European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 177-185
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 13

*Primary Use of Data in the European Health Data Space Proposal: Its Impact on National Electronic Health Records from a Spanish Perspective**

Andrea Salud Casanova Asencio
(PhD. Assistant Professor of Civil Law at University of Murcia)

María Belén Andreu Martínez
(Full Professor of Civil Law at University of Murcia)

ABSTRACT ***The European Health Data Space represents an important advance in the context of the European Data Strategy, among other issues, in relation to the promotion of the rights of natural persons regarding the primary use of their health data, a matter in which it offers some novel solutions. The Proposal for a Regulation published in 2022, and currently in the process of being discussed, provides for a series of rights that, in practice, require a new configuration in the national medical records system of Member States such as Spain, which serves as a reference in this study.***

1. *Introduction*

The European Health Data Space (EHDS) constitutes the first data space proposal within the framework of the European Data Strategy.[1] The basic purpose of the EHDS is to create a health data exchange mechanism within the EU, establishing a series of rules, standards, common practices, infrastructure and a governance framework for the primary and secondary use of electronic health data. The regulation contained on primary use[2] is the one likely to have the greatest impact on the configuration of national medical records. In relation to primary use, the basic objectives of the EHDS and the Proposal for a Regulation of the EHDS (which will subsequently be referred to as "the Proposal") are to:

1) Strengthen natural person's control over their health data.
2) Establish standards specifications for Electronic Health Records (EHR) systems.
3) Create a mandatory cross-border infrastructure for primary use of data.

The impact of these measures at the European level is clear, with the creation of instruments that must be available at a supranational level, as is the case with mandatory cross-border infrastructure for primary use. However, many of the provisions envisaged have a no less important effect on the internal legal systems of the Member States; and, in particular, the measures established to promote the rights of natural persons in relation to their health data have the potential to require important reforms in this regard. We will focus on these issues in the following pages, taking as a reference, in particular, the Spanish system.

2. *Configuration of medical records in the Spanish health system*

In the Spanish case, the medical record system is complex, since competence in health matters is shared between the State and the autonomous regions known in Spain as Autonomous Communities (CCAA), and the management of public health care corresponds to the health services of the CCAA. This has

* Article submitted to double-blind peer review.

[1] See European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European strategy for data", COM(2020) 66 final, 2020. Accessible here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066.
See also, in general, D. Horgan, M. Hajduch, M. Vrana, J. Soderberg, N. Hughes, M.I. Omar, J. A. Lal, M. Kozaric, F. Cascini, V. Thaler *et al*, *European Health Data Space – An opportunity now to grasp the future of data-driven healthcare*, in *Healthcare*, no. 10, 2022, 1629, accessible here: https://www.mdpi.com/2227-9032/10/9/1629.

[2] Which is defined in the Proposal as "the processing of personal electronic health data for the provision of health services to assess, maintain or restore the state of health of the natural person to whom that data relates, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social security, administrative or reimbursement services" (Art. 2.2.d).

given rise to the existence of eighteen health systems in Spain, each with its own model and medical record infrastructure.

The regional systems are, as of today, highly digitalized, although the regulation to develop said digitalization is scarce.[3] The high degree of digitalization offers great functionalities in the use of medical records, especially to professionals, but also to patients (through the different patient care web portals of the different health systems). However, access to these digitized medical records from the CCAA is in principle designed for the scope of the CCAA itself, so if the patient travels to other places in Spain, said information is not accessible neither to the patient nor to the health professionals.

In view of the above, the Digital Medical Record of the National Health System, known in Spanish as "Historia Clínica Digital del Sistema Nacional de Salud" (HCDSNS) was promoted, at a national level, by the Spanish Ministry of Health (in collaboration with the Autonomous Communities). Its purpose was to make available to citizens their existing health data (and those of other natural persons represented by them) in digital format in one of the regional health services, as well as to allow health professionals to access a set of relevant data generated in health services of other Autonomous Communities. This was intended to alleviate the problem derived from the lack of access to these data when a person traveled to another Autonomous Community in Spain.[4] Currently, the HCDSNS allows the Autonomous Communities to share relevant clinical information about their citizens so that it is available in electronic format in any regional service at the request of citizens.[5] The clinical information that can be shared is the following: Patient Summaries, known in Spain as "Historia Clínica Resumida" (HCR), that is, Summary Medical Records; Primary Healthcare Reports; Emergency Room Reports; Discharge Reports; External Surgery Reports; Laboratory Test Results Reports; Imaging Test Results Reports; Results of other Diagnostic Tests. Except for the first one, which is a document specifically created for the HCDSNS, the remaining reports already existed in the digital medical records systems of the regional services. Added to these is the possibility of communicating the EUPS (European Union Patient Summary).

