PURPOSE: For decision
CONCERNING: mHealth / data privacy
AUTHOR: CPME Secretariat / CC

CPME NUMBER: **CPME 2015/121 FINAL**
DATE: 8 December 2015

CPME Comments to the Draft Code of Conduct on privacy for mobile health applications

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].

CPME welcomes the opportunity to comment on the Draft Code of Conduct on privacy for mobile health applications.

As much as we do acknowledge that the Code of Conduct is mainly addressed to mHealth application developers and focuses on providing guidance as to how the EU Data protection regime applies to mHealth, we regret that only industry was involved in the drafting process and that other stakeholders, representing the main end-users of mHealth applications, have not been comprehensively included. We indeed believe that when such guidance documents - which are expected to have significant influence on the way data privacy is being conceptualized and managed by app developers - are drafted, the end-users of these apps such as Doctors should be given the possibility and the means to share their expertise in a meaningful way.

Doctors are bound by medical confidentiality[2]. Patient privacy is a fundamental principle of medical practice and is at the core of a trustful patient-doctor relationship. An important amount of mHealth apps are used and will presumably be used in the future by Doctors. Should doctors fear that data breaches may occur or that patient privacy is not fully guaranteed, they might simply refuse to use these apps and advise their patients not to use them. Doctors would not be willing to jeopardize their obligation to medical confidentiality, nor to threaten the trust relationship they have built with their patients. The Code of Conduct should also take this approach into consideration and therefore explicitly embrace the fundamental principles of medical confidentiality and patient privacy.

In general, we would recommend that for each assertion or statement of the draft Code of Conduct, a reference is made to the EU legal applicable framework.

---

[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] On 31 October 2015, the CPME Board adopted the ' CPME Statement on medical confidentiality' (CPME 2015/074 FINAL)

PURPOSE: For decision
CONCERNING: mHealth / data privacy
AUTHOR: CPME Secretariat / CC

CPME NUMBER: **CPME 2015/121 FINAL**
DATE: 8 December 2015

Further to the above general comments, CPME would like to make specific comments on the content of the draft Code of Conduct itself:

1. Definition of "data concerning health" (See section '2. Purpose', p. 1 onwards)

- The approach taken in the draft Code of Conduct on the definition of "data concerning health" is in line with the CPME's approach. We therefore invite the drafting team to reference the CPME policy on mobile health in the Code of Conduct: CPME 2015/095 FINAL. In the context of mHealth, "data concerning health" should be envisaged broadly so as to encompass not only the nature of the data, but also the purpose for which it is intended to be used. 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).

- We would advise the drafting team to reference in the paper, the European Court of Justice (ECJ) jurisprudence on the definition of "data concerning health". In particular the Lindqvist case (C-101/01, Slg. 2003, I-12971, No. 50) states that "(i)n the light of the purpose of the directive [95/46/EC], the expression 'data concerning health' used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual."

- The draft Code of Conduct alludes to the sensitivity of "data concerning health" (see §4, p. 2), but does not sufficiently explain the reason why this category of data is considered sensitive. CPME would recommend to further substantiate this assertion, by referring to the need to higher protection schemes for data which concerns one of the most intimate part of our lives: our health.

2. Adherence to the Code and governance structure

In order to ensure that the Code of Conduct is a reliable and credible tool, a robust, transparent and independent control mechanism should be in place. This would allow end-users of mHealth apps, such as doctors, to be confident in the apps they wish to use. Should a company not comply with the Code of Conduct it has adhered to in the first place, a mechanism should be in place to inform the end-users that there was a breach in the adherence to the Code of Conduct. This company should at the least incur a withdrawal of its certification; stricter sanctions could also be envisaged, in line with the EU data protection regime.

Without this robust, transparent and independent control mechanism, a disproportionate burden would be placed on end-users who would bear all the risks by not knowing if the app developer effectively complies with data privacy law. Data Protection Authorities (DPAs) or the European Data Protection Supervisor (EDPS) created by the General Data Protection Regulation could act as the control body. We strongly support the installation of appropriate control mechanisms in order to detect possible breaches in the adherence to the code of conduct. This could e.g. be implemented by a kind of "journal" or "log file" which lists all accesses to the app. Also, any residual data no longer needed remaining in the app must be avoided in order to prevent data waste accumulation.

3. Consent provisions

A reference to the possibility for data subjects to withdraw their consent should be inserted in the section "How should I obtain the consent of the users of my app?" (see § II. 1. p.5).

4. Secondary purposes and 'big data'

In medical research, the use of data for secondary purposes is subject to approval by independent research ethics committees and other independent review boards entitled to oversee such processes. The draft Code of Conduct (see § II. 7), p. 11) should refer to these competent bodies. Further insight on the use of data for secondary research purposes and big data can be sought in the CPME response to Commission's public consultation on the mHealth green paper (CPME 052/2014 Final)