*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.*

# Position on the European Health Data Space

## Main Messages:

1. European doctors believe that the European Health Data Space (EHDS) can contribute to the provision of improved quality of healthcare to patients for primary use. The EHDS can also contribute to the enhancement of the provision of healthcare by stimulating the availability of health data for scientific research.
2. A high degree of trust and acceptance by patients and healthcare professionals will be a cornerstone of a successful EHDS. These main users must be at the centre of the EHDS concept. The usability for primary users of the system is a must and the EHDS should not diminish patient consultation time and experience.
3. CPME worries that the implementation costs of the Proposal will exacerbate already strained healthcare systems.
4. CPME is concerned whether the EHDS Proposal can maintain a high level of protection of fundamental rights, including personal data, with sound procedures that respect human dignity, autonomy, and privacy of individuals.
5. The quality of data is of paramount importance to the provision of safe, effective, and quality healthcare.
6. The role, competencies and practice of doctors and healthcare professionals will undergo a profound change with digitalisation and the EHDS. These changes and consequent obligations, as well as the impact on the delivery of healthcare, are not sufficiently addressed in the Proposal.
7. A high degree of semantic, legal, and technical interoperability will be key for a successful EHDS. Strong obligations for software manufacturers for interoperability and usability are mandatory.
8. In order to respect existing traditions and contexts in Member States, there should be national discretion with regards to the implementation of ethical safeguards. This includes ethical requirements in relation to the secondary use of health data, such as the duty to obtain patient's consent or to involve ethics committees.

## Introduction

CPME congratulates the European Commission for presenting an innovative framework that addresses specific challenges to electronic health data access and sharing. The proposal for a regulation of the European Parliament and of the Council on a European Health Data Space ('the Proposal')[1] brings new possibilities to use health data for medical diagnosis, the provision of health, social care and treatment, or the management of health care systems and services. It is also another positive step towards the formation of the European Health Union.

Whereas the Proposal is based on Articles 16 and 114 of the Treaty on the Functioning of the European Union (TFEU), CPME would like to emphasise that, according to article 168(7) TFEU, Union action shall respect the responsibilities of Member States for the definition of their health policy and for the organisation and delivery of health services and medical care. CPME would like to reaffirm that the EHDS should not jeopardise this competency of Member States.

CPME welcomes the distinction between the use of health data for the provision of health services (the so-called 'primary use'), and the use beyond the individual care of patients, in particular for research (the so-called 'secondary use'). A precision should nonetheless be made in relation to research that uses electronic health data from biobanks and dedicated databases. Biobanks are often created for research purposes, which is their primary purpose, and thus do not fit well within the concept of 'secondary use'.

The number of delegated and implementing acts renders it difficult to predict the full impact of the Proposal. A better assessment of the legal, social, technical, and financial consequences for doctors, other healthcare professionals (HCPs), patients and the provision of healthcare is needed, in particular to estimate whether the implementation costs will be proportional to the benefits, especially in those Member States that have already invested significant human and financial resources in digital health care systems, including EHRs.

European Doctors call your attention to the following challenges stemming from the Proposal:

[1] COM(2022) 197 final.

## 1. Impact on healthcare delivery

CPME believes that the Proposal does not go far enough in ensuring national discretion in relation to the delivery of healthcare. This is particularly relevant as Member States and their individual traditions in safeguarding the informational self-determination of individuals will be challenged with the introduction of the EHDS. The (legal and ethical) conditions for how health data can be used cannot constrain current national practices.

Telemedicine is a healthcare service which is not harmonised at EU level. There are different rules at national level on when telemedicine services can be used, for which medical conditions and how often, on what can be diagnosed and by whom, on the required professional qualifications, on the reimbursement scheme and insurance, on medication prescriptions (e.g. antibiotics and opiates), on medical liability, and even on how privacy and confidentiality are dealt during the service. Article 8 of the Proposal implies regulating over Member States' responsibilities for the organisation and delivery of health services and medical care, including the management of health services. This provision should therefore be deleted.