In the creation and implementation of the HCDSNS, the Ministry of Health has been very aware of the work carried out by the e-Health Network[6] (in which it actively participates), in particular, in regards with the EU-Patient Summary and the EU electronic prescription and electronic dispensation projects (ePrescription/eDispensation). Taking into account the fact that the work of this network is the antecedent of the future EHDS, we can say that the HCDSNS is aligned with its objectives and, in fact, the HCDSNS aims to alleviate, on a national level, the same problems that the EHDS intends to tackle on a European level (in terms of primary use of data). In this sense, Spain is in a good starting position in order to implement the requirements regarding the primary use of data in the context of EHDS.

The priority categories of electronic health data that Member States will have to share for primary use under the EHDS are data which are already processed in the context of HCDSNS, as well as in the electronic prescription of Spanish national health system:[7] patient summaries; electronic prescriptions; electronic dispensations; medical images and image reports; laboratory results; discharge reports (Art. 5 of the Proposal[8]). This will allow the CCAA in

[3] At the regional level, the Decree 29/2009, of February 5th, which regulates the use and access to electronic medical records in Galicia, stands out. At the national level, we can highlight the Article 56 of Law 16/2003, of May 28th, on cohesion and quality of the National Health System; the Royal Decree 1093/2010, of September 3rd, which approves the minimum set of data for clinical reports in the National Health System; or the aw 41/2002, of November 14th, basic regulatory of the autonomy of the patient and rights and obligations regarding clinical information and documentation, which already contemplates the existence of medical records in electronic format, as well as the coordination of medical records on a national level by the Ministry of Health (Art. 14.2; additional provision 3rd).

[4] The background of this project is accessible at: www.sanidad.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_English.pdf .

[5] As of August 2023, the population coverage of the HCDSNS in Spain is 91%. The situational picture is accessible at: www.sanidad.gob.es/areas/saludDigital/historiaClinicaSNS/mapa/situacionActualHCDSNS.htm.

[6] This network was created based on Art. 14 of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (accessible at: http://data.europa.eu /eli/dir/2011/24/oj).

[7] The current situation of the electronic prescription of the national health system (RESNS) can be consulted at: www.sanidad.gob.es/areas/saludDigital/recetaElectronicaSNS/home.htm.

[8] These data are described in Annex 1.

Spain (which, as has been noted, have different medical record systems) to be able to comply with the EHDS prescriptions, thanks to the works carried out in preparation for the HCDSNS and the electronic prescription system. Additionally, and as we later on explain, the HCDSNS already incorporates some of the provisions in relation to the citizens' rights regulated in the Proposal (e.g., the possibility of hiding information from the medical record from health professionals, or the access to the "access record", which we will refer to later). In this, however, the situation is more disparate at the regional level, so the CCAA will have to make an additional effort when preparing their systems for the exercise of the rights that are recognized to citizens in relation to the use of primary data in the EHDS.

2. *Provisions of the Proposal on the exchange of electronic health data for primary uses and EHR systems*

The European electronic Prescription and electronic Dispensation services and EU Patient Summary, which we have referred to in the previous section, are currently offered through the EU cross-border electronic health service infrastructure "MyHealth@EU", to which Member States are gradually being incorporated. The EHDS foresees the creation of a cross-border infrastructure for the primary use of electronic health data called MyHealth@EU (Art. 12 of the Proposal), which will clearly build on the work already carried out within the framework of the Cross-Border Healthcare Directive (Directive 2011/24/EU).[9]

In view of the Proposal, this infrastructure would consist of (Art. 12):

1) A national contact point for digital health:
   - That offers cross-border health information services for primary use (joint data controllers).
   - Under the responsibility of the States.
   - That may be established within the digital health authority designated by each State, in compliance with the Proposal.
   - To which States must ensure connection of all healthcare providers (and pharmacies).
2) A central platform for digital health:
   - Which is an interoperability platform for data exchange between the national contact points.
   - Created by the European Commission (processor).

This infrastructure will serve for the bidirectional exchange of electronic health data for the provision of healthcare; the dispensing of electronic prescriptions; but also the provision of complementary services (such as telemedicine, access by the citizens to their translated health data, exchange of health/vaccination certificates, and others).

