On 20 March 2021, the CPME Board adopted the 'CPME Policy on the European Health Data Space - Focus on Health Research and Policy Making' (CPME 2021/097 FINAL).

CPME Policy on the European Health Data Space - Focus on Health Research and Policy Making -

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.

Policy Summary

Sharing patient data needs to go along with strong legal safeguards and security. Governance structures and transparency are essential to supervise the use and re-use of data. To foster trust in the sharing, there should be the involvement of research ethics committees or ethics review boards when the legal base to share patient data is other than consent of the data subject. The default position for sharing patient data for other purposes than primary care should be irreversible anonymisation, which should be legally guaranteed. Encryption should be the pseudonymisation technique when anonymisation cannot be fulfilled. High encryption standards should be adopted. Clear legal definitions on new concepts should be included in the European health data space legal framework.

Introduction

The European Commission's communication on a 'European strategy for data'[1] aims at creating a single market for data, where data flows between Member States and sectors, where clear rules on data governance, data access and data use exist, and where data is available respecting European values and rules.[2] The communication foresees developing common European data spaces in strategic economic sectors and domains of public interest, such as the common European health data space (EHDS). The strategy is part of a wider package of strategic documents, including the European Commission's communication on Shaping Europe's digital future[3] and a White Paper on Artificial Intelligence – A European approach to excellence and trust.[4]

[1] COM(2020) 66 final, 1-35.
[2] European Commission, Inception Impact Assessment on a Legislative framework for the governance of common European data spaces, 3 July 2020, <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Legislative-framework-for-the-governance-of-common-European-data-spaces>, last accessed 3 August 2020.
[3] COM(2020)67 final, 1-16.
[4] COM(2020)65 final, 1-27.

Rue Guimard 15 (4th Floor) - 1040 Brussels - Belgium
Tel.: +32 (0)2 732 72 02 - Fax: +32 (0)2 732 73 44 - E-mail: secretariat@cpme.eu - Web: www.cpme.eu
Company registration number: 0462509658 - Transparency register number: 9276943405-41

The preparatory work conducted by the European Commission included a study on the processing of patient data across the EU[5] to which CPME participated as a consulted stakeholder.[6] The European Commission collaborates with Member States as these are supported by the 'Joint Action for the European Health Data Space'.[7]

CPME welcomes the development of the EHDS to boost research and innovation for the 'public good'.

European Health Data Space (EHDS)

1. Functionalities

A common European Health Data Space (EHDS) is meant to "promote better exchange and access to different types of health data (e.g. electronic health records, genomics data, data from patient registries)".[8] The Space will work in two ways:

- to support healthcare delivery by strengthening citizens' access to health data and portability of these data, and to tackle barriers to cross-border provision of digital health services and products (so-called primary use of data), and
- for health research with the development of new treatments, medicines, medical devices and services and for health policy making purposes (so-called secondary use of data).[9]

2. Purpose

In its European strategy for data, the Commission announced the need to have more data available for the 'public good' and that the development of the EHDS is in the 'public interest'. The EHDS is meant to boost research and innovation for the 'public good'/ or in the 'public interest'. However, the public good/interest is volatile and up to interpretation. To consider boosting innovation and research 'in the public interest or for the public good' as a legitimate purpose of the space (which a priori it is), clear legal criteria are needed to 'fill up' the meaning and to avoid misuse.[10] For instance, it is in the public interest to respond to 'unmet medical need' as we wish to end suffering. The term 'unmet medical need' is currently misused to justify pharma innovation in profitable areas that are not necessarily neglected/unmet, while AMR or dementia remain largely unaddressed. It is an example of 'innovation' not being in the public interest but in the industry's interest.

3. Governance framework

As the implementation of the process is still unknown, CPME highlights the need for a robust governance framework for data access and data use, along with strong safeguards and enforcement mechanisms for data subject rights. Moreover, data controllers and joint data controllers have to be

[5] The study was conducted by the EUHealthSupport Consortium and also aimed at understanding how national regimes could affect the cross-border exchange of health data in the EU. The final report - Assessment of the EU Member States' rules on health data in the light of GDPR - was published on 12 February 2021.

[6] CPME contributed to the EUHealthSupport consortium study with CPME response to EUHealthSupport Consortium on health data processing (May 2020) and CPME response to the EUHealthSupport Consortium on Stakeholder Survey Assessing Member States' Rules on Health Data in light of the GDPR (July 2020).

[7] https://projectsites.vtt.fi/sites/premed/files/workshop2020/Premed_workshop_Kalliola_Sitra.pdf.

