CNS 48/2021

Opinion in relation to a Hospital consultation on the exercise of the right of access to the clinical history access register and its scope

A letter from the Data Protection Delegate of a Hospital is presented to the Catalan Data Protection Authority, in which an opinion is requested from this Authority in relation to the exercise of the right of access to the access register of the medical history and the scope of this access.

Specifically, the consultation raises the following questions for this Authority:

> **"-We can consider the data of the professional who has made improper access as personal data protected under the duty of confidentiality and, therefore, these should not be provided to the interested party who makes the request without the consent of the professional himself?**
>
> **- If, on the other hand, the interested party has the right to know the identification of the professional who has improperly accessed his clinical history, what data can be provided to him?"**

Having analyzed the request, which is not accompanied by more information, in view of the current applicable regulations and in accordance with the report of the Legal Counsel, the following is ruled.

I

(...)

II

According to the Hospital, "requests can be received from the professionals of the institution or from patients in order to know the accesses to their clinical history. If it is concluded from these requests and from their analysis that there has been an improper one, the applicant will be notified, apart from the entity proceeding to carry out the relevant internal procedures. Once the requester's response has been received, he could request the identification data of the user who has improperly accessed his medical history.

The Hospital explains that its criterion is that the right of access to the access register covers the knowledge of the information subjected to treatment but not the identity of the people who may have had access to this information, whether it is considered access right or wrong, as this would be a transfer of data that would require the consent of the user.

In this context, the Hospital asks the following:

> **"-We can consider the data of the professional who has made improper access as personal data protected under the duty of confidentiality and, therefore, not**

must these be provided to the interested party who makes the request without the consent of the professional himself?

- If, on the other hand, the interested party has the right to know the identification of the professional who has improperly accessed his clinical history, what data can be provided to him?"

Given the consultation in these terms, it should be borne in mind that Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection (hereafter, RGPD)), establishes that all processing of personal data must be lawful, fair and transparent (article 5.1.a)).

The historical clinic (henceforth, HC) collects the set of documents relating to the care process of each patient while identifying the doctors and other care professionals who have intervened (art. 9.1 Law 21/2000 of December 29, on the information rights concerning the patient's health and autonomy, and clinical documentation), and contains the information detailed in article 10.1 of Law 21/2000, to which we refer.

In the same sense, the provisions of Law 41/2002, of November 14, basic regulation of patient autonomy and rights and obligations in the field of information and clinical documentation.

The processing of data of natural persons, holders of the HC available to the Hospital, is subject to the principles and guarantees of the personal data protection regulations (RGPD and Organic Law 3/2018, of December 5, of personal data protection and guarantee of digital rights (LOPDGDD)).

III

This Authority has previously had the opportunity to examine (among others, in opinions CNS 15/2016, CNS 8/2019 or CNS 53/2019, which can be consulted on the website www.apdcat.cat), the possibility of communicating the identity of the professionals who have accessed the patients' HC data, in response to the requests made by the patients themselves, by their representatives or by relatives or people related to the patients, to those responsible for the treatment (art. 4.7 GDPR).

Regarding the content and scope of the right of access to personal information, article 15 of the RGPD provides the following:

"1. The interested party will have the right to obtain from the controller confirmation of whether or not personal data concerning him or her are being processed and, in such case, the right to access personal data and the following information:

a) the purposes of the
treatment; b) the categories of personal data in
question; c) the recipients or the categories of recipients to whom the personal data was communicated or will be communicated, in particular recipients in third parties or international organizations; d) if possible, the expected period of personal data conservation or, if not possible, the criteria used to determine this period; e) the existence of the right to request from the person in charge the rectification or suppression of personal data or the limitation of the treatment of personal data relating to the interested party, or to oppose said treatment;

f) the right to present a claim before a control authority; g) when the personal data has not been obtained from the interested party, any available information about its origin; h) the existence of automated decisions, including profiling, referred to in article 22, sections 1 and 4, and, at least in such cases, significant information about the logic applied, as well as the importance and expected consequences of said treatment for the interested party. (…).”