Therefore, each Member State should designate a national contact point for digital health, who will ensure the connection to all other national contact points and the central platform for digital health. In addition, it should ensure that all healthcare providers are connected to their national contact points for digital health and that they carry out bidirectional exchanges with the national contact point. It will be the national contact point that will facilitate the exchange of personal data with the other national contact points, in the European electronic medical records exchange format, which we will refer to below.

If we look at the current status of the implementation of MyHealth@EU,[10] we see that Spain is in an advanced position in the work of implementing the Patient Summary and also, although to a lesser extent, those of ePrescription and eDispensation. This should allow for easier implementation of the provisions relating to the cross-border health infrastructure of the EHDS.[11]

However, the regulation contained in the Proposal regarding EHR systems raises more doubts. A mandatory self-certification system is established, by which these systems must demonstrate that they comply with certain essential requirements regarding interoperability and security at the European

[9] See, on the shortcomings of this Directive, J. S. Marcus, B. Martens, C. Carugati, A. Bucher and I. Godlovich, *The European Health Data Space*, IPOL | Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament Policy Department studies, 2022, 19, 20, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4300393.

[10] Available at: https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en.

[11] The Joint Controllership group (newly created) will approve the incorporation or disconnection of a participant from MyHealth@UE (Arts. 12.9, 66 of the Proposal).

level (Annex II). This is intended, in the words of the Proposal itself, to ensure "that electronic health records are compatible between each system and allow easy transmission of electronic health data between them". To achieve this, certain obligations regarding product conformity must be implemented: application of common conformity specifications (Art. 23); technical documentation (Art. 24); information sheet (Art. 25); EU declaration of conformity (Art. 26); and CE marking (Art. 27).

This constitutes an essential element for the correct implementation of the EHDS. Not in vain, one of the legal bases of the Proposal is Article 114 TFEU (harmonisation of the internal market). However, it is debatable whether self-certification is sufficient to guarantee citizens' rights in an area as sensitive as health data or whether a third-party conformity assessment system should be established.[12]

On the other hand, we must not forget that the legal basis of the Proposal is Arts. 16 and 114 TFEU, so we are not dealing with health policy regulations, but rather harmonization of the internal market and data protection. However, Article 168 TFEU reserves powers to the States in health policy, which constitutes a limit to the EU's action in this area. Specifically, its paragraph 7 establishes that the EU's action in public health shall respect the responsibility of States in defining their health policy, as well as the organization and delivery of health services and medical care, which includes management of health services, as well as the allocation of resources assigned to said services. Which implies that, in addition to the measures included in the Proposal constituting a genuine example of harmonization of national legislations, principles such as proportionality must also be respected. This final aspect is fundamental, taking into account the impact that the EHDS can have on the management of national medical record systems.[13] In fact, the Council is considering the introduction of a new article to clarify the freedom of States to regulate the use of wellness applications.

3. *The configuration of the patient's rights in regards to the primary use of health data*

3.1. *Rights included in the Proposal and other provisions to enforce them*

As stated at the beginning of this work, one of the main objectives of the Proposal in the field of the primary use of data is to provide individuals with greater control over the health data included in their medical records. In this sense, the Explanatory Memorandum of the text indicates that "The general objective is to ensure that natural persons in the EU have increased control in practise over their electronic health data".[14]

The original text of the Proposal opted for a novel structure, departing from what is seen in the GDPR, or in national legislations such as the Spanish one, as it did not dedicate a differentiated provision to each of the rights included; dealing with all of them in Article 3 of the Proposal. It is to be noted that the latest proposal of the Council focuses its attention on this particular matter, separating out the rights into different articles "with the aim of clarifying the scope" of each one of them.[15] However, as a new version of the articulated text incorporating these changes has not been published, references will be made to the structure of Article 3, as it is known in the original Proposal, and considering the fact that its essential content remains unchanged.

Setting this aside, it can be said that the rights included in the Proposal delimit the specific area of power that patients have over their data, in a clear attempt to provide true effectiveness to a series of rights whose application in practice has faced, to this day,

[12] This is one of the aspects highlighted in the EDPB-EDPS *Joint Opinion on the Proposal for a Regulation on the European Health Data Space*, 2022, no. 73-76 (in addition to the impact and interrelation between the declaration of conformity and compliance with data protection regulations). It is also one of the topics discussed in the Council's work, which can be consulted here:https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CONSIL:ST_9368_2023_INIT.

