Response of the German Medical Association

To the Green Paper on mobile Health ("mHealth") of the European Commission

Berlin, 3 July 2014

Bundesärztekammer
Herbert-Lewin-Platz 1
10623 Berlin

We are grateful for the opportunity to contribute our answers to the questions set out in the Green Paper, and thus towards the development of a suitable regulatory framework for mHealth in Europe. In addition to our responses to the questions, we would first like to share the general concerns of the German Medical Association (GMA) regarding this topic. We would particularly like to point out that, due to its fundamentally positive stance towards mHealth, the Green Paper neglects to address some of the wide-ranging implications of mHealth for patient safety and data protection:

- Suitable definitions of the various concepts relating to mHealth are lacking in the Green Paper. Within the framework of the current political focus upon mHealth, the GMA asks the Commission to contribute towards the creation of a uniform terminology. In particular, the differentiation between "lifestyle" applications, on the one hand, and applications with require the medical expertise of physicians, on the other, should, in our opinion, be more clearly defined. Applications which fulfil the objective criteria of a medical device must be subject to the same regulation and certification which apply to other medical devices.

- There should be more emphasis upon data protection. From our point of view, this Green Paper does not sufficiently take into account the full implications of data collection in the medical field. This applies particularly to the multiple use of data. We would refer in this respect to the results produced by the Working Party set up under Article 29 of Directive 95/46/EC, which has already conducted valuable work on this complex topic.

The GMA would also like to draw attention to the response submitted by the Standing Committee of European Doctors (CPME) to this public consultation, which highlights the crucial points that should be respected.

Questions:

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

There should be maximum transparency. App developers should be obliged to disclose fully which data are collected, where they are stored, how they are protected and by whom, and for what purpose and with what consequences for the end user they are processed. In terms of data minimisation and purpose limitation, the possibility that data generated by mHealth apps are processed despite the fact that the apps themselves would not require any such processing needs to be excluded. Also, discount scenarios with incentives for consumers to disclose data should be prohibited. End-users willing to use mHealth apps should have the right to refuse the disclosure of their data to third parties. Consent to data disclosure should not be a prerequisite for making use of mHealth apps. In addition, we would like to refer to Opinion 02/2013 on apps on smart devices by the Article 29 Data Protection Working Party (adopted on 27 February 2013), which highlights the governing rules and principles applicable in data protection terms.

• 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?

This is a task for the operating systems and programming frameworks of the relevant mobile platforms like android and iOS. They should support developers by adapting general programming tools so that by default:

- All data stored on a mobile device are encrypted (protection in case of theft of the mobile device)

- All data which are processed via a network are encrypted e.g. with TLS1.2

- The communication endpoints are authenticated

- Backups in the “cloud” are always encrypted with secure keys derived from the user password

In addition, we would like to refer to Opinion 02/2013 on apps on smart devices by the Article 29 Data Protection Working Party (adopted on 27 February 2013) which highlights the governing rules and principles applicable in data protection terms.

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

First and foremost, there needs to be a legal framework which provides clear rules on how data can be processed and used, thereby respecting and not weakening the governing rules and principles applicable in data protection terms (see Opinion 02/2013 on apps on smart devices by the Article 29 Data Protection Working Party) as well as the applicable ethical standards (e.g. informed consent - safeguarding the person’s right to self-determination and thus his/her autonomy). This is of utmost importance, specifically when it comes to the multiple use of health data. Provided ethical requirements are met and legal safeguards are in place, multiple use may be viable to improve patient care, prevention and/or public health in the context of medical research. However, this requires complex solutions with governance structures in place that include an approval process by an independent research ethics committee. The exploitation and misuse of personal and sensitive data for other purposes (e.g. commercial uses) need to be prevented in all cases.

Therefore, we suggest focussing on how to improve anonymisation and pseudonomisation techniques. Since effective anonymisation in a “big data” scenario is very difficult, research in this field, especially for big data analysis, should be promoted. One idea might be to strictly separate “data custodians” from “data users“.

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

Yes.

Why: Current legislation enforces the classification and certification of a medical device only when the manufacturer declares it to be a medical device. Outside the mHealth market this system works because physicians and hospitals are obliged to use certificated medical devices in patient care. However, this is a problem for apps as a declaration as a medical device is not mandatory even when an app, by objective criteria, would clearly fall into the scope of the Medical Device Directive. The app market is a low cost market. The target group of the app market consists mainly of consumers and not health professionals. Consumers have no obligation to use certified medical devices for medical purposes. As a result, medical apps are usually not certified and can pose a risk to patient safety. App manufacturers often argue that a specific app is not intended for medical use but only for learning or entertainment.

How: Legislation (e.g. the Medical Device Directive, MDD) should be adapted so that apps which fall into the scope of the MDD must be certified and regulated even though the manufacturer/developer of the app does not declare them to be medical devices.

Legislation should be adapted so that:

- mHealth apps providing medical information should disclose the identity, professional qualifications and conflicts of interest of the source of this information.

- mHealth apps must provide a privacy statement informing consumers about which personal/medical data will be collected, transmitted or stored outside the mobile device and how these data are protected. In this respect we refer to the results produced by the Working Party set up under Article 29 of Directive 95/46/EC.

- mHealth apps must ask for permission before they transmit personal/medical data to third parties. Consent for data disclosure should not be a prerequisite for using a mHealth app. In this respect we refer to the results produced by the Working Party set up under Article 29 of Directive 95/46/EC.

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

To our knowledge there are no established good practices to better inform end-users about mHealth apps. An approach similar to the HONcode (Health on Net Foundation) could possibly be appropriate.

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

If apps are to be used or even prescribed in patient care then the efficacy should be proved as with other medical devices, e.g. by means of randomised controlled trials.

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

When patient health could be at risk, regulation is needed, e.g. as a medical device. For apps providing medical information, there should be mandatory disclosure of the identity, professional qualifications and conflicts of interest of the source of the information.

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

There are reports of some successful mHealth projects in patient care. To our knowledge there is no strong evidence yet on the uptake of mHealth solutions in European healthcare systems.

• 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)?

To our knowledge, good practices with strong evidence for raising the quality of patient care do not yet exist.

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

No.

• 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?

We would recommend that healthcare professionals use mHealth solutions that are certified – in terms of patient safety and efficacy - by a trustworthy and independent organisation. For mHealth solutions providing medical information, they should consider checking the professional qualifications and reputation of the source of the information, as they would do with a scientific publication.

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

Research and innovation should be promoted in the following areas:

- Privacy, pseudonymisation and anonymisation in big data settings

- Information security for mobile applications

- mHealth and patient safety
- Best practices for mHealth services
- Cost-benefit analysis of mHealth apps

• 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?

The large amount of eHealth apps suggests that there are no barriers to access the mHealth market.