BEUC The European Consumer Organisation

The Consumer Voice in Europe

EUROPEAN HEALTH DATA SPACE REGULATION: TRILOGUE RECOMMENDATIONS

Contact: Maria Merkou - digital@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-2024-003 – 22/01/2024

Why it matters to consumers

The creation of the European Health Data Space (EHDS) will allow healthcare professionals anywhere across the EU access to a patient's personal health data, making emergency treatment abroad easier and based on available data recorded previously. Patients will also be able to access their own health records and see what healthcare professionals are noting. Different kinds of entities such as public health authorities, scientists, governments, drug developers and other types of industries can also use this data in anonymised/pseudonymised forms for purposes other than treating us such as for research or public health reasons. A European Health Data Space has thus tremendous value and could improve treatment outcomes across the board. To make sure that the EHDS is a success that consumers can place their trust in, however, it is crucial that the final text of the regulation allows them to exercise their choice on who can access their health data and respects their right to privacy.

Summary

The Commission proposed to create the European Health Data Space in May 2022.[1] In December 2023 both the European Parliament[2] and the Council[3] reached their respective positions. Interinstitutional negotiations already started.

Overall, BEUC welcomes the improvements suggested by co-legislators to the Commission's proposal. For example, we welcome the Parliament's stance introducing a right to compensation for consumers (Article 69a) if their rights under the EHDS Regulation are infringed and to allow them to seek redress collectively in that case (Article 71a).

However, there are significant concerns which remain. The Council's position to weaken the proposed certification system which was already flawed in the proposed draft legislation, is a real concern.

BEUC calls on co-legislators to ensure that the EHDS Regulation delivers a high level of consumer protection. We would like to make the following recommendations:

1) **Ensure that definitions provide the highest level of consumer protection**
    - Co-legislators should adopt the definitions of 'wellness apps' and 'Electronic Health Record Systems' proposed in the Parliament's position.
2) **Allow consumers more choice to manage their health data in primary use**
    - Co-legislators should allow consumers to exercise granular restrictions on who can access their health data. This should include a right to restrict

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space, COM/2022/197 final, accessible here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197.
[2] https://www.europarl.europa.eu/doceo/document/TA-9-2023-0462_EN.html.
[3] https://data.consilium.europa.eu/doc/document/ST-16048-2023-REV-1/en/pdf.

access to registered data and a right to object to having one's data registered in an Electronic Health Record (EHR) System.

3) **Subject Electronic Health Record Systems to independent third-party conformity assessment.**

- Co-legislators should follow the European Parliament's position in Chapter III, requiring Notified Bodies to carry out the conformity assessment of EHR Systems.

4) **Introduce more safeguards for secondary uses of health data**

- Co-legislators should follow the Parliament's position, introducing a right to opt out from sharing one's health data for secondary purposes.
- Co-legislators should allow genetic data, data from biobanks and person-generated data from wellness apps to be shared for secondary purposes only if the consumer has given their prior consent, as seen in the Parliament's position (Article 33(5a)). Moreover, co-legislators should follow Article 33(1) of the Parliament's position to ensure that the categories of accessible data for secondary use are delineated and vague language is avoided. This is important to ensure that the scope of this article does not expand to data that reveals a lot about consumers but has little relevance for scientific health research.
- Co-legislators should follow the Parliament's position in Article 34(1)(e), under which innovation and development activities and AI training & testing would have to be classified first as scientific research benefitting end-users, such as patients. This would prevent all kinds of activities – even those barely health-related ones – from being classified as 'innovation activities', hence claiming access to sensitive health data that are not directly relevant to healthcare.
- Co-legislators should delete Article 49 allowing single data holders to issue data permits, following the Parliament's position.

5) **Enforcement & Individual Rights**

- Co-legislators should follow the Parliament's position, introducing a right to receive compensation for consumers if this law is broken and annexing the EHDS in the Representative Actions Directive.
- Co-legislators should foresee administrative fines, in case the Regulation is infringed, as introduced in Article 43a of the Parliament's position.
- Consumers should be able to lodge a complaint with the relevant Health Data Access Body and also have the right to an effective judicial remedy regarding the decisions of both Digital Health Authorities and Health Data Access Bodies.