## 2. Cultural shift and high impact for European doctors

The Proposal implies a cultural shift on health data sharing, even in countries where sharing is present for several years. It will generate a high impact for European doctors in relation to the primary use of electronic health data, with increased obligations (e.g. by registering data in a structured and specific way, adding to the workload), costs, and administrative burdens.

The Proposal will require doctors to improve their digital health literacy and digital competencies. Internal protocols will need to be adapted to the European electronic health record exchange format (EEHRxF), and during the data life cycle, several steps and actions will be required to prepare the data in the format and the quality that can be properly used. European doctors warn that, at present, neither healthcare systems nor practicing health professionals or the generation in training are adequately prepared.[2]

[2] CPME Policy on Digital Competencies for Doctors, November 2020, www.cpme.eu/api/documents/adopted/2020/11/CPME_AD_Board_21112020_100.FINAL_.CPME_.Policy.Digital.Competencies.for_.Doctors.pdf.

The Proposal must be clear that the design and technical implementation with EHDS complies with the principles of medical ethics[3] and does not pose any risks to medical confidentiality. The public needs to improve their digital maturity. Patients will need to improve their digital health literacy and understand about consent management.

The information and technology industry will need to avoid conflicting standards, and work to achieve interoperable systems, allowing portability, accessibility, and accountability.

Governments will need to properly budget for the major financial investments that digitising the healthcare sector requires, including a line for direct financial support for doctors and other HCPs willing to digitalise and connect their medical practice to the national electronic health system and/or to EHDS. Governments will also need to ensure that the new public authorities appearing in the healthcare landscape, which will provide and manage access to health data, do not conflict with the tasks and competences of current public authorities, namely data protection authorities and healthcare regulators. They will also need to ensure legal and ethical consistency in the decision-making of granting a data permit to avoid forum-shopping.[4] Governments should develop a specific register for digital health specialists who abide by ethically-based codes of conducts and are subject to regulatory and/or disciplinary sanctions to inspire trust and accountability of those behind (developing and maintaining) the system.

Researchers should be aware of the potential limitation of the EHDS, such as bias in case of patients' opt-out of the EHR and/or Member States' limited capacity to exchange health data.

European Doctors call for a better assessment and clear image of the consequences that the EHDS framework will have for doctors, patients, and the provision of healthcare.

[3] In medical research, the principles of the Declarations of Helsinki and Taipei have to be complied with. The General Data Protection Regulation (GDPR) is not sufficient to address the processing of health data for secondary purposes. The Declarations are more exhaustive in relation to the right to information, the right to access the information about one's health data, and requirements for consent and respective withdrawal limitations. Feedback of findings to the data subject is also desirable for transparency reasons and it may help promote the research by the community at large. See in this sense the 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; and the 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.

[4] In this context, forum shopping would mean the practice of data holders filing a permit request with a health data access body from a Member State that has more relaxed ethical requirements.

## 3. Data quality in the clinical file

The Proposal allows for the possibility of patients or their representatives to insert their electronic health data in their EHR and that information should be marked as inserted by the patient or representative (Article 3(6) of the Proposal). European Doctors warn that this possibility could both enrich the EHR or lead to the file becoming less suitable as a clinical tool. The file might be easily saturated with data (due to the future interactions of the EHR with medical devices, wellness apps and other software, or result from patient's medical condition which require continuous care), rendering it difficult to find relevant and useful information. For this reason, doctors need to have appropriate tools to deal with different types of health data. It must be possible for a doctor to see in the EHR data imported by the patient and easily select what to see in a query. The right for patients to insert their electronic health data in their EHR should be regulated at Member State level, as it interferes with the delivery of health care services at national level.

The Proposal lacks clarification on how doctors and other HCPs, limited by time constraints, should use the EHR in order to reach its full potential.