[13] The EDPB-EDPS *Joint Opinion* also reflects on the competence issues in relation to the legal basis of Art. 16 TFEU, raising doubts about the full compatibility of some of the provisions of Chapters II and IV of the Proposal with the law of States in the e-Health sector (in particular, the access of health professionals to restricted personal health data, the systematic registration systematic recording of the relevant health data by health.
professionals or the handle of unexpected findings by health data access bodies towards natural persons) (see, in particular, no. 14).

[14] See pp. 1, 2, 3, 5, 8, 14, 17, among others, of the Explanatory Memorandum; Recitals 1, 9, 12, 16, 67. See also the legislative financing statement attached to the Proposal.

[15] See p. 10 of the document issued by the Council, cited above.

multiple obstacles, as the Proposal itself admits.[16] In this sense, this text represents the definitive overcoming of the classic conception of personal data protection, in which the citizen acted as a mere passive spectator before the processing of their data, and their rights were not materialized, in most cases, neither from a legal point of view nor, particularly, in practice.

With this objective in mind, the Proposal takes, as a starting point, the catalog of rights already known and observable both in the data protection legislation prior to the publication of the GDPR, as well as, especially, in the latter. In this sense, it is possible to identify some classic rights, such as the right of access (paragraphs 1, 2, 3 and 10 of Article 3) or the right to rectification (paragraph 7 of the provision); while others that are somewhat more modern are also incorporated, such as the right to portability (paragraph 8), on which the Proposal insists on numerous times, from its Explanatory Memorandum.

Along with these well-known rights, the introduction of a series of provisions that can be considered as new stands out, such as the possibilities for the persons to authorise other natural persons to access their electronic health data of the person on their behalf (paragraph 5) -which appears as an obligation for Member States, who must establish services to enable this right-, to insert data into their own EHR -with indication as to whether the information has been inserted by the patient or their representative- (paragraph 6), or to restrict access to specific data (paragraph 9), among others.

Finally, within the same Article 3, there are other provisions aimed at complementing or guaranteeing the stated rights, such as the enforceability of data in electronic format (paragraph 4); provisions related to the powers of the supervisory authorities in matters of data protection regarding, specifically, these rights (paragraph 11); or a final provision, relating to the technical execution of the rights by the Commission (paragraph 12).

All of this is accompanied by the mechanisms that other parts of the Proposal provides for making these rights effective in the event of possible non-compliance or violations. This is the case, particularly, of Article 10, which introduces a new figure, the "digital health authority", responsible, as indicated in the precept, for the "implementation and enforcement of this Chapter at national level", with powers that appear to be in discordance with those provided for the supervisory authorities under GDPR, which could entail certain risks for the effective defense of the rights of natural persons.[17]

Returning to the regulation of rights done by the Proposal, it is appropriate to focus our attention on certain solutions that are particularly striking.

3.2. *The right of access: a broader scope*

The right of access to data is, as has already been said, a classic right in the matter. Observing the regulation made by Article 3 of the Proposal, some interesting points can be highglighted in relation to Article 15 GDPR and also, in regards to Spanish legislation, in Article 13 LOPDGDD (the Spanish *Ley Orgánica de Protección de Datos y Garantía de derechos digitales*, that is, the Organic Law of Data Protection and Guarantee of digital rights).

Firstly, the Proposal guarantees that the data are accessible to patients, there being a right to obtain "an electronic copy, in the European electronic health record exchange format referred to in Article 6" (paragraph 2 of the Article), of, at a minimum, the aforementioned priority categories of data collected in Article 5. But, also, this access must also be given "immediately" and "free of charge and in an easily readable, consolidated and accessible form" (paragraph 1).[18] In this

[16] It states that "Natural persons' access to their personal electronic health data remains burdensome, and natural persons have limited control over their own health data and the use of these health data for medical diagnosis and treatment" (see Explanatory Memorandum, p. 9. See also Recital 67). See also J. S. Marcus, B. Martens, C. Carugati, A. Bucher and I. Godlovich, *European Health*, 16.

[17] See the wording of Articles 3.11 and 11.1, which are clearly contradictory; or, in general, the idea, expressed in Recital 14 of the Proposal, that the supervisory authorities "must remain competent (…) to process claims submitted by natural persons", which clearly conflicts with the long list of powers conferred, according to the Proposal, to the digital health authority. In a similar sense, see EDPB-EDPS, *Joint Opinion*, no. 67, 69.

[18] In regards to the gratuity of the access to the data and the interpretation of Articles 12 and 15 GDPR, the recent CJEU ruling of 26 October 2023 (case C-307/22) confirms the right of the patient to obtain a free first copy of the medical record. The Court also elaborates on other requisites of said copy, including its intelligibility.

sense, the idea that access must be immediate is particularly noteworthy; for it is not stated in Article 15 GDPR, which is highlighted in Recital 8 of the Proposal as a circumstance that can cause significant harm to people.

