The Consumer Voice in Europe

BEUC COMMENTS TO

# COMBINED EVALUATION ROADMAP/INCEPTION IMPACT ASSESSMENT FOR LEGISLATIVE PROPOSAL ON A EUROPEAN HEALTH DATA SPACE

**Contact: Jelena Malinina – health@beuc.eu**

**BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND**
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2021-008 – 10/02/2021

BEUC, The European Consumer Organisation appreciates the opportunity to provide input to the European Commission's ongoing evaluation of the need for a legislative proposal on a European Health Data Space. We consider that the evaluation provides a timely opportunity to ensure that sensitive data of European patients and consumers used for scientific advancements is well protected and serves societal interests. BEUC supports the following proposals of the roadmap:

## 1. Primary and secondary uses of health data

### ➔ Sector specific regulation is needed

Health data comes from varied sources: (electronic) health records, medical devices, fitness trackers, apps and social media. Multisource health data combined with the use of advanced analytics is making privacy and data protection a more complex task than just putting in place the standard protection mechanisms foreseen by the existing data protection legal framework. For example, while user consent is one of the main means to control personal data, it will not provide in itself, sufficient protection regarding all possible future data uses, especially in the context of health research, where often combinations of multisource personal and non-personal data are used. It is necessary to build on and complement the GDPR on specificities of sensitive multisource health data. A sector specific legislation should not by any means undermine the GDPR. In particular, there is a need for binding rules on:

- Health data anonymisation and pseudonymisation to ensure high protection of patients and consumers data;
- Access to data available via EHDS, including but not limited to who can use the data, rules on consent, data minimisation, purpose limitation, data retention and other core data protection principles;
- Quality and security for all information systems where health data is generated, used or stored to prevent data misuse and unauthorised access;
- Accountability, liability and redress mechanisms in case of data misuse resulting in patient or consumer harm related to health, discrimination and/or other damages.

Furthermore, harmonised sector-specific rules will help to address existing fragmentation in policy on secondary health data processing across the Member States.

## 2. Digital health services

### ➔ Clear rules on digital cross border healthcare services are missing

The COVID-19 pandemic speeded up adoption of digital healthcare services across the EU. However, it is still a largely unregulated area, especially when it comes to the provision of such services cross border. The Cross Border Healthcare Directive seems to apply to certain aspects applicable to telehealth while it might not be applicable to others.[1] For instance, when telehealth is delivered as a healthcare service, some open issues remain as regards the requirements for health professional's qualification and registration in order to practice telemedicine. This is crucial for telehealth service

[1] Raposo VL. Telemedicine: The legal framework (or the lack of it) in Europe. GMS Health Technology Assessment. 2016;12:Doc03. doi:10.3205/hta000126.

liability, as they are directly linked with the questions of legal consequences of a treatment provided through telemedicine. In addition, according to EU legislation, a healthcare professional offering telemedicine needs only to be registered in the country where he/she is physically established. Yet it is not clear whether a physician must be registered first for traditional healthcare practice to be then allowed to practice telemedicine.[2] The EU Directive on the recognition of professional qualifications does not apply to healthcare professionals providing cross-border telemedicine, as it only covers healthcare professionals that physically move to another Member State to practice their profession. This is an important aspect to take into account, as what is considered 'regulated' health professionals differ across the EU Member States. For example, there are different approaches to 'traditional' and 'complementary' health professionals (e.g. homeopaths, naturopaths) and in some countries such professions are regulated, in some not.[3]

These ambiguities could potentially compromise the safety and qualityof digital health services and lead to the situations where it is unclear which liability mechanisms a consumer can use in cases where a service caused damage.

There is a need for a harmonized European approach ensuring that digital health services are performed by qualified professionals, while their medical advice/action facilitated through digital means must be based on scientific evidence and designed in a way to minimise health risks to consumers. Furthermore, platforms and apps through which such services are provided must be fully compliant with the GDPR and EHDS rules, and the competent authorities checks on such compliance must be enforced.

Furthermore, the issue of interoperability in some countries is particularly relevant, as is the case in Portugal where the lack of interoperability between healthcare providers is a crucial problem, according to DECO, Portuguese consumer organisation. For example, doctors at the hospital, have no access to patient information regarding primary care. That also shows that action by Member States alone is not sufficient and that it is required a common framework at EU level.

## 3. Regulatory framework for AI in healthcare and liability

The forthcoming proposal should further specify aspects related to access to health data via EHDS in the context of AI applications in the health sector, building upon the future horizontal AI framework covering safety and fundamental-right related aspects. The need for protection already starts at the level of data-collection. AI driven products and services usually require as much data available as possible to be developed and to perform at their best. A large proportion of this data is personal and sensitive, as it contains a lot of details about patients' and consumers' health. This raises additional concerns related to personal data and privacy protection in the context of AI and health, as well as concerns over the trustworthiness of algorithm-powered diagnosis, transparency and ethical use of AI and the level of accountability and liability of the developers and healthcare professionals.

[2] Report of the eHealth Stakeholder Group on implementing the Digital Agenda for Europe Key Action 13/2 'Telemedicine'.

[3] Wiesener, S., Salamonsen, A., & Fønnebø, V. (2018). Which risk understandings can be derived from the current disharmonized regulation of complementary and alternative medicine in Europe? BMC Complementary and Alternative Medicine, 18(1). doi:10.1186/s12906-017-2073-9.

In addition to rules regarding access to data via EHDS, rules on the development, testing and validation of AI systems used in healthcare, as well as specific rights and obligations of users and providers of AI health products and services (e.g. in relation to transparency, explainability and control of AI healthcare applications, the right to object and request human intervention) are necessary. It must be carefully examined how to integrate such specific rules into the EHDS proposal in a coherent manner.

ENDS

*This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).*