European Doctors recommend that Article 5(1) of the Proposal is readjusted as follows:

- the EHR should favour the use of structured data and documents that can be interoperable. The file should be concise, validated, accurate and relevant;
- allowing other categories of personal electronic health data to be available in the EHR (Article 5(1) third paragraph of the Proposal) should remain a Member State's competence;
- specific relevant fields in the EHR should be highlighted (e.g. patient ID, allergies, laboratory data, medical alerts, and current medication);
- any rectification to the clinical file requested by the individual is made in the presence of the competent registered doctor or HCP; and
- digitalisation must not place patients at a disadvantage or exacerbate existing disadvantages (e.g. poor access to the internet, poor digital skills, physical disabilities, homelessness, the effect of ageism or just being uncomfortable to use the virtual environment).

## 4. Liability and accountability

The digitisation and the EHDS will entail considerable uncertainties and risks for doctors. The EHDS should not foster further uncertainty that might impede the individual doctor's capabilities to provide healthcare. The legal accountability on the EHDS must not go beyond the doctors' competency or responsibility. Physicians can only be responsible for the data they have inputted in the EHR. Follow-up on investigations (e.g. blood tests) is the sole responsibility of the requesting physician and cannot be delegated to another physician without agreement.

Liability and accountability have not been sufficiently clarified. For example, the burden of proof when information is blocked by the patient, and healthcare professionals' responsibility in diagnosing and treating individuals based on incomplete information (Article 3(9) of the Proposal). Therefore, it should be up to Member States to decide whether patients should be granted the right to block data in the EHR. If information is excluded, a notification should be mandatory of such absence in the file.

European doctors request clarity concerning the case where a patient requests not to include his/her diagnosis in the EHR (e.g. STDs or domestic violence), and the consequences that action can entail for healthcare professionals' liability.

Doctors have a professional duty to maintain accurate and up to date clinical records. Data added by patients or imported into the EHR by wellness apps is not clinical. This data can pose a significant medico-legal challenge for doctors.

The Proposal is not clear who is responsible to provide access to the EHR, insert or obtain information therein. The doctor cannot be held liable for the non-compliance of Article 3 of the Proposal and the consequent administrative fines that supervisory authorities may apply (Article 3(11) of the Proposal and cf. Article 11).

The Proposal should also safeguard that the right of natural persons to obtain information on health professionals that have accessed their electronic health data in the context of healthcare (Article 3(10) of the Proposal) cannot cause unintended or dangerous situations for the health professional involved. It is crucial that exceptions to such rights can be made at Member State level.

## 5. Rights of natural persons

The Proposal does not clearly address the case of minors and of persons lacking legal capacity. The reference to the establishment of proxy services by Member States foreseen in recital 9 of the Proposal needs to be explicitly referred to in Article 3(6) of the Proposal.

The enforcement of the right of natural persons to receive an electronic copy of their electronic health data will be unmet as the healthcare sector (private vs public) is at different speeds, as are Member States. Administrative fines cannot be applied in this case.

## 6. Registration of personal electronic health data

Doctors and other healthcare professionals will be required to systematically register the relevant health data in the electronic format in an EHR system (Article 7(1) of the Proposal). The EHR system needs to have user-friendly interfaces which are co-designed with those directly using it; it should be simple and embedded in the doctor's care pathway; interoperable to reduce administrative burdens; and the electronic registration of health data should not be retroactive.

Doctors as data holders (Article 2(y) of the Proposal) should be excluded from the obligation to provide health data for secondary use (Article 33 of the Proposal). The Once Only Principle (OOP) should be applied, meaning that natural or legal persons provide data only once to public sector bodies or EHR providers under the primary use regime, while public sector bodies take the necessary steps to use such data for secondary purposes – even across borders – always in respect of data protection rules and other constraints. This is needed to avoid duplication and unnecessary burdens to doctors, especially in individual practices, to provide data again.

## 7. Certification of EHR systems

European doctors believe that mandatory self-certification schemes are not sufficient to create trust among patients and doctors that the EHR systems comply with security requirements laid down in Annex II of the Proposal and that they process health data according to the GDPR (Article 14 of the Proposal).