However, this rule has an exception, which is that this immediate access will not occur when, in the interest of the patient, it is more advisable to wait until a health professional can "properly communicate and explain to the natural person information that can have a significant impact on his or her health" (paragraph 3). This circumstance can be easily explained considering the type of information the Article is referring to -which also justifies that this exception provision is not included in the configuration of this right in general regulations, such as the GDPR or the Spanish LOPDGDD-.

Secondly, the most remarkable aspect of the right of access' regulation -at least, from the point of view of the Spanish experience- is, without a doubt, the rule contained in paragraph 10 of the Article, which indicates that "Natural persons shall have the right to obtain information on the healthcare providers and health professionals that have accessed their electronic health data in the context of healthcare". In short, we are talking about what in Spain is known as "access to the access record"; that is, access, by patients, to the file which reflects the accesses made by professionals to their medical records.[19]

This is an issue that has been widely debated in the context of the Spanish legal system. Although access to the access record is contemplated in the HCDSNS, the applicable regulations on the matter do not respond to the specific question of whether the patients have the right to know, specifically, the identity of the professionals who accessed their data; which is a fact of radical importance, to the extent that it is likely to condition, in most cases, the protection of the rights of the injured party before the Courts.[20]

The relevance of the issue can be easily understood, especially when one sees that it raises conflicting positions in important instances. And thus, on the one hand, the Spanish data protection control authority, namely, the Spanish Data Protection Agency (Agencia Española de Protección de Datos or AEPD), has taken a stand in various resolutions and reports against the communication of this particular information.[21] The same position can be identified in different rulings,[22] some, regulations of the Autonomous Communities [23] and, although it is not expressed in an excessively-clear manner, in the explanatory document of the HCDSNS.[24]

On the other hand, the possibility of knowing the identity data of those who access the medical records is supported by different regulations of the Autonomous Communities,[25] some sentences[26] and the

[19] The "access record", in the Spanish system, is a file initially introduced by Article 103 of Royal Decree 1720/2007, of December 21st, which approves the Regulations for the development of Organic Law 15/1999, of December 13th, on the protection of personal data (that is, the data protection law in force in Spain prior to the entry into force of the GDPR), and also provided for by Article 23 of Royal Decree 3/2010, of January 8th, which regulates the National Security Scheme. It consists of a record – useful for the purposes of audits and internal controls, among others- in which every access leaves a trace of, at a minimum, the user's identification, the date and time of access, the file being accessed, the type of access, and whether it is authorized or denied. See also the details in this regard of Report 584/2009 of the Spanish Data Protection Agency.

[20] It is explained in detail in A. S. Casanova Asencio, *Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias*, in *InDret: Revista para el Análisis del Derecho*, no. 2, 2019, 18-22.

[21] See Reports 267/2005 and 171/2008 - referred, in turn, by a large number of resolutions of the same Agency (R/01999/2017, R/02324/2017, R/02410/2017, R/02411/2017, R/03001/2017, R/00970/2018, RR/00342/2018) - and the more recent Reports 0101/2019, 0098/2020 and 003/2021. The Basque Data Protection Agency stated the same position (Opinion of May 17th, 2011).

[22] Among others, the SSAN of February 26th, 2014 and February 9th, 2018 are frequently cited.

[23] See Article 19.2 of Decree 24/2011, of April 12th, on the Health Documentation of Castilla-La Mancha.

[24] The most recent document in relation to this system can be consulted here (see pp. 16, 38, 45, 47 *et seq*., where it can be noted that the data related to the identity of the person accessing is not included in the information that the patients can consult through this service, also indicating that this information is registered - apparently, solely - for audit purposes): www.sanidad.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_English.pdf.

[25] See Arts. 31.1. of the Foral Law 17/2010, of November 8th, on the Rights and Duties of People in matters of Health of the Autonomous Community of Navarra and 35.3 of Law 3/2005, of July 8th, on Health Information and Autonomy of the Patient from the Autonomous Community of Extremadura.

[26] One recent and worthy to be highlighted example is the STS, Chamber 2, of 25 September 2020, to which the AEPD expressly refers, although with a somewhat surprising interpretation, in its Report 003/2021.

generality of Spanish doctrine,[27] in addition to other entities, both national[28] and international -as is the case, notably, of the Article 29 Working Part (current European Data Protection Board)[29]-.