Contents

1. Definitions

a) Electronic Health Record Systems

Defining EHR Systems as products, as proposed by the European Parliament in Article 2(2)(n), will make it easier for consumers to seek redress through the Product Liability Directive,[4] in case they suffer damages from a defective EHR system.

BEUC recommendation:

- Co-legislators should follow the definition of 'EHR systems' proposed by the European Parliament.

b) Wellness applications

Data from wellness apps is very low-quality data and also poses a high risk of re-identification especially when combined with health data from other sources. It is therefore important to ensure a narrow definition of this concept, to make sure that only data directly related to healthcare delivery gets included in the scope.

The proposed wording of the European Parliament for wellness applications would cover applications that process personal health data only for reasons related to the delivery of healthcare. This is significantly narrower to the Commission's proposal suggesting that wellness apps in scope are the ones processing health data for reasons such as 'wellbeing and pursuing healthy lifestyles'.

BEUC recommendation:

- Co-legislators should follow the definition of 'wellness applications' proposed by the European Parliament in Article 2(2)(a ea-new).

2. Primary use of health data

2.1 Right to receive a physical copy

Consumers should be able to receive a physical copy of their Electronic Health Record (EHR) upon their request. This is important for people with low levels of digital literacy and access, such as elderly people and people who do not own smartphones or computers.

BEUC recommendation:

- Co-legislators should follow the Parliament's position in Article 3(2), allowing people to receive a printed copy of their EHR upon their request.

2.2 Right to object & to exercise access restrictions in electronic health records

[4] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products, COM/2022/495 final, accessible here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A495%3AFIN.

Consumers should be able to exercise granular access restrictions to their personal health data. This would empower them for instance to restrict access to specific categories of health data (for example, such as lab results), or to decide they do not wish to share it with specific or entire categories of healthcare professionals.

This is important as consumer willingness to share their health data depends on the level of trust consumers place in different entities, according to a recent BEUC survey.[5] Therefore, consumers are for instance most open to sharing their health data with their general practitioners (88%), whereas only 28% of respondents were willing to share it with pharmacists.

Moreover, the Parliament's position ensures that the restrictions exercised are not visible to the healthcare professional in question, granting consumers a higher level of privacy. This can be particularly significant for people living in smaller communities.

BEUC recommendation:
- Co-legislators should follow the Parliament's position in Article 3(9), allowing people to exercise granular access restrictions to their EHRs.

2.3 Automatic notifications

As proposed by the European Parliament, consumers should be informed in real-time when their EHRs are accessed. Such a measure would ensure consumers are empowered to manage their health data. To achieve this, consumers should be able to receive automatic notifications, for example through emails or notifications on their smartphone applications.

BEUC recommendation:
- Co-legislators should follow the Parliament's position in article 3(10), foreseeing the possibility to receive automatic notifications when their EHRs are being accessed.

2.4 Access by health professionals to personal electronic health data

To respect consumers' privacy and protect their personal health data, their EHRs should only be accessed on a need-to-know basis and following specific access rules.

As included in the Parliament's provision, Article 4(1) should explicitly mention the GDPR data minimisation and purpose limitation principles. Moreover, Article 4(2) should oblige Member States to establish rules on the categories of health data accessible per different categories of health professions or healthcare tasks.

BEUC recommendation:
- Co-legislators should follow the Parliament's position in Article 4(1) – (2).

2.5 Right to object

Consumers should have a right to object to the registration of their personal health data in an EHR System, as suggested in the Parliament's text. While it would be up to Member States to decide whether to grant such a right, it is important to ensure that countries with national health systems foreseeing such rights are able to keep those mechanisms in place. This will allow consumers the freedom to manage their health records according to their wishes. Given that consumers' health data would be registered and linked to an EHR system by default, this right is important to ensure consumer choice.

[5] Accessible here: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-051_consumer_attitudes_to_health_data.pdf.

BEUC recommendation:
- Co-legislators should follow the Parliament's position in Article 7(1 a).