CPME supports the EDPB-EDPS recommendation for the EHR systems to be subject to a third-party conformity assessment procedure, involving notified bodies, in the assessment of the technical solutions on interoperability and security.[5]

## 8. Secondary use of electronic health data

CPME strongly recommends respecting national culture on health data sharing and the principle of data minimisation, as well as specific safeguards and derogations for data protection pursuant to Article 89 of the General Data Protection Regulation. However, certain provisions of the Proposal have the potential to challenge the traditions of Member States regarding the secondary use of health data.

Article 33 of the Proposal lists categories of 'electronic data' that 'data holders' will have 'to make available' for secondary use. This list is wide and extensive, comprising very sensitive data that cannot be anonymised. Therefore, certain categories listed in the Proposal such as 'human genetic, genomic and proteomic data' (Article 33(1)(e) of the Proposal), and 'electronic health data from biobanks and dedicated databases (Article 33(1)(m) of the Proposal) call for a differentiated approach allowing flexibility for Member States. Such categories are particularly sensitive, as they bring new discrimination risks (e.g. insurance, employment, credit, education, medical treatment) based on genetic or genomic information.

In order to uphold the current level of data protection pursuant to the GDPR, CPME recommends using both traditional tools, such as applying the highest technical standards of data protection, anonymising and pseudonymising personal data, requiring informed consent from the data subject and following the recommendations of data protection authorities.

Additional measures that should be used to protect patient privacy, confidentiality and autonomy include legal and technical tools, such as:

- Allowing opt-out options. In certain Member States, natural persons are accustomed to exercising rights over their data, in particular they can either opt-out or opt-in into the collection and usage of such data;

- Creating a secure data environment. Providing data access in closed secure data analysis environment from which the data cannot be removed;

[5] EDPB-EDPS Joint Opinion 3/2022 on the Proposal for a Regulation on the European Health Data Space, 12 July 2022, points 72-76, <https://edps.europa.eu/data-protection/our-work/publications/edps-edpb-joint-opinions/european-health-data-space_en>.

- Limiting the purposes for which data can be used. Member States need more flexibility to further restrict the purposes for which a health data access body can provide access to the applicant to electronic health data for secondary use. Ethical objections from patients against certain private entities' access to health data need to be taken into account;

- Sanctioning unauthorised disclosure and misuse of privileged information. Health data received under the secondary use regime should be considered 'privileged information'. The disclosure or misuse of such 'privileged information' (e.g. by breaking into computer systems) should be sanctioned. There should be no detrimental legal effects or discriminatory measures against the victim.

- Systematically involving **ethics committees or review boards**. Ethics committees or review boards are a cornerstone in medical research.[6] The use of data can be extremely damaging for an individual if misused. Ethics committees or review boards need to verify, among other, whether the data requested is indeed necessary, if the research in question is worthy, if it can produce scientific sound results, and if it will not be detrimental to the individual. This analysis should be made regardless of whether consent has been provided by the individual. Moreover, these entities could be entrusted to approve the establishment of a database concerning health used for research and policy-making; have the right to monitor on-going activities, ensuring regular ethical oversight; and observe whether IT usage does not compromise the principles of medical ethics.

- Prohibiting unethical practice. Profiling of individuals should be explicitly prohibited under Article 35 of the Proposal. As noted in the EDPB/EDPS joint opinion on the data act,[7] the processing of health data should not allow drawing precise conclusions concerning the private life of individuals or lead to high risks for their rights and freedoms. In addition, goods or services which are designed or modified in a way that incites addiction of individuals, in particular children and vulnerable groups, should also be prohibited under Article 35 of the Proposal.

[6] See CPME leaflet on 'Role of Ethics Committees in the European Health Data Space', 25 May 2022, CPDP Conference 2022, <https://www.cpme.eu/api/documents/adopted/2022/04/A4_CPDP_Flyer_220427.pdf>.
[7] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 4 May 2022, Executive summary page 2 and points 53-55, <https://edps.europa.eu/system/files/2022-05/22-05-05_edps-edpb-jo-data-act_en.pdf>.

