



---

On 7 September 2017, the CPME Executive Committee adopted the 'CPME statement on the Commission proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) - 2017/0003(COD)' (CPME 2017/064 FINAL)

---

**CPME statement on the Commission proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) - 2017/0003(COD)**

*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<sup>1</sup>.*

In the context of the negotiations on the Regulation on Privacy and Electronic Communications (ePrivacy Regulation) in the European Parliament and Council, CPME would like to draw attention to the impact of this regulation on medical confidentiality and health data privacy.

'Data concerning health', are defined as "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*" in the General Data Protection Regulation (GDPR). These are particularly sensitive data and therefore must be afforded the highest possible level of protection.

**Communication in health is sensitive**

With the growing digitalization of healthcare, doctors and patients increasingly communicate electronically. These communications contain sensitive information regarding patients' health. Considering that the patient-doctor relationship is built on the premise of confidentiality and trust, it is of utmost importance to guarantee the confidentiality and security of these electronic communications.

Patients' data may also be stored in the cloud. Consequently, the same level of confidentiality and security has to be guaranteed, as emphasized by the European Data Protection Supervisor (EDPS) in his opinion 6/2017.

---

<sup>1</sup> 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](http://www.cpme.eu)



### Metadata may reveal medical issues

In addition to the content of communications, metadata - which include data on the location of the device or the date and time of the communication - can reveal medical issues. As underlined by the EDPS, *“It has also been shown that intimate details about a person’s lifestyle and beliefs, such as political leanings and associations, medical issues, sexual orientation or habits of religious worship can be discovered through mobile phone traffic data.”* Therefore, both communications content and metadata deserve the same level of protection (Article 6).

However, the EDPS underlines that *“Despite its ambition to provide a high level of protection for metadata, the Proposal nevertheless allows its processing subject to less stringent safeguards.”*

### Connected devices can be health sensitive

Finally, personal health information can also be revealed by connected devices. While connected devices are also included in the scope of this Regulation - under the notion of ‘terminal equipment -, the provisions regarding the tracking of the location of terminal equipment do not comply with the GDPR requirements, in particular the principle of ‘privacy by default’. Again, the draft regulation does not ensure the same level of protection (Article 8).

In this respect, the EDPS noted that *“[Users] may not authorise that their medical or fitness tracker communicate their medical or fitness information to any and all devices designed to capture and process this information. With increased availability of IoT devices, including medical devices, often the mere fact whether one is wearing or not a particular device can be indicative of very sensitive, for example, health information, and therefore caution is needed.”* Consequently, it is recommended to amend the provisions in order to ensure that devices are not tracked without their users’ consent, as recommended by the EPDS and Article 29 Working Party.

In conclusion, **CPME calls on European legislators to take into account the recommendations of the EDPS and Article 29 Working Party** on the above issues to ensure at least an equal level of protection than the GDPR for personal data concerning health.