to data for researchers.

4) Patient safety and transparency of information

The safety of mHealth solutions and lifestyle and wellbeing apps may be cause for concern, explaining the potential lack of trust. In addition, the information these solutions provide can sometimes be insufficient as to who developed them and whether they have undergone appropriate reviews or followed established medical guidelines or clinical tests.

Some app certification programmes, where all apps have passed a review to prove their safety and compliance with data protection rules, are emerging in some Member States.

Finally, safety concerns arise when citizens can use the results of an mHealth solution or app to take decisions on their own health which can have dangerous consequences.

Questions:

Q6: What good practices exist to better inform end-users about the quality and safety of mHealth solutions (e.g. certification schemes)?

EHN: We are aware of two certification programmes in Europe. One is the NHS Choices health apps library[14] in England, proposing health applications that have been reviewed by the NHS to ensure they are clinically safe and relevant to people living in England. The other is the 'Aarts en Apps' project in The Netherlands that review and evaluate mobile health applications.[15] These platforms propose patient-friendly information and clear information on the health-related app, enabling users to download and use them in all safety.

Q7: Which policy action should be taken, if any, to ensure/verify the efficacy of mHealth solutions?

EHN: Certification programmes should be put in place in Member States, to review health applications and inform users of their quality and safety. Such programmes should be run under the authority of the national health system, and friendly to use both for end-users and app developers.

Q8: How to ensure the safe use of mHealth solutions for citizens assessing their health and wellbeing?

EHN: Patients should be discouraged from requesting change to or erasing of data if this compromises the treatment outcome. In any doubt of the use of data, or the data itself, patients should seek advice with their healthcare professionals.

---

[13] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009, 2012/0266/COD

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

[15] http://www.artsennet.nl/Home.htm

Also, information standards for communicating use of data to users with low level of literacy should be put in place. This factor is even more important given the correlation between low literacy and poor health. Policy actions or communication campaigns should be envisaged to minimize the misusage of health data and mHealth applications.

5) mHealth role in the healthcare system and equal access

mHealth is one of the tools that could help EU Member States maintain sustainable healthcare systems as it could support more efficient delivery of care. It should be noted that the introduction of mHealth services may require training for healthcare professionals, adding to their high work pressure.

It is estimated that 15% of healthcare utilization costs could be saved through remote monitoring, via mHealth.[16] However, healthcare providers and potential payers may need further evidence of its clinical and economic benefits before they scale up its adoption.

Finally, according to a recent survey, only one third of Europeans have access to the Internet via their mobile phones.[17]

Questions:

Q9: Do you have evidence on the uptake of mHealth solutions within EU's healthcare systems?

EHN: No.

Q10: What good practices exist in the organisation of healthcare to maximize the use of mHealth for higher quality care (e.g. clinical guidelines for the use of mHealth)?

EHN: No.

Q11: Do you have evidence of the contribution that mHealth could make to constrain or curb healthcare costs in the EU?

EHN: Although several studies show the potential for mHealth solutions to save money for national healthcare budgets (mainly in bed-days related costs), it is important to consider the origins of the studies.

On the other hand, mHealth will inevitably involve some costs at its first implementation, namely for staff training, IT networks upgrading and interoperability ensuring. Downloading an app might be cheap for the patient, but using the data of the app may incur cost to the national healthcare system. We still miss strong evidence to demonstrate the cost-effectiveness of mobile health solutions

Q12: What policy action could be appropriate at EU, as well as at national, level to support equal access and accessibility to healthcare via mHealth?

EHN: As showed by the European Commission Green Paper on Mobile Health, a big majority of consumers had never used their mobile phones for health-related applications. This proves that, even with a high penetration rate of smart devices inside the EU population, mobile health solutions are

[16] European Commission Green Paper on mHealth, 2014/219
[17] Ibidem

still under-used. Although it is said that health-related applications could promote equal access and accessibility to healthcare, adequate evidence is missing and large meta-analysis are required to demonstrate this impact.

A substantial number of CVD patients are over 60 years old, and may not be very familiar or confident with using a mobile health application in the course of their treatment or medication. Information campaigns should then be put in place to reassure patients about the safety of mobile health applications and making clear it will not impair their treatment or medication plan. Both aspects are critical to ensure patients' trusts in mHealth.

6) Interoperability

The absence of standards between mHealth solutions and devices impedes innovation and economies of scale.

The European Commission eHealth Action Plan[18] proposes to achieve wider interoperability via:

- guidelines on a dataset for patient summary records to be exchanged across borders
- common measures for interoperable electronic identification and authentication
- enhance security of health information and eHealth services and interoperability of databases for medicinal products
- establish the semantic and technical cross-border interoperability specifications and assets
- propose an EU interoperability testing, quality labelling and certification framework for eHealth systems

Questions:

Q13: What, if anything, do you think should be done, in addition to the proposed eHealth Action Plan 2012-2020, in order to increase interoperability of mHealth solutions?