## 9. Consent in secondary use of electronic health data

European Doctors warn that the need to comply with medical confidentiality, professional secrecy and 'consent-requirements' obligations must not be overruled by the processing activity for secondary use. In line with the joint EDPS and EDPB opinion on the European Health Data Space,[8] the interplay of the Proposal with the GDPR in relation to personal data protected by professional secrecy and to prior consent needs to be further clarified.

Pursuant to Article 9(2)(h) read together with paragraph (3) and Article 9(2)(i) of the GDPR, the respect of professional secrecy is a core element to safeguard the rights and freedoms of data subjects (natural persons). Removing the requirement to obtain informed consent from natural persons (Article 33(5) of the Proposal) proposes a very significant change to the legal grounds for accessing health data for secondary purposes as it may imply a breach of confidentiality and professional secrecy, compromise the principles of medical ethics, and hence the free access to healthcare. Indeed, patients may become reluctant to provide information or even consult with their treating physician if they fear that such information will not remain secret.[9]

The EHDS needs to respect individual consent according to national law (Article 9(4) of the GDPR) and the principles of medical ethics. There should be prior consent or another appropriate legal basis for both uses. The EHDS also needs to ensure national discretion. Such a cornerstone for maintaining confidentiality and trust in national health systems – and for organising and delivering health services – the requirement of consent should not be regulated at EU level. Rather, it should be left for each Member State to decide.

This is also relevant in case of incidental findings (Article 38(3) of the Proposal), as if there is no consent form in secondary use in relation to pseudonymised data, the natural person often cannot be traced back. In case the patient is traceable, the treating doctor should be informed first about the incidental finding to respect patients' wishes of not to be informed. Finally, the obligation to obtain consent prior to secondary use should fall under the entity responsible for setting up and managing the EHR system, not necessarily of HCPs.

[8] EDPB-EDPS Joint Opinion 3/2022, point 92.
[9] In this sense, see the WMA Declaration of Helsinki on Ethical Principles for Medical Research involving Human Subjects, points 25-32, and WMA Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks, which specifies that consent is only valid if the concerned individuals have been adequately informed about the research (point 12).

## 10. Re-identification risks in secondary use

Several scholars have shown that with little information (e.g. weight-size ratio, age and sex), the re-identification of natural persons is possible and remains a risk to protect patient's privacy.[10] CPME welcomes the principle of anonymisation as a rule for processing health data for secondary use (Articles 44(2) and 47(1) of the Proposal) and the prohibition to re-identify electronic health data in a pseudonymised format (Article 44(3) of the Proposal).

For CPME, the re-identification and disclosure of de-identified personal data is a major breach of trust that can put into jeopardy the secondary use system. Sanctions should be high in these cases, and Member States should consider criminalising such conduct to serve as a deterrent measure.

## 11. Digital applications

Health data generated by wellness applications and other digital health applications do not have the same data quality requirements and characteristics of those generated by medical devices.[11] Only certified digital applications which comply with ISO standards (e.g., ISO/TS 82304-2 on Health and wellness apps – Quality and reliability) and are CE approved can be integrated into the EHR systems. That data from certified digital apps should only be added to the EHR with agreement of the treating physician.

For secondary use, the integration of health data from wellness apps in EHR systems should only be included if medically provided.

The use of health data for secondary purposes generated by these applications must only be done with prior consent within the meaning of the GDPR regarding natural persons.[12] Wellness applications must not be able to access data in the EHR.

