File identification

Resolution of sanctioning procedure no. PS 71/2022, referring to the Catalan Health Institute.

Background

1. On 07/13/2021, the Catalan Data Protection Authority received a letter from a person who filed a complaint against the Catalan Institute of Health (hereinafter, ICS), on the grounds of an alleged breach of the regulations on the protection of personal data . Specifically, the person reporting stated that he had received a text message on his mobile phone, sent from *"Salut"* on 07/07/2021, informing him that his medical history had been accessed from the Center d 'Primary Care of Manso (hereinafter, CAP Manso). In this regard, the complainant pointed out that this access to his personal data was illegal, given that his Primary Care Center is in Solsona.

Along with his writing, the complainant provided a photograph showing the screen of what would be his mobile phone, in which it is observed that from "Salut", on July 7 at 1:07 p.m., the following message would have been sent: *"Dear, we inform you that the CIP data has been accessed: (...)... from the center: CAP MANSO"*

2. The Authority opened a preliminary information phase (no. IP 279/2021), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, on the common administrative procedure of public administrations (henceforth, LPAC), to determine whether the facts were susceptible to motivate the initiation of a sanctioning procedure.

3. In this information phase, on 07/19/2022 the reported entity was required to confirm the sending of the aforementioned SMS to the now complainant on 07/07/2021, indicate the personal data in the which were accessed from the Manso Primary Care Center, and provide a copy of the access register to the aforementioned medical history on 07/07/2021.

4. On 06/09/2022, the ICS responded to the aforementioned request, providing the testimony of the CAP Manso nursing professional who would have accessed the medical history of the now complainant. The nursing professional presented the following facts:

- *"The claimant's access to the HC was by mistake and no personal or clinical data from the history was accessed. It was an involuntary and momentary access when trying to access another patient with the same last name as explained below.*
- *On 7/7/2021 the history of a patient assigned to my seat with the same last name as the patient object of the claim should have been accessed. To get to this patient's entry, move the cursor through the list and when you hover over the patient in the complaint, a screen appears indicating that the patient is a restricted access patient, reject this warning and continue to access the patient you are looking for.*
- *At no time has there been any intention to enter the history of the patient making the claim. By rejecting the warning screen, an entry may have been registered in your history since you have to interact with the icons on that screen to be able to continue to the next patient and in this manipulation (accept or reject) by mistake you may have entered the history (...)"*

5. On 04/10/2022, also during this preliminary information phase, the Authority again required the reported entity to provide a copy of the record of access to the medical history of the reporting person, of date 07/07/2021, with the details of the information that would have been accessed, and to report if, as the nursing professional claimed, for the simple fact of rejecting a notice, the ICS system registers an access to a patient's medical history (and therefore sends an access notification SMS to the phone indicated by the patient), despite not having accessed their personal data; or if, on the contrary, the system records an access only when there is an access to clinical history, either to clinical or merely administrative data.

6. On 07/10/2022 and still within the framework of this preliminary information phase, the reported entity responded to the requirement indicated in the previous antecedent, in the following terms:

- " *All questions are answered jointly. For this purpose, two screenshots of the application are attached as annexes 1 and 2. The first screen (annex 1) is activated and appears when you want to access the data of a user who is exercising the right of opposition when the person who wants to access their medical history is not part of their EAP. The second screen (annex 2) is the one that is shown when the accept button is clicked on the previous screen, and at that moment the sending of the SMS is activated notifying the patient that the access to your data. This second screen only allows access to the patient's administrative data. Annex 3 is attached with the log of accesses.*"

The ICS attaches to its writing the two referenced annexes. Annex 1 contains a screenshot of your application, which allows you to view a notice to accept or cancel, which in literal terms reads as follows:

> *"This person has exercised the right to object to access to their personal data. The use of your information is restricted exclusively to the Primary Care Team. If you need to access this person's data, you must request express authorization from the person or their legal representative.*
> *The accesses that are made are registered and subject to monitoring and evaluation. The person will receive a notice that their personal information has been accessed."*

For its part, Annex 2 shows the capture of a screen that contains a series of fields with personal data of the user/patient. The personal data shown, among others, are the following: first and last name, CIP, address, telephone, gender and age, visit log.

Finally, the entity provides the copy of the record of access to the medical history of the now complainant, dated 07/07/2021, in which the following indications relating to the reported access are observed:

origin	module	Date of access	Surname and first name of the professional	Professional category	Name of the Center
EXTENSION	SIAP_PRINT - INITIAL FORM OF THE APPLICATION. ALLOWS SEARCH OF VISITS AND USERS.	7/7/2021 13:06	(...)	NURSE	ABS 3B

7. On 03/11/2022, the director of the Catalan Data Protection Authority agreed to initiate disciplinary proceedings against the Catalan Institute of Health for the alleged violation of article 83.5.a) in relation to article 5.1 f); all of them from Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free circulation thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 08/11/2022.