Aside from the arguments put forward in favor of one position or the other, the regulation of the Proposal on this point represents a decisive support for the position in favor of access to these data; which, if the text materializes in a Regulation, would undoubtedly lead to a change in the doctrine of the Spanish AEPD. All things considered, it is also the most favorable solution in regards to the promotion of the rights of patients, in line with the general objectives of the Proposal; reason for which it has to be judged favorably.[30]

3.3. *Medical records: between a basic tool for healthcare and the personal data spaces*

Some of the rights contained in Article 3 of the Proposal are in clear connection with the idea that the EHR is a data space over which the patient has an important scope of decision, and can partially configure it, in connection with certain initiatives carried out in certain States of the European Union.[31]

This is the case, mentioned above, of the possibility of data insertion by the patient; of the right of rectification, of which Article 3 of the Proposal provides only a brief overview, to refer, generically, to the GDPR (paragraph 7); or, in a particularly problematic provision, the right that the patient would have to "restrict access of health professionals to all or part of their electronic health data" (paragraph 9).

This last issue had been debated for some time in different forums;[32] in particular, regarding particularly sensitive health data, such as those related to infectious diseases, mental health data, voluntary terminations of pregnancy,[33] and others. Singularly, it had been raised by the Article 29 Working Party - which, among different options to articulate this right, discussed whether there should be a notice regarding the presence of this hidden data;[34] an idea that, on the other hand, has been criticised both by the Spanish doctrine[35] and by the AEPD.[36]

The system introduced by the Proposal implies that the professional cannot access the data unless there is express authorization from the patient, "including where the provider or professional is informed of the existence and nature of the restricted electronic health data",

[27] S. Gallego Riestra and I. Liano Galán, *¿Tiene derecho el paciente a saber quiénes y por qué han accedido a su historia clínica?*, in *Derecho y Salud*, vol. 2, no. 1, 2012, 88, 89; L. González García, *Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos*, in *Derecho y Salud*, vol. 24, no. 1 extra, 2014, 279-281; S. Gallego Riestra, *Los derechos de acceso, rectificación, cancelación y oposición del paciente a su historia clínica*, in *Derecho y Salud*, vol. 26, no. 1 extra, 2016, 137-139; or in A.S. Casanova Asencio, *Protección de datos*, 14 et seq. (in particular, 18 et seq.), recently supported, expressly, by I. Alkorta Idiakez, *El Espacio Europeo de Datos Sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios*, Cizur Menor (Navarra), Thomson Reuters Aranzadi, 2022, 55.

[28] Spanish Society of of Public Health and Health Administration (SESPAS: Sociedad Española de Salud Pública y Administración Sanitaria), *Protection of personal data and professional secrecy in the field of health: a regulatory proposal for adaptation to the GDPR*, (originally, in Spanish, "Protección de datos personales y secreto professional en el ámbito de la salud: una propuesta normative de adaptación al RGPD"), Spain, 2017, 65, 66, accessible here: http://sespas.es/2017/11/30/proteccion-de-datos-personales-y-secreto-profesional-en-el-ambito-de-la-salud-una-propuesta-normativa-de-adaptacion-al-rgpd. See also the nuances indicated in A.S. Casanova Asencio, *Protección de datos*, 17, footnote no. 50.

[29] Working Document on the processing of personal data relating to health in electronic health records (EHR) (Document WP131), 2007, 21 (hereinafter, Document WP131). Accessible here: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf

[30] In the same sense, EDPB-EDPS, *Joint Opinion*, no. 58.

[31] This is the case, singularly, of the *Personal Digital Healthcare Environment* of the Netherlands (*see,* in this regard, by I. Alkorta Idiakez, *Espacio Europeo*, 19)

[32] In favor, with limits, SESPAS, Protection of personal, 53, 54; J. Sánchez Caro, *La historia clínica gallega: un paso importante en la gestión del conocimiento*, in *Derecho y Salud*, vol. 18, no. 1, 2009, 70.

[33] The Spanish Organic Law 2/2010, of March 3rd, on sexual and reproductive health and voluntary interruption of pregnancy, provides for specific measures in relation to this issue; some of which have been subject to recent reform, furthermore, by virtue of Organic Law 1/2023, of February 28th, which modifies, among others, Articles 20 and 23 of the 2010 Law.

[34] Document WP131, p. 14.