This precept recognizes the right of the affected or interested person to request and obtain from the controller a copy of their personal data subjected to processing, including certain information about this processing, such as, for the purposes that concern, the recipients to whom these data have been communicated or are expected to be communicated (art. 15.1.c) RGPD).

Article 4.9 of the RGPD defines as recipient, "the natural or legal person, public authority, service or other body to which personal data is communicated, whether or not it is a third party. (...)".

For the relevant purposes, the key element of this definition would be the reference to the existence of a "data communication".

Although the RGPD does not contain a definition of what is to be understood by "communication", it seems clear that access by the staff of the person responsible (the Hospital, in the case at hand) cannot be considered as such, given that this staff is part of the manager. Only when it leaves the scope of the person in charge can it be considered that we are dealing with a recipient to whom the personal data is "communicated", for the purposes of the definition of article 4.9 of the RGPD.

Thus, access by people who carry out their professional functions as an integral part of the responsible entity (as an example, the care professionals or the administration and management of the Hospital), would not properly constitute a "communication" for the purposes of the data protection regulations since the data of the affected person (the patient holding the HC) do not leave the control and management scope of the person responsible.

What does allow the exercise of this right of access, given the provisions of the data protection regulations, is to know the data communications that may have occurred, if applicable, to recipients external to the person responsible for the treatment .

Therefore, as the consultation itself points out, access to the identity of specific Hospital professionals who have accessed the HC would not be part of the information that article 15.1 of the RGPD requires to be given to the affected person , since the entity's own staff that is responsible for the HC, would not be a "recipient to whom personal data has been communicated or will be communicated", for the purposes of article 15.1.c) of the RGPD .

This, without prejudice to the fact that, in line with what is established in the Working Document on the treatment of personal data relating to health in electronic medical records, of the Article 29 Working Group (February 15, 2007), may it would be advisable to establish systems that allow the citizen to know "who and when" has accessed their HC in order to generate a greater degree of trust in patients. However, this recommendation does not imply the obligation to communicate to the affected person the accesses of the Hospital's own staff responsible for the treatment, in application of art. 15 GDPR.

Having said that, it is necessary to examine whether there is another way other than the exercise of the right of access of the interested party (art. 15 RGPD) that allows applicants to be given information from the access register to the HC, and in which terms.

IV

Article 6 of the RGPD establishes that there must be a legal basis that legitimizes the treatment, either the consent of the affected person (section 1.a)), or any of the other legitimizing bases provided for , such as, that the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment (section 1.c)).

As can be seen from article 6.3 of the RGPD and expressly included in article 8 of the LOPDGDD, data processing can only be considered based on this legal basis of article 6.1.c) of RGPD when so established by a rule with the rank of law.

At the same time, according to article 86 of the RGPD: "The personal data of official documents in the possession of any public authority or public body or a private entity for the performance of a mission in the public interest may be communicated by said authority, body or entity in accordance with the Law of the Union or of the Member States that applies to them in order to reconcile public access to official documents with the right to the protection of personal data under this Regulation."

Given this, mention should be made of Law 19/2014, of December 29, on transparency, access to public information and good governance (LTC), which aims, among others, to "regulate and guarantee the right of people's access to public information and documentation" (article 1.1.b)), and which is applicable to the case raised (article 3.1.d) LTC).

Article 18 of the LTC establishes that "people have the right to access public information, referred to in article 2.b, in an individual capacity or in the name and representation of any legally constituted legal person" (section 1).

According to article 2.b) of the LTC it is "public information", the information prepared by the Administration and that which it has in its power as a result of its activity or the exercise of its functions , including that supplied by the other obliged subjects in accordance with the provisions of this law.