In the initiation agreement, the accused entity was granted a period of 10 working days to formulate allegations and propose the practice of evidence that it considered appropriate to defend its interests.

The deadline has been exceeded and no objections have been submitted.

proven facts

On 07/07/2021 a nursing professional from the Manso Primary Care Center accessed the medical history of the complainant (user of another center) with the details indicated in the antecedent 6th in fine , without that this access was related to any assistance action, nor to related administrative procedures that justified it.

Fundamentals of law

1. The provisions of the LPAC , and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of Catalan Data Protection Authority. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

2. In accordance with article 64.2.f) of the LPAC and in accordance with what is indicated in the agreement initiating this procedure, this resolution should be issued without a previous resolution proposal, given that the accused entity has not made allegations in the initiation agreement. This agreement contained a precise statement on the imputed liability.

3. In relation to the facts described in the proven facts section, relating to improper access to the medical history of the complainant here, it is necessary to refer to article 5.1 f) of the RGPD, which provides for the following according to the principle of data confidentiality:

> *"1. The personal data will be:*
> *(...)*
> *f) processed in such a way as to guarantee adequate security of personal data, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, through the application of appropriate technical or organizational measures (" integrity and confidentiality »)".*

For its part, Organic Law 3/2018 , of December 5, on the protection of personal data and guarantee of digital rights (hereafter, LOPDGDD), establishes the following in its article 5, relating to the duty of confidentiality:

> *"1. Those responsible and in charge of data processing as well as all the people who intervene in any phase thereof are subject to the duty of confidentiality referred to in article*

5.1.f) of Regulation (EU) 2016/679.
2. The general obligation indicated in the previous section is complementary to the duties of professional secrecy in accordance with its applicable regulations (...)".

The health legislation applicable to the case regulates the use of the clinical history in the following terms:

Article 11 of Law 21/2000, of December 29, on the rights of information concerning the patient's health and autonomy, and clinical documentation

Uses of clinical history
1. *The clinical history is an instrument primarily intended to help guarantee adequate assistance to the patient. For this purpose, the care professionals of the center who are involved in the diagnosis or treatment of the patient must have access to the clinical history.*
2. *Each center must establish the mechanism that makes it possible that, while assistance is provided to a specific patient, the professionals attending to him can at all times have access to the corresponding medical history.*
3. *The clinical history can be accessed for epidemiological, research or teaching purposes, subject to the provisions of Organic Law 15/1999, of December 13, on the protection of personal data, and State Law 14 /1986, of April 25, general of health, and the corresponding provisions. Access to the clinical history for these purposes obliges the preservation of the patient's personal identification data, separate from those of a clinical care nature, unless the latter has previously given consent.*
4. *The staff who take care of the administration and management tasks of the health centers can access only the data of the clinical history related to said functions.*
5. *The staff at the service of the Health Administration who perform inspection functions, duly accredited, can access the clinical histories, in order to check the quality of the assistance, the fulfillment of the patient's rights or any other obligation of the center in relationship with patients or the Health Administration.*
6. *All personnel who use their powers to access any type of data in the clinical history remain subject to the duty of confidentiality.*

Article 16 of Law 41/2002, of November 14, " *basic regulation of patient autonomy and rights and obligations in the field of information and clinical documentation"*

" *Article 16. Uses of clinical history* .
1. *The clinical history is an instrument primarily intended to guarantee adequate assistance to the patient. The healthcare professionals of the center who carry out the diagnosis or treatment of the patient have access to the patient's clinical history as a fundamental tool for their adequate assistance.*
2. *Each center will establish the methods that enable access to the clinical history of each patient at all times by the professionals who assist them.*
3. *Access to clinical history for judicial, epidemiological, public health, research or teaching purposes is governed by the provisions of current legislation on the protection of personal data, and Law 14/1986, of 25 April, General of Health, and other rules of application in each case. Access to the clinical history for these purposes requires the preservation of the patient's personal identification data, separate from those of a clinical and healthcare nature, so that, as a general rule,*

anonymity is ensured, unless the patient himself has given his consent to don't separate them.
The investigation cases provided for in Section 2 of the Seventeenth Additional Provision of the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights are excluded.
Likewise, cases of investigation by the judicial authority are excluded in which the unification of identifying data with clinical care is considered essential, in which cases the judges and courts in the corresponding process will follow. Access to clinical history data and documents is strictly limited to the specific purposes of each case.
When it is necessary for the prevention of a serious risk or danger to the health of the population, the health administrations referred to in Law 33/2011, of October 4, General Public Health, will be able to access the identifying data of patients for epidemiological or public health protection reasons. Access must be carried out, in any case, by a healthcare professional subject to professional secrecy or by another person subject, likewise, to an equivalent obligation of secrecy, with prior motivation on the part of the Administration that requested access to the data.

