Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

File identification

Resolution of sanctioning procedure no. PS 4/2022, referring to the Catalan Health Institute (CAP C(...) and CAP R(...)).

Background

1. 08/12/2020 , the Catalan Data Protection Authority received a letter from a person in which he filed a complaint against the Catalan Institute of Health (hereinafter, ICS), on the grounds of a alleged breach of the regulations on personal data protection .

Specifically, the complainant stated the following in his letter: a) that by letter of 02/03/2020, the Directorate of Primary Care Girona of the ICS had given him an answer to his request for access to the traceability of your medical history in the period between 02/10/2019 and 02/10/2020; b) that in this office he was informed that access had been detected which *"could not be ascertained to be linked to professional health visits or other non-assistance purposes",* which had *"proceeded to notify the Unit of Human Resources these facts, so that they assess whether they can be the subject of a disciplinary offense that motivates the initiation of an information procedure reserved for the people who made the accesses"* and that in the shortest possible period they would be informed of the result of this procedure and of the conclusions reached; and c) that no information had been provided to him since March 2020.

The complainant, together with his complaint, provided a copy of the letter sent to him by the ICS on 03/02/2020, detailing the following unauthorized accesses:

- Access carried out on 29/08/2019 at 13:40 from CAP R(...)
- Access carried out on 25/11/2019 at 14:51 from CAP C(...)

2. The Authority opened a preliminary information phase (no. IP 384/2020), 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 12/16/2020 the reported entity was required to comply with the following:

- That, in relation to each of the reported accesses, provide the following additional information: identification and professional category of the user who made the access, and the specific resources/records accessed.
- That, and indicate whether the aforementioned accesses were justified for welfare or administrative reasons.

- That, in case the accesses were not justified, inform if the ICS had initiated any case reserved for the professionals who made them, in order to settle any disciplinary responsibilities.

4. On 12/28/2020, the ICS responded to the aforementioned request in writing in which it set out the following:

- That the two accesses to the medical history of the person making the complaint *"were not justified for health care or administrative reasons".*
- That, in relation to the people who accessed it, the ICS had carried out the following actions: a) in relation to the access made on 08/29/2019 from CAP R(...), on 04/ 08/2020 *"a written warning" was given* to the person who had accessed it; and, b) in relation to the access made on 25/11/2019, a disciplinary case had been initiated against the person who had accessed it.

The reported entity attached a record that included the additional information that had been requested in relation to each of the accesses.

(...)

5. On 01/02/2022, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the ICS for an alleged infringement provided for in article 83.5.a), in relation to article 5.1.f); both of 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 movement thereof (hereinafter, RGPD). Likewise, he appointed Mrs. (...), an employee of the Catalan Data Protection Authority, as the person instructing the file. This initiation agreement was notified to the imputed entity on 02/03/2022.

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 29/08/2019 and 25/11/2019, respectively, two people in the service of the ICS - with the category of administrative assistant - accessed the medical history of the person reporting with the details indicated in the antecedent 4th, without these accesses being related to any assistance activity nor to related administrative management.

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 of the imputed liability.

3. In relation to the facts described in the proven facts section, referring to improper access to the clinical history, it is necessary to go to article 5.1.f) of the RGPD, which provides the following regarding the principle of data confidentiality:

> *"1. The personal data will be:*
> *(…)*
> *f) processed in such a way as to guarantee an adequate security of personal data, including protection against unauthorized or illegal processing and against its loss, destruction or accidental 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 Law 21/2000, of 29 December, 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.*

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

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 clinical 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 the Law of State 14/1986, of April 25, general 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 personnel in 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 relation to patients or the Health Administration.
6. All staff who use their powers to access any type of medical history data 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 clinical information and 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 April 25, 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

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

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 administration and management staff of the health centers can only access the clinical history data related to their own functions.
5. Duly accredited health personnel who carry out inspection, evaluation, accreditation and planning functions have access to clinical records in the fulfillment of their functions of checking the quality of care, respect for patient rights 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 a record of access to the clinical history and its use".

During the processing of this procedure, the fact described in the proven facts section, which constitutes the offense provided for in article 83.5.a) of the RGPD, which typifies the violation of *"the principios 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 article 70 of the LOPDGDD places the responsibility for breaches of data protection regulations, among others, on those responsible for the treatments, and not on their staff. Specifically, the mentioned article 70 of the LOPDGDD establishes that:

"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 the 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."*

And section 3 of art. 77 LOPDGDD, establishes that:

> *"3. Without prejudice to what is established in the previous section, the data protection authority must also propose the initiation of disciplinary actions when there are sufficient indications to do so. In this case, the procedure and the sanctions that must be applied are those established by the legislation on the disciplinary or sanctioning regime that is applicable.*
> *Also, when the infractions are attributable to authorities and managers, and the existence of technical reports or recommendations for the treatment that have not been properly attended to is proven, in the resolution in which the penalty is imposed, to include a warning with the name of the responsible position and it must be ordered to be published in the "Official Gazette of the State" or the corresponding regional newspaper.*

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, the ICS should not be required to adopt corrective measures in order to correct the effects of the infringement, since these are facts already accomplished.

On the other hand, it is also not appropriate to propose the initiation of disciplinary actions against the people who improperly accessed the medical history of the reporting person, since the ICS has reported having carried out actions in this regard (background 4).

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, nor to propose the initiation of disciplinary actions, in accordance with what has been set out in the legal basis 4th.

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,