New obligation to make health data available to third parties: issues with protected data

This paper explores the new obligation to make health data available to third parties in light of the Regulation of the European Parliament and of the Council on the European Health Data Space.

ÁNGEL GARCÍA VIDAL
Professor of Corporate & Commercial Law, University of Santiago de Compostela
Academic counsel (external adviser), Gómez-Acebo & Pombo

1. Preliminary remarks

The Regulation of the European Parliament and of the Council on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (the 'Regulation') - adopted on 21 January 2025 by the Council of the European Union and still pending formal signature (by both the said Council and the European Parliament) and publication in the Official Journal of the European Union— has two main pillars: first, the Regulation aims to facilitate patients' access to their health data and to promote its transmission, even across borders; and, second, it deals with the use of health data for purposes other than the treatment of the person to whom it belongs, such as research, public health, etc. A primary and a secondary use of health data are therefore regulated.

In relation to the secondary use of data, the Regulation requires holders of a series of health data to make them available to third parties who intend to make a permitted secondary use; failure to comply with this obligation will be sanctioned (Art. 64(4)) with

fines of up to ten million euros or, in the case of a company, of an amount equivalent to a maximum of 2% of its total worldwide annual turnover in the preceding financial year, whichever is higher.

This new obligation raises significant doubts and questions when the holders of such data have some legal mechanism for protecting them. It is necessary, first, to determine to which data the obligation to make them available to third parties applies and when this obligation operates; second, to remember what type of regulatory protection some of these data may have; and, third, to examine the mechanisms established in the Regulation to reconcile the aforementioned data protection with the obligation to supply to third parties.

2. The obligation of health data holders to make their data available to third parties for secondary uses permitted in the Regulation

2.1. *Data affected by the obligation to make data available*

The obligation to make data available affects a wide range of electronic data types listed in Article 51 of the Regulation, namely:

a) electronic health data from electronic health records (EHRs);

b) data on factors impacting on health, including socio-economic, environmental and behavioural determinants of health;

c) aggregated data on healthcare needs, resources allocated to healthcare, the provision of and access to healthcare, healthcare expenditure and financing;

d) data on pathogens that impact human health;

e) healthcare-related administrative data, including on dispensations, reimbursement claims and reimbursements;

f) human genetic, epigenomic and genomic data;

g) other human molecular data such as proteomic, transcriptomic, metabolomic, lipidomic and other omic data;

h) personal electronic health data automatically generated through medical devices;

i) data from wellness applications;

j) data on professional status, and on the specialisation and institution of health professionals involved in the treatment of a natural person;

k) data from population-based health data registries such as public health registries;

l) data from medical registries and mortality registries;

m) data from clinical trials, clinical studies, clinical investigations and performance studies;

If protected, access to data may be denied

n) other health data from medical devices;

ñ) data from registries for medicinal products and medical devices;

o) data from research cohorts, questionnaires and surveys related to health, after the first publication of the related results;

p) health data from biobanks and associated databases.

In addition, the Regulation allows Member States to provide in their national law that additional categories of electronic health data are to be made available for secondary use.

Consequently, the obligation to share health data in the context of secondary use affects the holders of this type of data, such as, for example, entities that are healthcare providers or care providers or carry out research with regard to the healthcare or care sectors, or develop products or services intended for the healthcare or care sectors (including, among others, legal persons developing wellness applications). And all these organisations, as stated in the explanatory notes to the Regulation (para. 59), can be "public, not for profit or private".

2.2. *Cases in which the obligation to make data available applies*

In accordance with the new Regulation, applications for access to data for secondary use will be submitted to the relevant national authority. To this end, it is provided that each Member State will designate one or more health data access bodies, which will be responsible for granting access to electronic health data for secondary use.

Any natural or legal person may submit a health data access application to an access body so that, if the application meets all the requirements of the Regulation and is approved by the access body, the latter will request that it be delivered to the data holder.

In any case, access to the data will only be possible when the secondary uses for which it is requested meet the purposes established in the Regulation (Art. 53). Thus, when the applicants are public sector bodies and Union institutions, bodies, offices and agencies exercising the tasks conferred on them by Union or national law, they will be granted access when the use of the data is in the public interest in the areas of public or occupational health; for policy-making and regulatory activities to support public sector bodies or Union institutions, bodies, offices or agencies, in the health or care sector to carry out their tasks defined in their mandate; or for the production of statistics, such as national, multi-national and Union-level official statistics, related to health or care sectors.