4. *The staff of the administration and management of the health centers can only access the data of the clinical history related to their own functions.*
5. *The duly accredited health personnel who exercise functions of inspection, evaluation, accreditation and planning, have access to the clinical histories in the fulfillment of their functions of verification of the quality of the assistance, the respect of the rights of the patient or any other obligation of the center in relation to patients and users or the health administration itself.*
6. *The personnel who access the clinical history data in the exercise of their functions are subject to the duty of secrecy.*
7. *The Autonomous Communities will regulate the procedure so that there is evidence of access to the clinical history and its use".*

During the processing of this procedure, the fact described in the section on proven facts has been duly proven, which is constitutive of the violation provided for in article 83.5.a) of the RGPD, which typifies the violation of "the *principles básicos para el tratamiento",* among which the principle of confidentiality is at the top.

The conduct addressed here has been included as a very serious infraction in article 72.i) of the LOPDGDD, in the following form:

"i) The violation of the duty of confidentiality established by article 5 of this Organic Law"

At this point it is not superfluous to add that, although the commission of the imputed offense would be materially attributable to the employee who improperly accessed the medical history, the system of responsibility provided for in the RGPD and, particularly in the article 70 of the LOPDGDD, places responsibility for breaches of data protection regulations, among others, on those responsible for the treatments, and not on their staff. In this sense, the aforementioned article 70 establishes the following:

"Responsible subjects.
1. They are subject to the sanctioning regime established by Regulation (EU) 2016/679 and this Organic Law:

a) Those responsible for the treatments ."

So things are, in accordance with the liability regime provided for in the data protection regulations, and from the point of view of the right to the protection of personal data, the person responsible for the facts that are considered proven is the ICS, given his status as responsible for the treatment, in relation to which the offense alleged here has been committed.

4. Article 77.2 LOPDGDD provides that, in the case of infractions committed by those in charge or in charge listed in art. 77.1 LOPDGDD, the competent data protection authority:

> *"(...) must issue a resolution that sanctions them with a warning. The resolution must also establish the measures to be adopted so that the conduct ceases or the effects of the offense committed are corrected.*
> *The resolution must be notified to the person in charge or in charge of the treatment, to the body to which it depends hierarchically, if applicable, and to those affected who have the status of interested party, if applicable."*

In terms similar to the LOPDGDD, article 21.2 of Law 32/2010 , determines the following:

> *"2. In the case of violations committed in relation to publicly owned files, the director of the Catalan Data Protection Authority must issue a resolution declaring the violation and establishing the measures to be taken to correct its effects . In addition, it can propose, where appropriate, the initiation of disciplinary actions in accordance with what is established by current legislation on the disciplinary regime for personnel in the service of public administrations. This resolution must be notified to the person responsible for the file or the treatment, to the person in charge of the treatment, if applicable, to the body to which they depend and to the affected persons, if any".*

In the present case, it is not appropriate to require the ICS to adopt corrective measures in order to correct the effects of the infringement, given that it is a one-time event, already accomplished.

For all this, I resolve:

1. To warn the Catalan Institute of Health, as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1.f), both of the RGPD.

It is not necessary to require corrective measures to correct the effects of the infringement, in accordance with what has been set out in the 4th legal basis.

2. Notify this resolution to the Catalan Health Institute.

3. Communicate the resolution to the Ombudsman, in accordance with the provisions of article 77.5 of the LOPDGDD.

4. Order that this resolution be published on the Authority's website (apdcat.gencat.cat) , in accordance with article 17 of Law 32/2010, of October 1.

Against this resolution, which puts an end to the administrative process in accordance with articles 26.2 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, and 14.3 of Decree 48/2003 , of February 20, by which the Statute of the Catalan Data Protection Agency is approved, the imputed entity can file, with discretion, an appeal for reinstatement before the director of the Catalan Data Protection Authority Data, within one month from the day after its notification, in accordance with the provisions of article 123 et seq. of the LPAC. You can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

If the imputed entity expresses to the Authority its intention to file an administrative contentious appeal against the final administrative decision, the decision will be provisionally suspended in the terms provided for in article 90.3 of the LPAC.

Likewise, the imputed entity can file any other appeal it deems appropriate to defend its interests.

The director,