CPME/AD/EC/07052020/048_Final/EN

On 7 May 2020, the CPME Executive Committee adopted the 'CPME response to EUHEalthSupport Consortium on health data processing' (CPME 2020/048 FINAL).

CPME response to EUHEalthSupport Consortium on health data processing

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 institutions and European policy-making through pro-active cooperation on a wide range of health and healthcare related issues. [1]

I – Introduction

CPME welcomes the work being developed by the EUHealthSupport Consortium[2] to conduct a study which examines EU Member States' rules governing the processing of health data, with the objective of highlighting possible differences and identifying elements that might affect the cross-border exchange of health data in the EU. The processing of health data at national level is characterised by many derogations to the General Data Protection Regulation.

CPME further welcomes the consultation of stakeholders, together with representatives of national Ministries, in particular the expert workshop organised on 16 March 2020 to discuss European rules on the processing and further compatible processing of health data, on health data governance models and databases, on patients' control over their own data, on codes of conduct on the secondary use of health data and on the European Health Data Space.

II – General observations

CPME believes that a high level protection of all citizens' personal data is essential, in particular 'data concerning health' as it may reveal the most intimate and private information of individuals. Patient-doctor relationship is built on confidence and trust, from the beginning, and should not be undermined against the need to increase data exchange or sharing for health research purposes and innovation.

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

[2] The Consortium was awarded the contract 'Chafea/2018/Health/03 – A Single Framework Contract for the provision of support services for managing expert groups in the field of (public) health' by the Consumers, Health, Agriculture and Food Executive Agency (Chafea), <https://www.euhealthsupport.eu/>, accessed on 21 April 2020.

Physicians are bound by ethical and professional obligations, including confidentiality, having an obligation to remain silent about any personal data entrusted to them in their professional capacity. Therefore, data security, privacy and medical confidentiality need to be ensured, *inter alia*, when collecting, recording, storing, consulting, using, disclosing by transmission or even when destroying health data.

III – Observations on the primary use of health data[3]

CPME considers as best practice for the primary use of 'data concerning health' obtaining patient's consent. The context and purposes in which health data is initially collected – health and social care environment for preventive medicine, diagnosis or treatment –, implies following strict ethical and legal considerations from physicians. Only with consent can physicians ensure full transparency and confirm if it was intelligible to the patient while fostering and nurturing doctor-patient relationship. Consent to be lawful needs to be freely given, specific, informed, unambiguous and made by a statement or a 'clear affirmative action' [Articles 4 (11), 6 (1) (a), 7 and 9 (2) (a) of the General Data Protection Regulation, hereinafter 'GDPR'].

Entities having access to such data, either private or public, to provide care across borders need to demonstrate compliance with the minimum safeguards and principles provided for by the General Data Protection Regulation.

On the use of apps and wearable devices, CPME believes that 'data concerning health' generated by such applications and devices should be kept confidential and not be shared with unauthorised entities, in particular corporate providers and/or employers. Patients need to be aware of who, how, what, when and where the data is being used. Experience shows that data-sharing practices have not been transparent and patients are not fully aware of its implications.[4]

As far as the use of electronic health records (EHR) is concerned, experience shows that it can include additional information about patients that may not be appropriate or related to the provision of care,

[3] For the purposes of this document, 'primary use of health data' is understood as *"health data collected directly from a patient in the context of health and social care provision for the purpose of providing health or care services to that patient. Such data may need to be shared across EU borders in the case of patients receiving care in a Member State other than their usual Member State of residence. (…) It includes in-person care as well as telecare using eHealth or mHealth solutions."* – definition provided by the EUHealthSupport Consortium at the 16 March Workshop.

[4] Huckvale, Kit, John Torous, and Mark E. Larsen. "Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation." JAMA network open 2, no. 4 (2019): e192542-e192542, < https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782>, accessed 22 April 2020. This study analysed 36 top-ranked apps for depression and smoking cessation available in public app stores, where 29 transmitted data to services provided by Facebook or Google, but only 12 accurately disclosed this in a privacy policy. Many privacy policies were indeed inaccurate or out-of-date. Critical evaluation and technical scrutiny shown to be essential for informed decision making by consumers and health care professionals wishing to use health apps.

for example economic irregularities to the insurance fund. In relation to the integration of health apps into EHR, experience reveals that cross referencing information with other data increases, thus revealing the state of health or health risks.

IV – Observations on the secondary use of health data for research purposes[5]

CPME considers important to foster trust in the sharing of health data for research purposes. When consent is the legal basis used to process personal data, consent should be equally provided for further processing for research purposes. The data subject needs to be made aware before the research activity takes place.

There may be exceptional circumstances where consent cannot be obtained or involves a disproportionate effort, and anonymisation cannot be achieved without undermining the quality of the research, then ethically sound governance is required. **In particular, there should be involvement of independent research ethics committees and other independent review boards entitled to oversee such processes.** Furthermore, data protection impact assessments should be carried out. It is also important to regularly verify whether consent withdrawal is effective and, following up on the recent guidelines issued by the European Data Protection Board, whether there is a power imbalance that could pressure or disadvantage a reluctant patient to share his/her data.[6]

Concerning patient information, experience shows that patients are more receptive to give their consent on the use of health data for research purpose, if the explanation (to obtain consent) for processing such data comes from a person they trust or have some sort of relationship.

Due to the numerous derogations across Europe, in particular on the exercise of data subject rights, CPME supports the development of a EU Code of Conduct for secondary use of health research data,

[5] For the purposes of this document, 'secondary use of health data for research purposes' is understood *as "re-use of health data that were collected initially in the context of providing care, for scientific or historical research by both public and private sector organisations including the pharmaceutical and medical technology industries and insurance providers. (…) re-use of health data that were collected initially in the context of providing care, for scientific or historical research by both public and private sector organisations including the pharmaceutical and medical technology industries and insurance providers."* - definition provided by the EUHealthSupport Consortium at the 16 March Workshop.

[6] European Data protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 21 April 2020, <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en>, accessed 23 April 2020.

advocating the need to embed the principles of the Helsinki[7] and Taipei[8] and declarations, adopted by the World Medical Association (WMA), in such a code.

The transmission of health data has to be confidential, secure and purpose-related. The absolute respect of medical confidentiality is of utmost importance. When using a research platform or adopting a specific data governance structure, the minimum safeguards of Article 89(1) of the GDPR must be provided for, while also respecting the principles of integrity, data protection by design and by default, and an appropriate level of security pursuant to Article 32 (1) of the GDPR. In particular, the transmission of health data must rely on:

i. secure and encrypted paths of transmission,
ii. mechanisms for acknowledging message reception and reading so that the sender can be sure the transmission is successful,
iii. logging procedures,
iv. trustworthy identification and authentication procedures,

The use of non-disclosure agreements amongst researchers to ensure confidentiality should also be supported and facilitated.

V – Observations on the secondary use of health data for wider public health purposes

The same observations in point IV are valid, *mutatis mutandis*, for point V.

***

[7] WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects, adopted by the 18th WMA General Assembly, Helsinki, Finland, June 1964 and as amended by the 64th WMA General Assembly, Fortaleza, Brazil, October 2013.
[8] WMA Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks, adopted by the 53rd WMA General Assembly, Washington, DC, USA, October 2002 and revised by the 67th WMA General Assembly, Taipei, Taiwan, October 2016.