EHN: The EHN Position Paper on eHealth identified technical interoperability as the main challenge to the implementation of eHealth services. This is also the case for mobile health solutions, as for instance, patients will be able to bring their own device to be connected to the hospital network. Interoperability can only be achieved if common high-quality standards are established, so that patients all over the EU will benefit from the same data security, safety and quality.

Q14: 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?

EHN: Yes, healthcare professionals, patients and national healthcare services must be able to work with interoperable Electronic Health Records (EHRs). This is particularly crucial with nomad patients, who move from one hospital to another. Stakeholders should be consulted on how to ensure interoperability of mHealth applications with EHRs.

7) Reimbursement models

One existing model is based on reimbursement by institutional payers and national authorities, which decide whether mHealth can be included into the nomenclature of reimbursable healthcare activities. Users' role in bearing the costs of mHealth solutions needs careful assessment. As regards lifestyle

[18] European Commission eHealth Action Plan 2012-2020 Innovative healthcare for the 21st century, 07/12/2012.

and wellbeing apps, users often pay for their apps via app stores. Cases are also emerging where a partner can pay for these apps (e.g. a pharma company) in the context of an existing therapy.

Creating incentives for healthcare professionals to use mHealth solutions also requires reflection.

Questions

Q15: Which mHealth services are reimbursed in the EU Member States you operate in and to what extent?

EHN: No.

Q16: What good practice do you know of that supports refund of mHealth services (payer-reimbursement model, fee for a service model, other?) Please give evidence.

EHN: No.

8) Liability

Identifying potential liability arising from the use of a mHealth solution may be complex, because of the numerous actors involved: manufacturer, healthcare professional, internet provider, etc.

Damage to patient's health can come from: a defective device, a wrong diagnosis based on inaccurate data, an error by an IT specialist, the patient did not use the device correctly or sent the wrong data to the doctor.

Question:

Q17: 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?

EHN: Liability arising from the use of mobile health applications is very diverse.

The app developer is liable if it is proven that design, manufacturing or marketing is defective. If the patients' health status is damaged because of proven medical malpractice, then the liability of the healthcare professional who used the mHealth application could be engaged. Finally, if the patient him/herself misuses the mobile application, then his/her liability could also be engaged if his/her negligence is proven[19].

App developers (including manufactures, promoters, traders…) must be encouraged to use the highest quality standards when developing their apps, to minimize the risks of defects. Healthcare professionals should use mHealth applications very carefully and instruct their patients to strictly follow their advice, which includes using the app only as indicated, and not to change/delete data included in the application.

9) Research and Innovation in mHealth

There is a need to invest more in research and innovation in the field to support the development of more advanced and innovative mHealth solutions, while ensuring a high degree of efficacy and reliability as well as secure processing.

[19] mHealth, Legal and Regulatory Liability Issues, Presentation by Sarah Bailey, 18/04/14, http://prezi.com/svk20v2jqthv/mhealth-legal-regulatory-liability-issues/

Funding will continue under Horizon2020 prioritising mobile technologies and applications for integrated, sustainable, citizen-centred care.

Questions:

Q18: Could you provide specific topics for EU level research and innovation and deployment priorities for mHealth?

EHN: N/A.

Q19: How do you think satellite applications based on EU navigation systems can help the deployment of mHealth solutions?

EHN: Location data can be very useful in informing users on the availability and location of external defibrillators, emergency hospitals, 24/7 stroke units.

10) International cooperation

Economic disparity is reflected in the degree of mHealth uptake where higher-income countries show more mHealth activity than lower-income countries.

In this context, the WHO-ITU (International Telecommunication Union) joint agreement on mHealth[20] for non-communicable diseases intends to scale-up already approved mobile technology in some priority countries, at least one drawn from each geographical region.

Questions:

Q20: Which issues should be tackled in the context of international cooperation to increase mHealth deployment and how?

EHN: It is important that any international trade agreement should include provisions for high standards on safety of mobile applications.

Q21: Which good practices in other major markets could be implemented in the EU to boost mHealth deployment?

EHN: N/A.

11) Access of web entrepreneurs to the mHealth market

One of the conditions for the successful uptake of mHealth is the web entrepreneurs' capacity to enter this promising market, which is crucial to support the European ambition to becoming a front-runner in this field.

Questions:

Q22: Is it a problem for a web entrepreneur to access the mHealth market? If yes, what challenges do they face? How can these be tackled and by whom?

EHN: N/A.

[20] WHO ITU joint agreement on mHealth for NCDs, June 2013.

Q23: If needed, how could the Commission stimulate industry and entrepreneurs involvement in mHealth?

EHN: N/A.