[10] Sweeney L, Abu A, and Winn J. Identifying Participants in the Personal Genome Project by Name. Harvard University. Data Privacy Lab. White Paper 1021-1. April 24, 2013. (PDF), <https://dataprivacylab.org/projects/pgp/1021-1.pdf>; Gutmann, A. (2013). Data re-identification: prioritize privacy. Science, 339(6123), 1032-1032, <https://www.science.org/doi/10.1126/science.339.6123.1032-b>; El Emam, K., Jonker, E., Arbuckle, L., & Malin, B. (2011). A systematic review of re-identification attacks on health data. PloS one, 6(12), e28071, < https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0028071>; Y. Sei, H. Okumura and A. Ohsuga, "Re-Identification in Differentially Private Incomplete Datasets," in IEEE Open Journal of the Computer Society, vol. 3, pp. 62-72, 2022, doi: 10.1109/OJCS.2022.3175999, < https://ieeexplore.ieee.org/abstract/document/9779455>.

[11] EDPB-EDPS Joint Opinion03/2022 on the Proposal for a Regulation on the European Health Data Space, adopted on 12 July 2022, point 35.

[12] Ibid, point 36.

## 12. Health data access bodies

Health data access bodies should act in complete independence from external interference when performing its tasks and exercising its powers. Its members should remain free from external influence, whether direct or indirect, and should neither seek nor take instructions from anybody.

## 13. Data permit

Data permits should not be tacitly approved when the health data access body fails to provide a decision within the time limit. CPME understands the rationale behind to ensure that the procedure remains responsive to data requests. However, there is the possibility that health data access bodies are flooded with requests with a sole purpose of paralysing them. Considering the risk of third parties using health data without the necessary evaluation and defined conditions, including big online platforms, the final sentence of Article 46(3) should be deleted.

## 14. Costs and impact on small medical practices

Member States need to plan in advance and foresee at national level specific budget lines for direct financial support for doctors and other healthcare professionals willing to digitalise and connect their medical practice, with all that it implies (e.g. new infrastructure and cybersecurity maintenance, capacity building and other preparatory actions). The Commission should ensure that Member States distribute the EU financial incentives available evenly and fairly among those affected by the Proposal.[13] The costs of digitalisation must not be passed on to healthcare workers without appropriate compensation.

The time spent by a doctor and other healthcare professionals reviewing and analysing the electronic file may vary considerably, depending not only on the purpose of the consultation (diagnosis, treatment, referral) but also on the patient-doctor relationship (new patient, chronic patient, or regular patient). This time needs to be accounted for by Member States, as well as the time spent in updating or rectifying the electronic file.

[13] Member States are expected to receive from the EU4Health programme a substantial initial contribution of almost 110 million euros to promote the establishment and functioning of the EHDS. It will cover, among other, the development, deployment, and maintenance of infrastructures for primary and secondary uses of electronic health data. Additional funds are foreseen from this programme (up until 60 million euros) and from the Digital Europe Programme (50 million euros). Instruments such as Recovery and Resilience Facility (RRF) and the European Regional Development Fund (ERDF) will be able to support the connection of Member States to the European infrastructures.

Micro-enterprises[14] are excluded from the obligation to make their data available for secondary use in the framework of EHDS. For CPME, this threshold should be higher to also exclude small enterprises such as individual or small practices[15] or, at least, adherence should be made voluntary.

The environmental cost of digital health also needs to be considered.[16]

## 15. Conclusion

For the Proposal to be successful, great efforts from all involved parties will be required. Member States are at different digitisation speeds, doctors and other HCPs have different digital skills and individuals have different attitudes towards health data sharing. The development of the data economy, a consequence of the processing of health data, must not lead to unequitable access to healthcare. Medical confidentiality, privacy and personal data protection and individuals' consent need to be at the centre of secondary use of electronic health data. In addition, the new way of working will demand investments and continuous development of technical solutions. It is necessary to ensure that the tasks which will have to be performed by doctors do not create a disproportionate administrative burden or cost on professionals. The projects' timeline needs to be realistic in view of its complexity. European doctors remain committed to finding workable solutions to achieve a EHDS which will benefit patients.

***

[14] Article 2(3) of the Annex to the Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium sized enterprises (OJ L 124, 20.5.2003, p. 36): *"(…), a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million."*

[15] Article 2(2) Commission Recommendation 2003/361/EC: "(…) a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million."

[16] French Presidency, European Ethical Principles for Digital Health, 2 February 2022.