In addition, any individual and public sector bodies may access the data for secondary use in the context of the following activities:

a) education or teaching activities in health or care sectors at vocational or higher education level;

b) scientific research related to health or care sectors that contributes

to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators; or

c) the improvement of the delivery of care, of the optimisation of treatment and of the provision of healthcare, based on the electronic health data of other natural persons.

In any case, the secondary use of data for advertising or marketing purposes to take decisions that negatively affect a person or group (for example, to exclude them from the benefit of an insurance contract), as well as to develop harmful products or services (with express mention of 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, contravene public order or cause a risk for human health).

2.3. *Conditions for making data available*

Data holders shall make the requested data available to the health data access body within a reasonable period of time and no later than three months from the receipt of the request by the data access body. In justified cases, the health data access body may extend this period by a maximum of three months.

Subsequently, once received, the health data access body will make the data available to the person who applied for it (the so-called health data user). In this regard, it is provided that access bodies will provide users with access to health data only through a secure processing environment which is subject to technical and organisational measures and security and interoperability requirements. The security measures to be complied with include, among others, the restriction of access to authorised natural persons; the minimisation of the risk of unauthorised reading, copying, modification or removal of health data through state-of-the-art technical and organisational measures; and ensuring that data users have access by means of individual and unique user identities and confidential access modes only.

As a general rule, the data will be provided in an anonymised format (Art. 66). However, if the purpose for which the data is requested cannot be achieved with anonymised data, health data access bodies will provide access to electronic health data in pseudonymised format. The information necessary to reverse the pseudonymisation will be available only to the health data access body, so that the data users cannot re-identify the electronic health data provided to them in pseudonymised format.

On the other hand, there is no obligation for this data to be made available free of charge. In fact, it is expressly provided (Art. 62) that fees may be charged, which shall be in proportion to the cost of making the data available and shall not restrict competition. The health data access bodies will be the ones to set the amount of these

fees, which may include "compensation for the costs incurred by the health data holder for compiling and preparing the electronic health data to be made available for secondary use", as provided for in Article 62(2), which also states that the "part of the fees linked to the health data holder's costs shall be paid to the health data holder", which means - as clarified in paragraph 70 of the explanatory notes - that the "health data user ought to be charged such fees by the health data access body in a single invoice. The health data access body should then transfer the relevant part of the paid fees to the health data holder".

3. The protection that the data to be made available to third parties may have

Much of the data that, as explained above, the holders have to make available to the access body so that it, in turn, can deliver it to the third party applicants, may enjoy protection under other legal rules.

Firstly, they may be protected as a trade secret, in accordance with Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (and in Spain, according to the Business Secrets Act 1/2019 of 20 February).

Secondly, the set of data made available may be subject to the sui generis right on databases, by virtue of which protection is afforded to databases which, without being considered a work protectable by intellectual property, have involved a substantial investment (assessed qualitatively or quantitatively), either of financial resources, or of use of time, effort, energy or similar for the obtaining, verification or presentation of their content (Art. 7 of Directive 96/9/EC on the legal protection of databases and Art. 133(1) of the Copyright Act). Although, as provided in Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Art. 43), the sui generis right shall not apply when the data is obtained or generated by a connected product ("an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user") or related service.

Thirdly, the data may form part of an invention protected by industrial property rights. And, finally, the data may enjoy the period of exclusivity recognised in Directive 2001/83/EC on the Community code relating to medicinal products for human use (Art. 10); in Regulation (EC) No. 726/2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency (Art. 14(11)), and in the Medicine and Healthcare Product Guarantees and Rational Use Act (Art. 17). This period of exclusivity complies with the obligation laid down in Article 39(3) of the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights, according to which members, "when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall

protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use". Consequently, in accordance with EU legislation, during this period of protection of test data by means of an exclusive right, the generic drugs industry has two alternatives: either to wait for the data protection period to elapse, or to repeat all the trials and tests again.