[8] https://ec.europa.eu/health/ehealth/dataspace_en, last accessed on 20 March 2021.

[9] European Commission, EU Health Data Space, <https://ec.europa.eu/health/ehealth/dataspace_en>, last accessed on 11 November 2020.

[10] The EDPS Opinion 3/2020 on the European Data Strategy, 16 June 2020, paras 21-22, addresses the requirements.

clearly identified upfront. Encryption should be the pseudonymisation technique[11] considered when sharing and storing medical records.[12]

The governance framework of the EHDS needs to inspire trust among its legitimate users and contributors to the data sets.[13] The criteria for a user to be considered 'legitimate' needs to be further specified. CPME supports the development of mandatory certification mechanisms and seals to demonstrate compliance with the EHDS rules. The EHDS should be governed by an independent authority with overarching control on the generated datasets in the Space, where an independent expert from each Member State is represented. Such authority must also be subjected to the supervision of the European Data Protection Supervisor, ensuring consistent coordination with the European Data Protection Board. The sustainability of the EHDS (financially and human resources), should be sufficiently accounted for in the respective legislative framework to be developed.

A thorough impact assessment needs to be conducted before the deployment of the EHDS followed by stakeholder consultations on the preliminary findings. The EHDS will imply processing special categories of data (i.e., data concerning health) on a large-scale combining data from various sources which could result in a high risk to the rights and freedoms of patients, a data protection impact assessment is required (Article 35(3)(b) of the GDPR). Moreover, as the processing will be novel, the impact assessment should consider other fundamental rights such as the right to a private life and human dignity, as well as ethical and societal concerns that can emerge. The impact assessment should be revisited when future data sources and technologies emerge, and the results of such assessments should be made public.

4. EHDS Code of Conduct

The EHDS should be governed by a code of conduct which should apply to any entity, public or private, that uses or contributes to the data space. This code should cover the rights of the legitimate data contributors[14] and their enforcement, clauses governing data quality standards, state-of-the-art encryption requirements, and high standards for interoperability[15] solutions which respect fundamental rights and ensure a high level of security, and the concept of medical confidentiality as a starting point. The implementation of the code by its signatory parties must be monitored. Legitimate data contributors or end-users should be informed about a breach of the code compliance.

---

[11] See 'Pseudonymisation techniques and best practices - Recommendations on shaping technology according to data protection and privacy provisions', ENISA, November 2019.

[12] Cyberattacks are significantly increasing in the healthcare sector. Recently, mental health data from patients from Finish Psychotherapy Center were published after blackmail, <https://abcnews.go.com/Health/wireStory/finland-shocked-therapy-center-hacking-client-blackmail-73817011>, last accessed on 26 October 2020.

[13] The overarching term of 'legitimate users and contributors' is to encompass the different processing operators which are still uncertain at this moment. As 'legitimate users', CPME envisages researchers, government officers, etc.; as 'legitimate contributors', CPME envisages healthcare providers and patients.

[14] Ibid.

[15] Interoperability refers to the ability of different information systems, devices and applications to access, exchange, integrate and cooperatively use data in a coordinated manner, within and across organisational, regional and national boundaries.

Moreover, in medical research the principles of the Declarations of Helsinki[16] and Taipei[17] have to be complied with. The code should therefore incorporate these principles, in particular the right to information, the right to access the information about one's health data, requirements for consent and respective withdrawal limitations. Feedback of findings to the data subject is desirable for transparency reasons and it may help promote support about the research by the community at large. The right balance between individual rights and research needs to be ensured.

The Code of conduct should define what constitutes a qualified legitimate interest to use health data.

5. Data availability and access regime

The data sources that will feed the EHDS and consequent access to datasets are still unclear. The European Commission has identified four different data relationships where data sharing could increase: i) government-to-business (G2B); ii) business-to-business (B2B); iii) business-to-government (B2G); and iv) between public authorities (G2G).[18] CPME also identifies the health data relationships between patients and businesses which are expanding further (e.g., big tech initiatives such as the Apple Health) (P2B).

Access to patient data requires a sectoral approach and a specific solution focused on regulating access on a dataset-by-dataset basis. For CPME, medical confidentiality, privacy, and data security need to always be ensured when processing patient data,[19] in particular when personal data are processed for other purposes than the purpose for which the data were originally collected, such as the treatment of the patient (secondary use of patient data). The EHDS must only be fed with data that comply with data protection legislation and the future EHDS code of conduct.