3. EHR Systems Conformity Assessment & Wellness Applications in Primary Use

3.1 EHR Systems Conformity Assessment

BEUC welcomes the European Parliament's position to subject EHR systems to third party conformity assessment and introduce notified bodies for this purpose. EHR systems will be storing extremely sensitive datasets, creating very high risks of cyberattacks. This fear is well-founded given a recent ENISA report, showing that the frequency and sophistication of cybercrime on critical infrastructure in the health sector is increasing steeply. But the Council's position would water down an already weak Commission proposal on this matter, as certain components of the EHR systems would not even be assessed at EU level.

As regards the criteria against which the conformity of the EHR Systems will be assessed, we recommend that co-legislators follow the provision of Article 23 of the European Parliament's position. When drafting common specifications, the Commission should be able to take existing standards into account but must not be obliged to follow them. Moreover, the European Data Protection Board and the European Data Protection Supervisor should be consulted before adopting common specifications having an impact on data protection, as suggested in the Parliament's position (Article 23 (4a)).

BEUC recommendation:
- Co-legislators should follow the Parliament's position in Chapter III and Section III of this Chapter in particular.

3.2 Interoperability of wellness applications with EHRs.

We are concerned about the security and privacy implications that could arise from connecting wellness applications to EHRs. To ensure the highest level of consumer protection, we urge co-legislators to subject interoperable wellness applications to a mandatory labelling system, as the one proposed in Article 31 of both the Council's and the Parliament's position. Moreover, in this case, market surveillance authorities, which will also be competent to check the compliance of wellness apps with, shall also be informed once the label has been issued, according to Article 31(1) of the Parliament's mandate.

Most importantly, we recommend following also Article 31a of the Parliament's position. The ability to connect one's EHR to wellness applications should not mean automatic transmission of data from the app to the EHR. Such transmission should be strictly limited to the situations where the consumer has provided their consent, as per Article 4(11) of the GDPR. Consumers' consent would need to be freely given, informed, specific and unambiguous, while the deployment of dark patterns that infringe on GDPR requirements should be strictly forbidden.

BEUC recommendation:
- Co-legislators should subject interoperable wellness apps to a mandatory labelling scheme, following the Parliament's position in Articles 31 and 31a.

4. Secondary Use

4.1 Right to opt-out from Chapter IV

BEUC welcomes the European Parliament's position to introduce a right to opt-out of the processing of their electronic health data for secondary use (Article 33(5)). This is crucial to ensure that consumers are enabled to exercise their choice when sharing their health data for secondary purposes. The willingness to share health data depends on the type of data, the entity in question and the purpose as well which requires a more granular approach.

According to a recent BEUC survey, the majority of consumers are against sharing their health data with entities that are not directly involved in their healthcare provision. Allowing national governments to take this decision at national level, following the Council's position, may create considerable discrepancies on how consumers can exercise their choice and rights across different Member States.

BEUC recommendation:

- Co-legislators should follow the Parliament's position in Article 33(5).

4.2 Minimum Categories of data to be shared for secondary use.

We are concerned about the possible implications from certain categories of health data being shared for secondary use. The categories of health data available for secondary use and the exact purposes foreseen in that context must be clearly delineated to enhance consumers' trust in the EHDS. For that purpose, strong safeguards need to be installed ensuring that consumers' privacy is respected.

Regarding the health data categories in scope for secondary uses, Article 33 of the Council's position contains vague wording such as *"other administrative data relating to an individual's socioeconomic status"* (Article 33(1)(d)), which risks expanding the scope to data that reveals a lot about consumers but has little relevance for scientific health research.

Co-legislators also need to be mindful of the possible implications and discrimination risk that could arise from the inclusion of genetic and other types of genomic data, which cannot be effectively anonymized. This poses a high risk of a person being re-identified which reveals information not only about the individual but also for all their blood relatives. Similarly, person-generated data from medical devices and wellness apps can reveal a lot about individuals, especially when combined with genetic and medical data from other sources.

For those reasons BEUC urges co-legislators to follow the European Parliament's position in Article 33, making genetic data and person-generated data from wellness applications subject to consumers' prior consent (Article 33(5a)). An opt-in clause for those extremely sensitive types of health data, would ensure that they are not made available for secondary uses by default. Instead consumers are empowered to decide themselves, striking the right balance between the needs of the research community and the rights of consumers to determine themselves what happens to their health data.

