Brussels, 22 September 2026

Joint Statement on protecting patient data in the Digital Omnibus

European organisations representing patients, doctors, nurses, community and hospital pharmacists, hospitals and healthcare services, consumers, older people, health insurance funds and not-for-profit health mutuals (*to be adapted depending on the signatories)* call on legislators to ensure that the Digital Omnibus does not weaken the protection of patients' personal data.

Digitalisation can support better healthcare, safer medicines use, innovation and more accessible services. However, simplification must not come at the expense of fundamental rights, patient confidentiality, professional secrecy or trust in healthcare. Health-related data are among the most sensitive categories of personal data. They can reveal intimate information about a person's physical or mental health, treatment, medicines use, disability, vulnerability or life circumstances. This includes not only data explicitly labelled as health data, but also data inferred from searches, purchases, online consultations, pharmacy interactions, use of medicines-related websites, wearables, apps or connected services.

We call upon the co-legislators to:

1. **Preserve the specific protection of health data in the digital environment**

The Digital Omnibus must not introduce broad exceptions that weaken the protection of health, genetic or biometric data, including information from which a person's health status may be inferred. Such data should only be processed where there is a clear and specific legal basis and all relevant safeguards under Article 6 and Article 9 of the General Data Protection Regulation (GDPR) are met. These safeguards must continue to apply when patient data are used in digital services, AI systems or research. Any derogation or simplification measure should clearly exclude health-related data unless processing is expressly authorised by Union or Member State law, subject to robust safeguards, clear liability rules and effective supervision. The Digital Omnibus must not weaken professional secrecy, including the legal and professional duties of confidentiality owed by healthcare professionals to their patients.

2. Ensure that AI development does not bypass safeguards for the use of patient data

AI can bring important benefits to healthcare, but trust in the deployment of AI will depend on strict respect for patients' rights. General rules intended to support AI development should not allow the incidental or secondary use of patient or health-related data without appropriate safeguards and comprehensive information to patients.

Where health data or inferred health data are involved, processing should require a specific legal basis, documented necessity and proportionality and effective measures preventing re-use for profiling, advertising, commercial targeting or unrelated commercial purposes.

Developers and providers of AI systems and other digital health technologies should remain accountable for ensuring that patient data processed through their products are protected in accordance with the GDPR. The Digital Omnibus should not transfer or dilute this responsibility.

3. Protect patients from tracking, profiling and commercial exploitation

Searches, visits and purchases on medicine-, pharmacy- or health-related websites can reveal or allow the inference of health conditions. Patients should not have to choose between accessing healthcare information and preserving their privacy online.

Audience measurement should use anonymous data, be strictly purpose-limited and remain clearly separated from behavioural advertising, personalised advertising, customer segmentation, profiling or the inference of health status. Where processing involves personal data, online identifiers, cross-service tracking or the potential to make health-related inferences, it should require the data subject's consent and must not be misrepresented as technical measurement, service improvement or scientific research to avoid obtaining consent.

4. Maintain strong safeguards for pseudonymised health data

Pseudonymisation is an important security measure, but it does not automatically make health data untraceable. Health-related datasets may remain capable of being linked to an individual, particularly when combined with other data sources or analysed through advanced linkage and inference techniques.

Pseudonymised health, genetic and biometric data, including data from which health-related information may be inferred, should not be presumed to be anonymous or treated as no longer constituting personal data. Any amendments introduced through the Digital Omnibus should remain consistent with the European Health Data Space and should not weaken its safeguards for the primary or secondary use of personal electronic health data.

In particular, access to electronic health data for secondary use for AI development must comply with the specific limitations in Article 53(1)(e) of the EHDS, which permits such access only as part of scientific research related to the health or care sectors and subject to the EHDS safeguards.

Treating pseudonymised data as not necessarily constituting personal data risks creating legal uncertainty in healthcare and significantly weakening the data-protection safeguards on which the EHDS is built.

At the same time, pseudonymised data and robust pseudonymisation methods are important for cross-sectoral health research. The possibilities for GDPR-compliant merging and AI-supported analysis of pseudonymised health data for public-benefit research should therefore be maintained and further developed.