CPME supports granting special access to the European Medicines Agency and the European Centre for Disease Prevention and Control to the EHDS. EMA and ECDC should have clearly defined roles and responsibilities in the EHDS legal framework.

CPME further advocates:

- G2B access – patient data in public databases should only be shared with private entities that demonstrate a legitimate interest, e.g., for research purposes, and in an anonymised and/or aggregated form. If anonymisation cannot be achieved without undermining the quality of the research, then consent from the data subject should be sought. When consent cannot be obtained or involves a disproportionate effort, then a positive advice by an independent research ethics committee and other independent review board should be guaranteed. In such case, the patient data to be shared should not be related to the individual patient, e.g., having undergone pseudonymisation. The use of and access to genetic data for insurance, credit, criminal justice, education or employment purposes should never be allowed. No one should

[16] 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.

[17] 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.

[18] COM(2020) 66 final, p 7-8.

[19] Processing of patient data is understood as the general term of the GDPR, including collecting, recording, storing, consulting, using, disclosing by transmission or even when destroying health data.

be discriminated because of their genome. Moreover, ethical objections on a societal and patient level against certain private entities need to be taken into account.

- B2B access – a black market can occur between a legitimate user and a non-legitimate user, using patient data to develop new treatments, medicines and medical devices. There needs to be legal, organisational, and technical assurances that the data is not shared outside legitimate users.
- B2G access – patient data in electronic health records from healthcare providers private databases should only be shared with public authorities in an anonymised form, except if otherwise provided by law. A specific legal regime must be foreseen to avoid any abuse of identifiable data, e. g. for mass surveillance or discrimination. The relevant public health purposes need to be clearly identified and justified. A traceability mechanism should be set up in case of governmental use of health data from mobile applications and wearable devices.
- G2G access - sharing of patient data between public authorities for the purposes of the EHDS needs to be based on a common EU definition of 'public health interest', to be defined by law. Such law also needs to specify the precise type of data to share and the legitimate public authorities to whom the data are transferred to.
- P2B access –health data should not be for sale, or traded between companies, and no advantage should be granted or promised to individuals for providing health data. The European Commission proposes[20] that individuals should provide data to European dataspaces via 'data intermediaries' or 'data altruism organisations'. The concept of separate entities that collect and anonymise data from individuals before making them available to legitimate users deserves consideration. Private entities who intend to use health data should demonstrate a qualified legitimate interest, and an independent body, e.g., an ethics committee, should decide on the use.

The EHDS should start from specific and identified use cases where data sharing is urgently required, for example in the case of pandemics.

Nudging techniques or dark patterns should not be used or supported. The incentives for healthcare providers or data controllers to share their data should be ethically assessed. General guidance about the practices allowed should be developed.

6. Children's data and other vulnerable groups

Access to children's data or other vulnerable groups needs to go along with stronger safeguards. Authorisation by the holder of parental responsibility or by another legal representative of the data subject, needs to be verified in practice.

Moreover, due to the 'explosion' of data collection and data analytics in today's digital society, EU co-legislators should consider developing the right for a 'clean data slate' for minors.[21] When they are old enough to understand the consequences of data collection, minors should be granted the right to demand companies to delete any personal information collected about them, as data subjects, prior to their legal emancipation, safeguarding patient data as determined by the data subject him/herself.

[20] Proposal for a Regulation on Data Governance of 25 November 2020, COM(2020)767.

[21] Eva Lievens and Carl Vander Maelen. 'A Child's Right to be Forgotten: Letting Go of the Past and Embracing the Future?' Latin American Law Review n.º 02 (2019): 61-79, doi: https://doi.org/10.29263/lar02.2019.03, p 6 and 11.

7. Mixed patient data sets

The use of mixed data sets, where personal and non-personal data (ex. industrial data, smart cities data, anonymous data, etc.) combine, are very common.[22] Mixed patient data sets can be found in electronic health records, clinical trials or data sets collected by mobile health and wellbeing apps.[23] If the non-personal data part and the personal data parts are 'inextricably linked',[24] the data protection rights and obligations stemming from the GDPR must fully apply to the whole mixed dataset.[25] As a result, a valid legal basis to process patient data, an appropriate justification, secure processing and sufficient safeguards should be in place.

8. Data altruism

CPME supports the concept of data altruism when patient data will be used for the common 'public health interest' and the latter are clearly identified in advance by law. It must be based on patients' consent and in full compliance with the General Data Protection Regulation (GDPR)[26] and with the national regulations of medical confidentiality. A European approach to obtaining patients' consent in line with the GDPR should be developed. In particular, the patient should be allowed to choose the purpose, the public sector body or the research type for which the consent has been given.