The information requested, regarding the traceability of accesses to the HC, would form part of the register or control of accesses to the HC of the patients, which the Hospital has. This is public information for the purposes of the LTC and would therefore remain subject to the access regime provided for in this regulation, which establishes, as a general criterion, that the right of access to public information can only be denied or restricted for the reasons expressly established by law (article 20 et seq.).

In this sense, and in the case of information that includes personal data, the provisions of articles 23 and 24 of the LTC should be applied.

Although, according to article 10.1.a) of Law 21/2000, the HC contains, among others, information of the "doctor responsible for the patient", the information relating to the different accesses to the HC does not form part of the HC, nor is it information corresponding to categories deserving of special protection (article 9 RGPD), so access must be governed by article 24 of the LTC, according to which:

"1. Access to public information must be given if it is information directly related to the organization, operation or public activity of the Administration that contains merely identifying personal data unless, exceptionally, in the specific case it has to prevail over the protection of personal data or other constitutionally protected rights.

2. If it is other information that contains personal data not included in article 23, access to the information can be given, with the previous reasoned weighting of the public interest in the disclosure and the rights of the people affected. To carry out this weighting, the following circumstances must be taken into account, among others:

a) The elapsed time. b)
The purpose of the access, especially if it has a historical, statistical or scientific purpose, and the guarantees offered. c) The fact that it is data relating to minors. d) The fact that it may affect the safety of people. (...).”

With regard to Article 24.1 LTC, it should be noted that information on the traceability of accesses to a patient's HC actually encompasses a set of information that goes beyond what can be understood as data merely identifying information related to the organization, operation or public activity of the data controller, that is the identity (name and surname) and the position or, where appropriate, the professional profile or category (care or not), of the affected

We refer, in particular, to information such as the identity and profile of the person who accessed, the date and time of access, the center and module or unit from which the access occurred and the reason . This information could reveal the existence of an irregular action on the part of a professional at the Hospital.

In view of this, the provisions of article 24.1 of the LTC cannot be considered applicable to the present case, so access to said information requires a prior weighting between the interest public in the disclosure of information and the rights of the persons affected (art. 24.2 LTC).

According to the consultation, the Hospital receives "requests from the professionals of the institution or from patients in order to know the accesses that are in their clinical history."

In accordance with article 18.2 of the LTC, the exercise of the right of access is not subject to motivation, but the fact that the applicant expresses what is the purpose he pursues and ultimately the reasons for which he is interested knowing the information, may be relevant when deciding on the prevalence between the applicant's right of access and the right to data protection of the affected persons (Hospital professionals).

In fact, the purpose is one of the weighting criteria indicated by the LTC itself (article 24.2. b) LTC).

Point out, in this regard, that the right of access to public information can legitimately respond to particular interests. Regarding this, article 22.1 of the LTC, in demanding that the limits applied to the right of access to public information be proportional to the object and purpose of protection, mentions the taking into consideration, in the application of these limits, of "the circumstances of each specific case, especially the concurrence of a superior public or private interest that justifies access to the information."

For its part, State Law 19/2013, of December 9, on transparency, access to public information and good governance, mentions taking into consideration the fact that the applicant justifies their request for information in the exercise of a right (article 15.3.b)).

Taking into account the context in which we find ourselves and the type of personal information requested, it seems clear that the intended purpose of the request for information on access to the HC can respond, mainly, to the will to check for possible improper access (as the query itself points out). Therefore, we can understand that the purpose of the access would be related to the defense of the interests of the applicant, holder of the HC.

For weighting purposes, it must be borne in mind that patients cared for in health centers may have a legitimate interest in knowing which accesses have occurred to their HC, since this is the main instrument for managing patient information, which which has an impact on the health care he receives and, ultimately, on his state of health.