[35] SESPAS, *Protection of personal*, 54; J. Sánchez Caro, *La historia clínica*, 70; J. Etreros Huerta, *Historia clínica electrónica*, in R. Cáliz Cáliz (coord.), *El derecho a la protección de datos en la historia clínica y la receta electrónica*, Cizur Menor (Navarra), Thomson Reuters Aranzadi, 2009, 181 (especially, 190); A.S. Casanova Asencio, *Mecanismos de prevención del acceso indebido a la historia clínica por parte del personal sanitario y nueva legislación de protección de datos*, in *Bioderecho.es: Revista internacional de investigación en bioderecho*, no. 7, 2018, 11.

[36] Report 656/2008.

as indicated in Article 4.4.

Patients' mandatory authorization can only be bypassed, as an exception, when there is a risk to the vital interests of the patient or another person, in which case the data may be accessed, subsequently informing the interested party and other subjects indicated by the precept. In this sense, we cannot ignore the fact that the right in question can pose a significant risk to both the life and health of patients and that of third parties, including health professionals themselves.[37]

The addition of this exception is palpable proof of the awareness of the important potential risks derived from the exercise of this right, with the Proposal warning that the natural person who opts for the unavailability of health data must "assume responsibility for the fact that the healthcare provider cannot take the data into account when providing health services" which is quite significant.[38]

This provision, moreover, leaves a good number of questions unresolved. Thus, it does not specify aspects such as whether all the data contained in the medical records could be hidden;[39] if, as stated above, there would be some type of notice to the health professionals regarding the presence of hidden data;[40] or if discrimination could be made in regards to specific professionals, professional categories, or, also, specific types of data.[41] Certainly, the formulation used by the Proposal is fairly brief on this point; noting that it refers to national regulations for the purposes of establishing "the rules and specific safeguards regarding such restriction mechanisms", which may favor a particularism somewhat contrary to the objectives of the Proposal itself.

In relation, precisely, to the national configuration of this measure, it can be remarked that this option is already included, in the case of Spain, in the HCDSNS, where the concealment of clinical reports and documents is allowed, after the display of a notice about the risks involved in exercising this right, and as a solution that may be "reversed by the user at any time".[42]

What is even more relevant: it is provided that the professional "will be informed of the existence of hidden information (without specifying what kind of information it is) so that, if knowing all the information were so important in the specific clinical context, the patient may understand the convenience of revealing the non-visible contents after having been duly informed". And, in addition, it is also foreseen that protected information can be accessed in the event of an "emergency situation requiring urgent action", when the patient is not in a position to give consent, although then "an audit trail indicating both circumstances" would be left.[43]

4. *Concluding remarks*

Once the preceding analysis has been made, it is worth considering that the rights of natural persons regarding primary use of their data are developed,[44] and even expanded,[45]

[37] It could be criticised that the limit relating to the rights of third parties is only applicable when the "vital interests" of said third parties are at stake, and not simply their right to health, resulting to be an excessively lax limit. Furthermore, this idea may encounter obstacles in practice, if health professionals are unaware of the existence of the data; especially, if the patient is not in a position to communicate this circumstance.

[38] Furthermore, it is indicated that "these restrictions may have life-threatening consequences and, therefore, access to personal electronic health data must be possible to protect vital interests in the event of an emergency", in addition to specifying what should be understood by "vital interest" (Recital 13). This would undoubtedly have an impact on the liability that would correspond to health professionals who do not administer a treatment, or administer an incorrect treatment, due to lack of necessary data in the evaluation of the patient's condition; which could then be significantly reduced or even completely eliminated.

[39] Certainly, the text of the Proposal does not establish a limit in this regard, and the Article 29 Working Party raised it as a possibility (*Document WP131*, 14). See also I. Alkorta Idiakez, *Espacio Europeo*, 61, 62.

[40] No specific statement on this regard can be found in the Proposal, while the wording used in the Article isn't particularly conclusive.

[41] The option of restricting the data regarding specific individuals who could have access to the medical records and have a previous relationship with the patient has been raised; as well as the possibility to discriminate depending on the professional category of the person accessing; or, similarly, the possibility of restricting access to data other than clinical data - thus, identifying data - (see A. S. Casanova Asencio, *Mecanismos de prevención*, 12-14; AEPD Report 0054/2010).

[42] See p. 17 of the explanatory document of HCDSNS, linked above.

[43] See p. 18 of the explanatory document of HCDSNS, linked above.

[44] According to the Explanatory Memorandum of the Proposal, its Chapter II, which is aimed at strengthening and promoting the control of natural persons over their own data, "develops the additional rights and mechanisms designed to complement the natural person's rights provided under the GDPR in relation to their electronic health data" (p. 18).