5. Preserve the right not to be subject to automated decision-making and ensure meaningful human oversight in healthcare

The right not to be subject to automated decision-making in Article 22 GDPR should be reinstated, and automated decision-making systems, including AI, should not determine access

to, recommendation, pricing or marketing of medicinal products or pharmacy services without appropriate human review and oversight. Where decisions may significantly affect patients and their health, individuals must have access to meaningful human oversight, clear explanations, and healthcare professionals' support, thus guaranteeing that the information is clearly understood by patients. There should also be a clear liability framework for automated decision-making using AI.

We highlight the importance of preserving patient agency and reaffirm the central role of the patient-healthcare professional relationship in ensuring that decisions concerning a patient's health are balanced, informed and grounded in established medical expertise.

Data concerning health or inferred health status should not be used for such decisions without explicit consent or another specific legal basis under Article 9 of the GDPR.

6. Support innovation without weakening fundamental rights

The signatories support digital innovation that improves healthcare, strengthens patient safety and supports healthcare professionals. However, innovation in healthcare must be built on trust. Weakening privacy, confidentiality or data protection would undermine patients' willingness to use digital services and share information with healthcare professionals.

In particular, legislators should ensure a clear distinction between scientific research in the public interest and activities that primarily pursue commercial or business objectives. The concept of scientific research should not be expanded in a manner that weakens existing safeguards for health-related data or facilitates their use for commercial purposes.

The Digital Omnibus should streamline requirements where they do not add value to patient safety or where they stifle meaningful, patient-centred innovation, but not where this would reduce the protection of sensitive health data, enable commercial exploitation or blur the distinction between healthcare, advertising and profiling, or weaken the distinction between scientific research and commercial data use.

We urge the European Parliament and the Council to ensure that the Digital Omnibus preserves the protections provided by the GDPR and ePrivacy framework as a cornerstone of patient trust, public health and responsible digital innovation in Europe.

*The **International Association of Mutual Benefit Societies (AIM)** is a global network for equitable health and social care, which serves as the international umbrella organisation for federations of health mutuals and statutory and complementary health insurance bodies. The work of our members is based on solidarity, not-for-profit work and democracy across Europe, Latin America, Africa, and the Middle East. We advocate for equal access to health and care, fair pricing of medicines, a digitalization that serves the insured, the integration of health in all policies and a stronger focus on prevention.*

*The **European Consumer Organisation (BEUC)** is the largest organisation promoting the general interests of Europe's consumers. Founded in 1962, it proudly represents more than 40 independent national consumer organisations from over 30 European countries.*

*The **Council of European Dentists (CED)** is a European not-for-profit association which represents over 350,000 dentists across Europe. The association was established in 1961 and is now composed of 32 national dental associations from 30 European countries.*

*The **Standing Committee of European Doctors (CPME)** represents national medical associations across Europe, covering more than 1.7 million doctors in 36 countries.*

*The **European Association of Hospital Pharmacists (EAHP)** represents and develops the hospital pharmacy profession across 37 European member countries to ensure the continuous improvement of care and outcomes for patients in the hospital setting. This is achieved through science, research, education, practice, and sharing best-practice and responsibility with other healthcare professionals.*

*The **European Federation of Nurses Associations (EFN)** is a European not-for profit association representing 38 national nurses associations and represents as such over 3 million EU Nurses.*

*The **European Patients' Forum (EPF)** is an umbrella organisation of patient organisations across Europe and across disease-areas. Our 81 members include disease-specific patient groups active at EU level and national coalitions of patients.*

*The **European Hospital and Healthcare Federation (HOPE)** is a European organisation, representing 36 national public and private hospital and healthcare associations and hospital, health and social care services owners from the 27 Member States of the European Union, the United-Kingdom, Switzerland and the Republic of Serbia. HOPE mission is to promote improvements in the health of citizens, fostering efficiency, effectiveness and humanity in the organisation and operations of hospital and health services.*

*The **Pharmaceutical Group of the European Union (PGEU)** is the organisation representing community pharmacists in 33 European countries. In Europe over 500.000 pharmacists provide services throughout a network of more than 200.000 pharmacies.*