It is worth remembering, in this sense, that the patient autonomy legislation regulates a right to information to the patient in fairly broad terms (article 2.2 Law 21/2000 and art. 4 Law 41/2002), by establishing that the patient has to be able to have all the information referring to the different aspects that have an impact on your treatment and, ultimately, o

Following the criterion of this Authority in Opinion CNS 15/2016, these aspects would include, among others, knowing which professionals are in charge and have intervened in your care process, that is to say, knowing which professionals attend to you and , by extension, could be considered to include knowing which Hospital professionals have accessed their HC to carry out or participate in this care, or carry out the functions provided for in HC regulatory legislation.

In any case, the right to receive complete information about the medical treatment and care that the patient receives, is a right that the patient autonomy legislation configures in a reinforced way.

On the other hand, data protection legislation imposes the obligation on the data controller to adopt the necessary technical and organizational measures to guarantee the security of personal data processed, including protection against unauthorized or illegal processing. lawful (articles 5 and 24 RGPD).

At the same time, it recognizes the affected person's right to submit a claim before, in this case, this Authority when it considers that there has been a breach or infringement of the data protection regulations affecting the processing of their personal data (articles 77 RGPD), as would be the case if there had been improper access to the data of your HC. This, without prejudice to being able to take other legal actions that it deems appropriate.

In this context, it seems clear that, in order to take this or other legal actions to defend their interests, the patients treated at the Hospital, or their representatives, must be able to access certain information about access to the your HC.

The data related to the Hospital's professionals (identification or labor data) are personal data protected by the principles and guarantees of the data protection regulations.

Among others, according to the principles of integrity and confidentiality, the data must be processed in such a way as to ensure adequate security of personal data, including protection against unauthorized or unlawful processing and against its loss, destruction or accidental damage, through the application of appropriate technical or organizational measures (art. 5.1.f) RGPD).

However, the fact that personal data is subject to the principle of confidentiality does not mean, as the consultation seems to point out, that it cannot be the subject of treatment (art. 4.2 RGPD), specifically, of communication, if this communication is lawful (art. 6.1 RGPD).

At this point, the principle of data minimization must be taken into account (article 5.1.c) RGPD), which requires access to be limited to the data strictly necessary to achieve the intended purpose.

Apart from knowing the identity and position or category of the professional or professionals who will have accessed the HC, from the perspective of the principle of minimization it also seems reasonable to inform the applicant of the date and time of the accesses made and /or the center and module or unit from which these accesses may have occurred, since this information would allow us to verify the belonging of said accesses.

For this reason, it is necessary to recognize the existence of a legitimate interest on the part of the patient in knowing, among others, the accesses that may have occurred to his HC, in order to be able to contrast, if necessary, that these occur from in accordance with the provisions of said legisla

Regarding this, from the perspective of data protection, it should be noted that, according to the tenth additional provision of the LOPDGDD:

"The responsible persons listed in article 77.1 of this organic law may communicate the personal data requested by subjects of private law when they have the consent of the affected or appreciate that the applicants have a legitimate interest that prevails over the rights and interests of those affected in accordance with the provisions of article 6.1 f) of Regulation (EU) 2016/679".

The legal basis of article 6.1.f) RGPD, does not apply when data processing is carried out for the fulfillment of a mission carried out in the public interest or in the exercise of public powers of the person in charge - as would be the case of the treatment of health data in the field of centers that participate in the public health network of Catalonia, as in the case we are dealing with.

However, the tenth additional provision of the LOPDGDD provides for an authorization for communication based on the legitimate interest of third parties, as it could be, in this case, patients who request access to the log of access to their HC .

This qualification would be based on the legitimate interest that patients generally have to recognize, which is a weighting element that would justify, from the perspective of data protection regulations, the patient's access to said record accesses

In any case, providing the information as indicated in the query ("only the interested party is notified if the access has been due or improper"), without identifying the professionals who have accessed the HC, does not seem to allow ascertaining whether the accesses to the HC are really justified or not, that is to say, if they have been carried out by the professionals who are legitimate to access them when responding to these accesses to assistance or administrative actions. For this purpose, it is necessary to be able to dispose of their identity

professionals, so that it is the person affected (and not the Hospital, performing a prior filter of the required information), who can check whether the accesses are justified or not.

