CPME/AD/EC/05062014/052_Final/EN

On 5 June 2014, the CPME Executive Committee adopted the 'CPME response to the public consultation of the European Commission on the mHealth Green Paper - COM(2014)219 final' (CPME 2014/052 FINAL)

CPME response to the public consultation of the European Commission on the mHealth Green Paper - COM(2014)219 final

The Standing Committee of European Doctors (CPME) represents national medical associations across Europe. We are committed to contributing the medical profession's point of view to EU and European policy-making through pro-active cooperation on a wide range of health and healthcare related issues.[1]

[1] CPME is registered in the Transparency Register with the ID number 9276943405-41.
More information about CPME's activities can be found under www.cpme.eu

CPME welcomes the opportunity to comment on the green paper on mobile Health ("mHealth") and to provide the European physicians' perspective through the open public consultation.
CPME previously commented on the eHealth Action Plan proposed by the Commission (CPME 2013/017).

CPME believes that mHealth applications can be valuable additional tools to the provision of care. For instance, mHealth may support patients' empowerment and motivation, facilitate contacts between physicians and patients living in remote areas, improve the quality of the health service delivery, as well as its efficiency.
To reach this aim, mHealth applications would however need to be carefully regulated and subject to detailed efficacy and safety tests.

Building upon our previous positions related to eHealth, we would like to highlight the following points:

- Legal gap

Legal uncertainty at EU level with regard to mHealth applications is of concern. It is duly acknowledged that some mobile applications are to be considered as medical devices under Directive 93/42/EEC, as in vitro diagnostic medical devices under Directive 98/79/EC or as Radio Equipment and Telecommunications Terminal Equipment (RTTE) under Directive 1999/5/EC. Subsequently, mobile applications fulfilling the criteria to qualify as medical devices will also fall under the applying Regulations when adopted. This still does not clarify what is the applicable legal framework for those applications which do not fall under the scope of these instruments. The delimitation between medical device applications and wellness/well-being applications should be legally specified. With this purpose and for future reference, we refer to the CPME Statement on Medical Devices and In Vitro Diagnostic Medical Devices, specifying criteria for safety, ethics and clinical evidence for all applications qualifying as medical devices (CPME 2012/150 FINAL).

- Quality and reliability of mHealth applications

Due to this legal vacuum, several wellbeing applications are being developed and used without the necessary scientific basis and control. For instance, some applications propose self-diagnosis solutions, whereby the user after introducing his symptoms in the application is provided with a diagnosis. The legal vacuum and the absence of control from which this type of applications benefit, raise serious concerns about their reliability and impact on patient safety. While certain mHealth applications may indeed be of true benefit to patients, there is an urgent need to ensure sufficient quality and safety safeguards, for instance through certification mechanisms. CPME believes that mHealth applications should in no way lead to putting patient safety at risk. It must also be clear to the user that, mHealth applications are not to replace face-to-face medical consultations with a physician.

- Approval and quality certification processes

In order to ensure sufficient reliability and safety of applications, an approval process in the form of a certification mechanism should be envisaged. mHealth applications should undergo a strict scientific review process based on generally accepted evaluation criteria and led by healthcare professionals. Allowing this type of certification process would ensure these applications can be trusted by end-users. In the Netherlands for instance, the "Aarts en Apps" project has been set up by which applications are being reviewed and evaluated[2]. The HON label for online health information used in Switzerland is another good example[3].

- Remaining legal uncertainties

In addition to safety and reliability guarantees, physicians willing to use mHealth applications, would be expecting that the medical service they provide is legally viable. Similarly to general eHealth services, it is presumed that physicians might be reluctant to use such applications if liability provisions are not clarified from the start. The remuneration of services provided by physicians outside the usual consultation framework, ie. with support of mHealth tools, would also need to be addressed. This is particularly true in a cross-border situation.

- Data protection

Most of the data stored through mHealth applications contain individual health information. These data are therefore highly sensitive and require adequate security features. The NSA scandal whereby United States' authorities have been accessing EU citizens' data and notably individual health data, has shown how crucial it is to ensure strict data protection safeguards[4].

CPME believes it is of utmost importance that health data stored electronically through mHealth applications should be protected against any attempt of unauthorised third parties to access it. Individuals who trustfully enter their personal health information in an mHealth application expect that this information will be kept confidential and not be shared with any unauthorised entity. Especially, CPME firmly insists that any further use of these data, for instance by insurers or employers, should be strictly forbidden.

Furthermore, it is crucial that patients, when using mHealth applications, are well aware of how and when the data may be used. The providers of mHealth applications should be obliged to declare if the data is shared with third parties, in which circumstances, how securely the data is stored and if it is anonymized. This information should not be hidden in fine print but should be easily available to the patient. One possibility could be to set up ethical criteria and to black-list (or white-list) mHealth applications if they do not fulfill (or fulfill) these ethical criteria.

[2] http://www.artsennet.nl/Kennisbank/Medische-apps.htm

[3] http://www.hon.ch/home1.html

[4] Please see the CPME Open letter on PRISM and the CPME Statement on the draft report of MEP Claude Moraes on electronic mass surveillance and the subsequent amendments (CPME 2014/009).

- Electronic Health Records

CPME believes individual health information obtained through mHealth applications may be of some added value to personal health records, ie. Electronic Health Records. This may indeed provide physicians with useful additional information for diagnostic and treatment purposes. However, one should ensure that only clinically relevant and quality information is included in the health record. The systematic collection of all the data generated through mHealth should be avoided. Instead, the data should be carefully selected through quality criteria.

- "Big data"

Finally, CPME believes that the new potentials for research envisaged with the collection of "big data", notably through mHealth applications, should not result in the weakening of currently applicable ethical standards. As such, informed consent is the backbone principle ensuring that research is conducted in an ethically acceptable way. With regard to the participation in research, every patient has the right to decide for him/herself, in a voluntary way and free from any undue influence. To consciously decide on whether or not he/she wants to take part in a research study, the patient needs to be fully informed of the foreseen risks and benefits of the study, but also of his/her rights as well as possible alternatives. The ethical conduct of medical research is based on the premise that informed consent is fully respected. Only when consent cannot be collected due to the fact that it would prove impractical or even damageable to the research study, can derogations be envisaged. In this case a governance structure that includes an approval process by an independent research ethics committee should be in place.