BEUC recommendation:

- Co-legislators should follow the Parliament's position so that:
    - Genetic data, data from biobanks and person-generated data from wellness apps are made available for secondary use upon consumers' consent,

understood per Article 4(11) of the GDPR, according to Article 33(5a) of the Parliament's position.

- The categories of health data in scope are circumscribed (in Article 33(1)), and vague language is avoided.
- Article 33(1)(n) of the Commission's Proposal referring to *'electronic data related to insurance status, professional status, education, lifestyle, wellness'*, and article 33(1)(d) of the Council's position referring to *'other administrative data relating to an individual's socioeconomic status'* are deleted.

4.3 Purposes for Secondary uses

While the use of health data for secondary purposes can contribute to valuable research and improve decision-making in the health sector, it might have unintended consequences for consumers' privacy and personal data protection if the EHDS is not well designed.

Access to patient data for overly vague, broad and potentially intrusive purposes such as *'innovation activities', 'training, testing and evaluating of algorithms'* and *'treatment optimisation'* pose a high risk of abusing consumer data to generate commercial profit without safeguards or without delivering concrete benefits for consumers. For example, in relation to training AI algorithms, there is an inherent risk that they will be biased, leading to false scientific conclusions and perpetuating health inequalities. Moreover, our survey shows consumers are against sharing their health data with entities that are not directly involved in their healthcare provision, such as companies developing wellness apps and digital technology companies (92%).

Although we regret to see that those purposes remain part of both institutions' positions, we are glad to see that the Parliament takes a more cautious approach. This proposes that 'innovation and development activities' and 'training, testing and evaluating of AI algorithms' are allowed insofar as they can be classified as scientific research, benefitting end-users such as patients. This more restrictive approach would subject data access applicants to more stringent criteria, when compared to the Commission proposal.

Finally, purposes for secondary use allowed pursuant to the EHDS should be defined as clearly as possible to safeguard consumers' privacy. In the case of Article 34(1)(h) that refers to 'personalised medicine' the Commission's proposal would provide the highest level of consumer protection, as it is more descriptive.

BEUC recommendation:
- Co-legislators should follow the Parliament's position in Article 34(1)(e).
- Co-legislators should follow the Commision proposal text in Article 34(1)(h).

4.4 Prohibited uses

We are glad to see that both the Council and the Parliament have clarified the interplay between Article 34 and 35, regarding the permissible and prohibited secondary uses, while also expanding the list of prohibited uses. The Parliament's position in Article 35(1a) brings, however, more clarity, as it explicitly mentions that *'any secondary use of electronic health data for purposes other than those referred to in Article 34 shall be prohibited.'*

As regards the list of practices for which an entity cannot gain access, we urge co-legislators to reach a compromise including provisions from both texts, which would ensure the highest level of consumer protection.

BEUC recommendation for a compromise on Article 35:

Any secondary use of electronic health data for purposes other than those referred to in Article 34 shall be prohibited.

Health data users shall be prohibited to access, process or use electronic health data ~~obtained via a~~ ***outside the scope of the*** data permit issued ***pursuant to Article 46 or data request*** pursuant to Article ~~46~~***47 or for any of*** the following purposes

(a) taking decisions detrimental to a natural person ***or a group of natural persons*** based on their electronic health data; in order to qualify as "decisions", they must produce legal***, social or economical,*** effects or similarly significantly affect those natural persons;

(b) taking decisions in relation to a natural person or groups of natural persons ***in relation to job offers or offering less favourable terms in the provision of goods or services, including*** to exclude them from the benefit of an insurance, ***such as life assurance contract or a policy of health insurance or health-related insurance or credit*** contract or to modify their contributions and insurance premiums ***or conditions of loans, or taking any other decisions in relation to a natural person or groups of natural persons having the effect of discriminating on the basis of the health data obtained;***

(c) advertising or marketing activities ~~towards health professionals, organisations in health or natural persons~~***~~, with the exception of public health messaging by competent public sector bodies~~***~~;~~

(d) providing access to, or otherwise making available, the electronic health data to third parties not mentioned in the data permit;

(e) developing products or services that may harm individuals, ***public health or*** societies at large, including, but not limited to illicit drugs, alcoholic beverages, tobacco ***and nicotine*** products, ***weaponry or products*** or services which are designed or modified in such a way that they ***create addiction or that they*** contravene public order or morality;

(f) automated individual decision-making, including profiling, in accordance with Article 22 of the Regulation (EU) 2016/679, whether solely on the basis of the datasets shared under this Regulation or in combination with other data.