For weighting purposes, it is also necessary to take into account the possible impact that access to the HC access register may have for professionals who access patients' HCs.

We start from the basis that, in the workplace, workers can make a certain private use of computer resources or work tools (a mobile phone, a computer, etc.) that the company makes available to them for development of the tasks and functions entrusted to them, in accordance with the policies for the use of these means established by the company. Regarding this use, in general terms, workers could have a certain expectation of privacy.

However, beyond that, it does not seem that healthcare workers can have the same expectations of privacy in relation to their use of these tools, when it comes to access and management of patient information.

As already pointed out, the patient autonomy legislation delimits the uses of the HC and the accesses that can occur in relation to these uses. For this reason, the legislation places on health centres, in this case, the Hospital, a specific responsibility in relation to the management, conservation and security of the HC (art. 11 Law 21/2000). Specifically, according to article 11.4 of Law 21/2000, "Health centers must take the appropriate technical and organizational measures to protect the personal data collected and avoid their destruction or accidental loss, and also the access, alteration, communication or any other processing that are not authorized."

Thus, given that any access to the HC must necessarily be managed, protocolized and supervised by the health center, and that the traceability of accesses is a necessary measure to ensure the protection of the information contained therein, it does not seem that the expectation of privacy that Hospital workers may have in other areas of their professional activity is applicable, to the same extent, when these workers access and manage patient information, that is to say, the HCs.

In addition, the health center must have informed (and trained) its workers about the correct management of HCs (and therefore the impossibility of carrying out unwarranted access and the consequences of non-compliance in this sense), among others, because this follows from article 11.4 Law 21/2021, mentioned, and the duty of secrecy (art. 11.6 Law 21/2000), and the principles of data protection (specifically, the principles of integrity and confidentiality, ex. art. 5.1.f) RGPD).

If we take into account that the Hospital workers have prior information about the correct use of the HC, and about the traceability of accesses, it does not seem that the expectation of privacy can be a determining counterweight in the aforementioned weighting.

This, without prejudice to the fact that in some cases the weighting must take into account other elements, as we will see in the following legal basis. In any case, the privacy expectations of Hospital workers do not, in the case at hand, constitute a reason for the general denial of patients' access to their HC access register.

From all the above, it is concluded that there is sufficient legal basis (art. 6.1.c) RGPD) in relation to transparency legislation to communicate to Hospital patients who request it, the information relating to access to your HC, including the identity, position or category of the professionals who have accessed it (whether they are healthcare staff or not), as well as any relevant information about access (date and time of access, and/ or center,

module or unit from which it occurred), without the consent of these professionals being necessary.

v

It should be remembered that, according to article 31 of the LTC, if the request for public information may affect the rights or interests of third parties, identified or easily identifiable, they must be given a transfer of the request, so that they can make the allegations they consider appropriate, in those cases in which they can be decisive for the meaning of the resolution.

This procedure is essential so that the affected people have the possibility to expose if there is any element that, depending on the personal situation of the affected person, in their opinion should lead to a limitation of access.

In the case that we are dealing with, the Hospital, as responsible (art. 4.7 RGPD) will have to carry out this hearing procedure for those affected (the professionals who have accessed the HC of the complaining patient) prior to the resolution of the applicant's request for access, for the purposes, if applicable, of opposing it.

In accordance with the considerations made in this opinion in relation to the query raised, the following are made,

Conclusions

Access to the identity of the persons who provide services to the data controller who have accessed the clinical history is not part of the content of the right of access recognized by the RGPD.

However, based on article 6.1.c) RGPD and the transparency regulations, the Hospital can communicate to patients who request it the information related to access to their HC, including the identity, position or the category of professionals who have accessed it, as well as any relevant information about access (date and time of access, and/or center, module or unit from which it occurred and reason), without that the consent of the affected professionals is necessary.

Barcelona, November 2, 2021