CPME/AD/Board/31102015/095_Final/EN

On 31 October 2015, the CPME Board adopted the 'CPME Policy on mobile health' (CPME 2015/095 FINAL)

CPME Policy on mobile health

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].

Mobile health (mHealth) is defined by the World Health Organisation (WHO) as the "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices. mHealth involves the use and capitalization on a mobile phone's core utility of voice and short messaging service (SMS) as well as more complex functionalities and applications including general packet radio service (GPRS), third and fourth generation mobile telecommunications (3G and 4G systems), global positioning system (GPS), and Bluetooth technology."[2]

mHealth covers a wide variety of services, such as services provided by diet, sleep or fitness apps; or services provided by mobile medical devices used in patient care by a doctor or by a patient to monitor his/her condition. The delimitation between apps having a sole wellbeing/lifestyle purpose and apps having a medical purpose is often blurred. For instance, sleep and diet data used in wellbeing/lifestyle apps may very well be medically relevant.

mHealth constitutes a growing innovative market, as this has been highlighted in the European Commission's green paper on mobile health[3]. CPME acknowledges that mHealth may be a valuable

[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
[2] WHO report « mHealth – New horizons for health through mobile technologies, Global Observatory for eHealth series – Volume 3", 2011, p. 6
[3] European Commission Green Paper on mobile health (mHealth), COM (2014)219final, p. 6

tool in healthcare and may help promote a healthy society, eg. by fostering patient empowerment, helping people living with a chronic condition to share data with their doctor, facilitating access to medical assistance in sparsely populated areas, or even by facilitating contacts between doctors themselves and other healthcare professionals. One should however not disregard potential risks entailed by the use of these technologies.

CPME recommendations:

1. When using mHealth applications, users should be cautious and aware that not all of them are reliable and safe to use.
2. mHealth services may be only a complementary tool to patient care; they cannot and must not fully replace medical face-to-face consultations with a doctor. mHealth services may only be used in conjunction with medical face-to-face consultations.
3. A clear regulatory framework should be in place at European level, in order to delimitate mHealth services which have a medical purpose from those services having a sole wellbeing purpose.
4. mHealth apps having a medical purpose should be regulated in the same way as medical devices by Health authorities. mHealth services which do not qualify as medical devices, ie. wellbeing/lifestyle apps, should nevertheless undergo independent assessment before entering the market.
5. Doctors' liability when using mHealth services should be clarified. Doctors and patients would expect that the medical service they provide and receive through mHealth is legally viable.
6. Data privacy should be strictly protected. Although the data used in mHealth are not always 'health data' by nature – such as lifestyle or physical data – they may reveal information about the health status of the individual, ie. provide sensitive personal information and therefore be medically relevant. When defining the concept of 'health data', it is not simply the nature of the data but what the data is being used for that should be considered (purpose of use).
7. Privacy principles should be embedded in the design and architecture of mHealth apps already during the conception phase, in order to prevent any privacy invasive events to occur. mHealth app developers must inform the users of the character of the application (medical, lifestyle, wellbeing), of what their data will be used for, for how long, and how securely they are stored. Users must be duly informed and give their prior consent thereto. This information should not be hidden in fine print, but should be easily accessible. Re-use of data by any secondary entities without informed consent, eg. by insurers or employers, should be strictly forbidden.
8. The integration of data generated by mHealth apps in medical records, may help improve care. It is therefore all the more important to ensure qualitative, reliable, useful and clinically relevant data is collected. The use of the data should be medically proper and ethically sound.