[45] In the same sense, R. Martínez Martínez, *Digitalización y construcción normativa de los Espacios Europeos de Datos. Retos para el sector público. Los*

through an application to the context of health data, which responds to the specific nature of the Proposal, in contrast with the general scope of the GDPR.[46]

In general, the proposed solutions are clearly aimed at seeking the announced strengthening of natural persons' control over their data,[47] which, on many occasions, serves to respond to questions that had been consistently raised in view of current regulations. And, what is more, some of them can be clearly controversial, as has been explained.

In any case, what seems obvious is that the configuration of the rights presented in the analysed Proposal will have a decisive influence, if it ends up being approved as a regulation, on the way in which the management of national medical records systems is structured.[48] In this sense, it is worth noting that medical records have traditionally been considered only as a tool or instrument at the service of health personnel for the provision of health care;[49] which is very far from the conception that presides over both the Proposal and the European Data Strategy, in which we would be faced with personal data spaces over which patients would have broad configuration powers.

Therefore, it seems clear that the development of this Strategy will require a reform of national legislations such as the Spanish one, either to restructure the already-existing medical record services, so that they can comply with the requirements derived from the European Health Data Space, or to create data spaces independent of national electronic medical records, in connection with the obligation for Member States provided for in Article 3.5.a) to establish electronic health data access services that allow the exercise of the rights enshrined in the precept.

On top of this, the implementation of the cross-border infrastructure for the primary use of data within the EU will be more or less complex depending on the specific state of preparation of each of the countries where it must be implemented. In the case of Spain, it should not entail excessive problems, to the extent that the HCDSNS system is planned, as has been said, to alleviate -at the national level, and with the territorial particularities of Spain- problems similar to those noticeable in the sharing of data for primary use between the different Member States of the Union. Furthermore, it is pertinent to remember that the e-Health Network has been a clear reference for the implementation of the HCDSNS.

Likewise, it has also been indicated that Spain is advanced in the implementation work of the Patient Summary, ePrescription and eDispensation. In contrast, the self-certification scheme for EHR systems generally raises more doubts, which must be resolved, both because of its relevance in relation to the protection of citizens' rights, and because of the impact that these measures are likely to generate in the internal legal systems of the Member States upon their implementation.

datos de salud, in *La Ley Privacidad*, no. 13, 2022, 5; see also S. Navas Navarro, *Datos sanitarios electrónicos. El espacio europeo de datos sanitarios*, Madrid, Reus, 2023, 117.
However, see also L. Marelli *et al*., *The European health data space: too big to succeed?*, in *Health Policy*, no. 135, 2023, 2, available at: www.sciencedirect.com/science/article/pii/S016885102300146X.

[46] In the same sense, EDPB-EDPS, *Joint Opinion*, no. 19, 47, 50, which also addresses the coordination problems that may arise, regarding the rights of natural persons, between these two texts; see also D. Horgan, M. Hajduch, M. Vrana, J. Soderberg, N. Hughes, M. I. Omar, J. A. Lal, M. Kozaric, F. Cascini, V. Thaler *et al*, *European Health*, 1629.

[47] Always in the context of the primary use of the data, which stands out in comparison with the treatment of secondary use of data, in regards to which the rights of natural persons are not defined (see M.B. Andreu Martínez, *Datos de salud y bien común: hacia la construcción de un mercado europeo de datos sanitarios*, in M. B. Andreu Martínez and A. Espinosa de los Monteros Rodríguez (coord.), *Tecnología para la salud: una visión humanista desde el Bioderecho*, Madrid, Plaza y Valdés Editores, 2023, 236), which has been heavily criticised (EDPB-EDPS, *Joint Opinion*, no. 35; European Digital Rights (EDRi), *Make the European Health Data Space serve patients and research*, 2023, 3, accessible here: https://edri.org/wp-content/uploads/2023/03/EHDS-EDRi-position-final.pdf), conforming one of the matters on which the Council has suggested important changes (see p. 10 of the explanatory document, linked above).

[48] See, for instance, the data collected regarding the implementation of electronic medical records in different EU countries (among others, Belgium, Netherlands, Portugal, Estonia, Germany, The Netherlands, Spain and Finland) in J. S. Marcus, B. Martens, C. Carugati, A. Bucher and I. Godlovich, *European Health*, 26, 27.
See also L. Marelli et al, *European Health*, 2.

[49] In the case of the Spanish legislation, it is identified, not in vain, as "an instrument fundamentally intended to guarantee adequate care to the patient" (Art. 16.1 of the aforementioned Law 41/2002, of November 14th, on patient autonomy).