(g) activities in conflict with ethical provisions pursuant to national law;

4.5 Information provision

It is important to ensure that Article 14 of the GDPR is applicable regarding the provision of specific information from Health Data Access Bodies to people when their pseudonymised data is being processed, as has been suggested in the Parliament's mandate.

BEUC recommendation:
- Co-legislators should follow the Parliament's position and delete Article 38(2).

4.6 Single Health Data Holders

Bypassing Health Data Access Bodies to receive data access permits issued from single health data holders should not be an option under the EHDS Regulation, as proposed in the Parliament's position. Health Data Access Bodies, in their competence of assessing data access permits and applying anonymisation and pseudonymisation criteria, are the main safeguards protecting consumers' sensitive health data. Allowing single data holders to directly issue access permits and data holders to perform those tasks themselves would significantly water down the level of protection afforded to consumers.

BEUC recommendation:
- Co-legislators should follow the Parliament's position and delete Article 49.

5. Specific rights for consumers & Enforcement

5.1 Right to an effective judicial remedy

Consumers must be enabled to better enforce their rights under the EHDS Regulation, as suggested in the Parliament's mandate. This includes the introduction of a right to lodge a complaint with the Health Data Access Body, shall their rights under Chapter IV be infringed. This has been already been included in Article 11 of the Commission proposal, regarding Digital Health Authorities.

Moreover, the Parliament's position foresees additionally the right to an effective judicial remedy against a digital health authority (Article 11a) and a health data access body (Article 38b). This would mean in practice that consumers would be allowed to bring an action to court against the legally binding decision of a digital health authority or in case they lodged a complaint that went unanswered.

BEUC recommendation:
- Co-legislators should follow the Parliament's position and introduce:
    - a right to lodge a complaint with Health Data Access Bodies (Article 38a).
    - a right to an effective judicial remedy against legally binding decisions of Digital Health Authorities (Article 11a) and Health Data Access Bodies (Article 38b).

5.2 Right to compensation and access collective redress

Consumers should have a right to receive compensation and be allowed to use existing collective redress mechanisms. By annexing the EHDS to the Representative Actions Directive,[6] qualified entities can represent consumers collectively and ask for injunctions and collective redress for consumers in case their rights are infringed. This is crucial for consumer protection, given the power and information asymmetry at stake.

[6] Representative Actions Directive (EU) 2020/1828.

BEUC recommendation:

- Co-legislators should follow the Parliament's position regarding specific consumer rights and:
  - introduce a right to receive compensation (Article 69a),
  - a right to mandate a not-for-profit body to represent them in case their rights have been infringed (Article 69b)
  - annex the EHDS Regulation to the Representative Actions Directive (Article 71a).

5.3 Administrative Fines

Health Data Access Bodies must be competent to impose administrative fines if the regulation is infringed (Article 43a).

Infringing the EHDS regulation should not be without penalties. This is why administrative fines should apply cumulatively with administrative measures (for example to revoke permits for data users, or exclude data holders from placing data access applications), if data holders or data users breach their obligations. This was not originally foreseen in the Commission's proposal. The Parliament's position introduces a new article foreseeing benchmarks per type of infringement and detailed criteria that should be weighed in by Health Data Access Bodies when deciding on the fines. This will ensure that fragmentation across Member States is being avoided and will maximise safeguards for consumers.

BEUC recommendation:

- Co-legislators should follow the Parliament's position and include Article 43a in the final text of the Regulation, which allows Health Data Access Bodies to impose administrative fines.

[END]

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.