4. Data protection under the Regulation

Despite the possible protection of health data by one of the above means, such data must also be made available to third parties for secondary uses, in accordance with the aforementioned provisions of the Regulation. Therefore, the data holders may not refuse to provide it on the grounds that it is protected data. This is made abundantly clear in Article 52(1) of the Regulation, which states that electronic "health data protected by intellectual property rights, trade secrets or covered by the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC of the European Parliament and of the Council35 or Article 14(11) of Regulation (EC) No 726/2004 of the European Parliament and of the Council36 shall be made available for secondary use in accordance with the rules laid down in this Regulation". However, the Regulation seeks to reconcile data protection with making data available to third parties by establishing a series of measures set out in Article 52:

a) Firstly, when the health data access body requests protected data from a data holder, the holder shall inform the body about such protection, identifying which parts of the datasets are concerned and justifying the need for specific protection of the data to be communicated.

b) Once the protected data has been identified, the Regulation stipulates that the health data access bodies shall "take all specific appropriate and proportionate measures, including of a legal, organisational and technical nature, they deem necessary to protect the intellectual property rights, trade secrets or the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) 726/2004". And, immediately afterwards, the Regulation insists that health data access bodies shall "remain responsible for determining whether such measures are necessary and appropriate". As can be seen, it is an open and indeterminate clause that requires a case-by-case approach. But it is very significant that it is stipulated that all possible measures will be taken to safeguard data protection and, furthermore, that these measures must be appropriate for achieving this end.

In the same vein, Article 57 of the Regulation emphasises once again that the tasks of health data access bodies include "taking all measures necessary to preserve the confidentiality of intellectual property rights, for regulatory data protection and to preserve the confidentiality of trade secrets as provided for in Article 52, taking into account the relevant rights of both the health data holder and health data user". However, this is not well-worded because intellectual property rights are not confidential (suffice it to say, for example, that patents or supplementary protection certificates are subject to public registration).

Starting from this broad and indeterminate premise of the measures

to be adopted, the Regulation expressly recognises (in Article 52(4)) that health data access bodies may make the access to certain electronic health data conditional on legal, organisational and technical measures, which may include contractual arrangements between health data holders and health data users for the sharing of data containing information or content protected by intellectual property rights or trade secrets. And it is provided that the Commission will develop and recommend non-binding models of contractual terms for such arrangements.

Furthermore, paragraph 60 of the explanatory notes to the Regulation refers to a specific measure that can be taken to protect trade secrets, namely: "pre-processing the data to generate derived data that protect a trade secret but nonetheless have a utility for the health data user or configuration of the secure processing environment so that such data are not accessible to the health data user".

c) However, it cannot be ruled out that there will be cases in which no technical, legal or organisational measure is sufficient to achieve appropriate protection of the aforementioned data rights. For this reason, the Regulation itself stipulates that, where "the granting of access to electronic health data for secondary use entails a serious risk of infringing intellectual property rights, trade secrets or the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) No 726/2004 which cannot be addressed in a satisfactory manner, the health data access body shall refuse access to the health data applicant to such data. The health data access body shall inform the health data applicant of, and provide to the health data applicant a justification for, that refusal".

5. The obligation to publish the results obtained from secondary use

As can easily be understood from the above, people who, in accordance with the new Regulation, access health data held by another person for secondary uses obtain a clear advantage, justified in the explanatory notes, because electronic "health data protected by intellectual property rights or trade secrets, including data on clinical trials, investigations and studies, can be very useful for secondary use and can foster innovation within the Union for the benefit of Union patients".

Precisely as a way of avoiding undue exclusive advantage, the Regulation (Art. 61) requires that health data users - in addition to acknowledging the sources of the electronic health data and the fact that they have been obtained in the framework of the European Health Data Space - make public the results or output of secondary use, including information relevant for the provision of healthcare, within 18 months - which may be extended where justified - of the completion of the processing of the electronic health data in the secure processing environment or of having received the response to the health data request.

To this end, health data users shall inform the health data access bodies from which a data permit was obtained about the results or output of secondary use and assist them to make that information public on health data access bodies' websites. Such publi-

cation shall be without prejudice to publication rights in scientific journals or other scientific publications. But, in any case, the results or output of secondary use shall contain only anonymous data.

Furthermore, health data users shall inform the health data access body of any significant finding related to the health of the natural person whose data are included in the dataset.