CPME/AD/EC/14012011/158_Final/EN

On 14 January 2011, the CPME Executive Committee adopted the "CPME response to Public Consultation on the Commission's comprehensive approach on personal data protection in the European Union " (CPME 2010/158 Final EN)

CPME[1] response to the

Public Consultation on the Commission's comprehensive approach on personal data protection in the European Union

The Standing Committee of European Doctors (CPME) aims to promote the highest standards of medical training and medical practice in order to achieve the highest quality of health care for all patients in Europe.

CPME is also concerned with the promotion of public health, the relationship between patients and doctors and the free movement of doctors within the European Union.

CPME represents the National Medical Associations of 27 countries in Europe and works closely with the National Medical Associations of countries that have applied for EU membership as well as specialized European medical associations.

CPME welcomes the opportunity to reply to the Consultation on the Commission's comprehensive approach on personal data protection in the European Union and to present the position of doctors on the action points identified by the Commission.

CPME agrees that in light of technological developments and the increasing transfer of patient-identifiable information in cross-border care, the issue of data protection in the field of healthcare gains new relevance and dimensions. CPME therefore welcomes the Commission's objective to ensure a coherent application of data protection rules, especially with regard to the impact of new technologies.

Generally, CPME notes and supports the twin overarching aims set out in the introduction. However, in relation to the second of these - the "free flow of personal information" in support of the internal market - it must be emphasised that the "free flow" of patient-identifiable data in support of the healthcare and other markets (such as pharmaceutical regulation, research and public health monitoring) must take place within a legal and ethical framework. If this is not done, patient confidence will be eroded, and along with it the market potential from wider information transfers.

In addition, although the "Digital Agenda" is mentioned, almost in passing, in the consultation document, the fact that the Communication from the Commission on 'A comprehensive approach on personal data protection in the European Union' document makes a priority of allowing patients access to their medical records, the legal and ethical considerations in this (such as access to genetic data, "third party" information, and the right to have records amended) all need addressing.

CPME noted that there is some conflict in the consultation document's focus on strengthening data control measures at national level, while also seeking a legal framework at European level. The document acknowledges that authorities at member state level have interpreted the existing directive in different ways, so it without much doubt that consistency between them is desirable.

[1] CPME is registered to the European Commission's Register of Interest representatives with the identification number 9276943405-41.

Rue Guimard, 15 - B-1040 Brussels - Belgium
Tel. : +32 (0)2 732 72 02 - Fax : +32 (0)2 732 73 44 - E-mail : secretariat@cpme.eu - Web : http://www.cpme.eu

The fundamental doctor-patient relationship is built on the premise of confidentiality and trust. All data contained in medical records (written and electronic) should therefore be considered to be sensitive personal data and must be afforded the highest possible level of protection in order to ensure that these key principles are upheld. CPME supports the Commission's plans to review the categorisation of 'sensitive data' so as to include genetic data, which should enjoy the best possible protection especially with regard to parties outside the health services. Genetic data is especially problematic, since information about one individual has direct relevance for others. CPME would support a separate review of the concept of "ownership" of such data.

Patient data should be stored securely and protected from unauthorised access, which is especially relevant for data stored electronically. This includes limiting access to patient data to the healthcare professionals involved in their care and the scope of data necessary to their treatment. Furthermore, technologies for processing patient data should provide for the possibility to trace access attempts and track corrections made to the patient records, by providing a clear data trail. Insufficient or insufficiently enforced authorisation mechanisms carry the danger that safeguards are circumvented and patient data becomes accessible arbitrarily, thus violating the premise of patient-doctor confidentiality and also patients' rights derived from European and international law, e.g. Art. 8 of the Charter of Fundamental Rights as well as Art. 8 of the European Convention on Human Rights and Fundamental Freedoms and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. A recent situation in Belgium has lead to the matter being brought to the attention of the European Court of Human Rights.

A significant problem, in relation to patient data, is a strong variation in approach to consent. CPME believes that implied (verbal) consent is required for the collecting and sharing of patient information in support of immediate healthcare, but also believes that a higher level of consent is needed for secondary use of data, including financial and clinical audit, and research. Much of these concerns can be addressed if such data is fully anonymised. CPME welcomes the Commission's commitment to enhance legal certainty as to patients' rights to access and amend their data. In the framework of electronically processed data, CPME encourages that a data collector should not be allowed to use any data without the data subject having online access to the same data, to the access log of people using this data and to the particular rules regulating access to this particular data. Any exception from this general rule should be explicit and agreed upon by the data subject or his or her substitute.
In addition, patients should have the option of restricting access to highly sensitive data to a limited number of healthcare professionals.

CPME supports the Commission's plans to enhance the legal provisions to sanction the accessing and processing of patient data by unauthorised parties including non-medical entities such as insurances or public authorities. Such sanctions should be directed at data holders and processors, with clear and uniform penalties across member states.

In the context of the provision of cross-border healthcare, as currently discussed in the context of the legislative proposal COM/2008/414/FINAL on patients' rights in cross-border healthcare, the implications for the security of patient data reach a new dimension. A particular problem for doctors involved in transferring data from one jurisdiction to another is a lack of knowledge about how that data will be handles upon reception. Greater clarity and harmonisation will assist the taking of valid consent for the transfer. CPME reaffirms its position on the need to provide for interoperable and secure systems of data transfer between Member States to maintain medical confidentiality and patient safety. In cases of cross-border transfer of information it is of utmost importance to ensure that patients' have full information and legal certainty as to their rights and have given their explicit consent to the transfer and processing of their data.

When viewing the cross-border transfer of data against the background of cloud-computing technologies[2] it is important to note that while these technologies may assist patient access to

[2] , i.e. location independent computing, whereby shared servers provide software, resources and data to computers and other devices on demand. The principle concept of cloud computing is that the computing i.e. the processing (and the related data) is not in a specified, known or static place(s) known as 'the cloud'. Generally, cloud computing customers do not own the physical infrastructure, instead avoiding capital expenditure by renting usage from a third-party provider. The consumer bears no costs beyond the payment for resources that are actually used.

Rue Guimard, 15 - B-1040 Brussels - Belgium
Tel. : +32 (0)2 732 72 02 - Fax : +32 (0)2 732 73 44 - E-mail : secretariat@cpme.eu - Web : http://www.cpme.eu

relevant information, cloud-computing also implies wider issues of privacy, e.g. by requiring attention to adequate firewalls. Furthermore it raises questions as to data ownership and the protection of standards in cases of data export to third countries. While the advantages of cloud-computing are obvious, any revision of the personal data protection in the European Union should take into account the impact of these technologies on data privacy in a timely manner.

The CPME is prepared to further provide its expertise in this consultation and in future discussions on the issue of personal data protection in the European Union.

Rue Guimard, 15 - B-1040 Brussels - Belgium
Tel. : +32 (0)2 732 72 02 - Fax : +32 (0)2 732 73 44 - E-mail : secretariat@cpme.eu - Web : http://www.cpme.eu