9. Digital health literacy

CPME supports investing in digital health literacy for patients, doctors and IT professionals.[27] Education is necessary in order to build trust on the use of patient data for secondary purposes. CPME would welcome the creation of a 'fair data label' to inform patients that the use of their patient data is compliant with basic principles and standards of data protection and secondary use. Moreover, a specific register for digital health specialists who abide to ethically-based codes of conducts and are subject to regulatory and/or disciplinary sanctions should exist.

10. Interoperability and data infrastructures

CPME supports standardisation for interoperability purposes of operating systems as long as it does not translate into regulating medical practice or diminishing the scope of the delivery of healthcare services, which must continue to be provided in accordance with patient needs and evidence-based medicine reflecting technical and scientific progress.

CPME advocates for high level requirements for the protection of patient data. For example, the transition of IHE-Profiles from HL7v2 and HL7v3 to HL7-FHIR should be considered as well as the SNOMED CT's ability to create and sustain semantic interoperability of electronic health applications.

---

[22] Commission's Communication on "Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union", COM(2019) 250 final, 1-22.
[23] Idem, p 9-10.
[24] *"A situation whereby a dataset contains personal data as well as non-personal data and separating the two would either be impossible or considered by the controller to be economically inefficient or not technically feasible*.", COM(2019) 250 final, p. 10.
[25] Idem, p 9-10.
[26] Regulation (EU) 2016/679 of 27 April 2016.
[27] For further information, see CPME Policy on Digital Competencies for Future Doctors, adopted by the CPME Board on 21 November 2020.

There are currently several ongoing European Initiatives which allow data sharing. For example, the International Data Spaces Association (German model), iSHARE (Dutch model) and IHAN (Finish model).[28] These models and best practices within each should be compared to the architectural model of the EHDS, at the moment unclear (who stores what and where for what purpose).

Until such analysis is made, CPME draws the attention to the European Network of Cancer Registries (ENCR),[29] in operation since 1990, which promotes collaboration between cancer registries and defines data collection standards. This seems to be a good model to be taken into account.

Recommendations

- Trust is critical for a successful EHDS. Therefore, CPME supports investing in digital health literacy for patients, doctors and IT professionals.
- The EHDS should have a clear legal framework, based on the GDPR and transparent policies concerning the processing of patient data available for business and government, in particular on medical confidentiality, data access, secondary use of data, information rights, feedback of findings, transfer to third parties, mixed patient data sets, data altruism, interoperability and data infrastructures, etc.
- The EHDS legal framework should provide clear criteria for using patient data in the 'public health interest', of for the 'public good'. Legal criteria should be sought for 'scientific research' and 'innovation' to guide the purpose of the space andto avoid that these notions are perceived as general exemptions to key requirements of the GDPR (e.g. purpose limitation, data minimisation, anonymisation, consent).[30]
- The oversight of the EHDS should be composed of three layers:
    - legislative, with a specific regulation for the space;
    - institutional, with an independent ethical review Board for certain data sets or certain processing operations; and,
    - other safeguards and a code of conduct for users. The safeguards need to respond to the legal and ethical risks related to data sharing and they must be dynamic and evolutive.

References

- Staunton, Ciara, Santa Slokenberga, and Deborah Mascalzoni. "The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks." European Journal of Human Genetics 27, no. 8 (2019): 1159-1167.
- SITRA. "35 Proposals to Make the European Data Strategy Work". Working paper, 18 May 2020.

[28] For further information see INNOPAY and SITRA's "White Paper on Data sovereignty and soft infrastructures: key enablers for the next phase of the European data economy", 1 October 2020.

[29] The ENCR was established within the framework of the Europe Against Cancer Programme of the European Commission. The ENCR also provides training for cancer registry personnel and regularly disseminates information on incidence and mortality from cancer in the European Union and Europe. Further information see www.encr.eu.

[30] For further information, see EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, 2 February 2021.

- INNOPAY and SITRA's "White Paper on Data sovereignty and soft infrastructures: key enablers for the next phase of the European data economy", 1 October 2020.
- European Data Protection Supervisor:
    - Opinion 3/2020 on the European Data Strategy, 20 June 2020
    - Preliminary Opinion 8/2020 on the European Health Data Space, 17 November 2020
- ENISA, 'Pseudonymisation techniques and best practices - Recommendations on shaping technology according to data protection and privacy provisions', November 2019.

***