File identification

Resolution of sanctioning procedure no. PS 88/2022, referring to the Catalan Health Institute (CAP (...)).

Background

1. On 04/22/2021, the Catalan Data Protection Authority received a letter from a person who filed a complaint against the Catalan Health Institute - CAP (...) - (hereinafter , ICS), due to an alleged breach of the regulations on the protection of personal data .

Specifically, the reporting person (identified in the initiation agreement) that provided services as a care nurse at (...), stated the following:

1.1 That another nurse (Mrs. (...), a colleague of the same care team from (...), had accessed clinical histories of users without any health care reason to justify it).

1.2 That the clinical histories which she reported improper access to, corresponded to ' *her work schedule'* , so access to them by her colleague would not be justified at all.

1.3 That Ms. (...) ' *entered and abnormally scheduled in my work schedule days before December 23rd. Without being in her competence, she dedicated herself to signing up patients who, in some cases, she had not even visited. He forced the agenda with 3 visits at the same time without being urgent, scheduled (6-8 visits) with 10 minutes instead of the 20 minutes needed (...). He unprogrammed – deleted an address scheduled for December 23 and it disappeared from the list as well (...), between December 21 and 22, 2020 Mrs. (...) made, again approximately 17 illegitimate entries in the medical records of my patients to verify which patients I had treated during my shift on the 20th of December and what I had done to them'.*

1.4 In the last one, the reporting person related the CIPS linked to the clinical histories which improper access they reported. Specifically, the 17 CIPS that are transcribed below:

(...)

2. The Authority opened a preliminary information phase (no. IP 175/2021), 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 05/27/2021, this Authority required the ICS to provide a copy of the access register corresponding to the clinical histories identified in the complaint, regarding the accesses that would have been made by the Mrs. (...) between 1/12/2020 and 31/12/2020. Likewise, it was requested that detailed information be given on the reason justifying each of the accesses.

4. On 06/15/2021, the ICS provided the required access log, but without detailing its justification.

5. In view of the incomplete response of the reported entity, on 18/06/2021 the ICS was again required to provide detailed information on the justification of each of the reported accesses within a period of 10 days.

6. On 07/09/2021, the ICS responded to the request by providing an ' *Excel* ' document which included the accesses that Ms. (...) had carried out the clinical histories related in said requirement and the justification of each of them. As explained by the ICS in its written response, in the ' *Excel* ' list that was provided two types of access had been differentiated, ' *the accesses in green are justified by an assistance activity and those in white are not related to any assistance activity carried out by Ms. (...), but they are HC consultation accesses. Most of them from patients already visited by herself, days before.'*

The access details are as follows:

(...)

7. On 29/11/2022, 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).

8. The initiation agreement explained the reasons why no charge was made in respect of a series of accesses to clinical histories.

Regarding this, the following was set out in the section of reported events not imputed in the initiation agreement:

"Then proceed to address a series of accesses which are considered justified.

Specifically, it is the access to several clinical histories, also carried out by Ms. (...) which, as stated by the ICS, would be directly linked to assistance actions carried out that same day by this professional. These accesses are:

CIP	***ACCESS DATE***
(...)	*10/12/2020*
(...)	*10/12/2020*
(...)	*04/12/2020*
(...)	*10/12/2020* *15/12/2020* *17/12/2020* *18/12/2020*
(...)	*10/12/2020*
(...)	*10/12/2020*
(...)	*04/12/2020*
(...)	*11/12/2020*
(...)	*16/12/2020*
(...)	*10/12/2020*

(...)	*21/12/2020*

In accordance with what has been exposed and given that the existence of elements or indications that allow the opposite of what the ICS claims have not been proven during the present information, that is to say, that the accesses analyzed in this section would be justified and, therefore, that they would not constitute an infringement of those provided for in the regulations on data protection, proceed with the filing of the complaint regarding said accesses."

9. On 01/24/2023, the person instructing this procedure formulated a resolution proposal, by which he proposed that the director of the Catalan Data Protection Authority admonish the ICS as responsible for a violation provided for in article 83.5.a) in relation to article 5.1.f), both of the RGPD.

This resolution proposal was notified on the same date, 24/01/2023 and a period of 10 days was granted to formulate allegations.

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

proven facts

Ms. (...), a nurse who provided services at the CAP of (...), accessed the clinical history of several patients without these accesses being linked to any care or diagnostic action. Specifically, the accesses that are considered unjustified are the ones listed below:

CIP	DATE AND TIME	MODULE DESCRIPTION
(...)	22/12/2020 18:49:34	PRSFG320 - NEW TRACK
(...)	22/12/2020 15:02:09 22/12/2020 18:52:10	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK
(...)	15/12/2020 16:40:34 22/12/2020 18:36:55	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK
(...)	10/12/2020 17:06:04	PRSFG320 - NEW TRACK
(...)	15/12/2020 16:40:56	PRSFG320 - NEW TRACK
(...)	15/12/2020 16:40:19 22/12/2020 18:39:36	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK
(...)	15/12/2020 16:44:13 22/12/2020 18:44:00	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK
(...)	10/12/2020 17:08:21 22/12/2020 18:46:57	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK
(...)	22/12/2020 15:01:36 22/12/2020 18:51:18 23/12/2020 10:07:55	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK
(...)	15/12/2020 16:40:44 22/12/2020 18:36:30 22/12/2020 18:39:28	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK
(...)	12/15/2020 16:44:01 12/22/2020 18:39:54	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK
(...)	10/12/2020 17:08:38 22/12/2020 18:47:07	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK
(...)	10/12/2020 17:07:27 22/12/2020 15:00:27	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK

(...)	22/12/2020 18:41:27	PRSFG320 - NEW TRACK
(...)	12/15/2020 4:45:10 PM 12/22/2020 6:47:18 PM	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK
(...)	7/12/2020 8:49:19 10/12/2020 17:10:55 22/12/2020 15:01:12 22/12/2020 18:51:37 22/12/2020 18:51:55	PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK PRSFG320 - NEW TRACK

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. The accused entity has not made allegations in the resolution proposal, but it did so in the initiation agreement. Regarding this, it is considered appropriate to reiterate below the most relevant part of the motivated response of the instructing person to these allegations.

In the statement of objections to the initiation agreement, the ICS referred to the answer given in the preliminary information phase (on 07/09/2021), in which it provided an Excel document in which they detailed all the accesses to clinical histories that Ms. (...) and differentiated two types of access, ' *the accesses in green are justified by a care activity and those in white are not related to any care activity carried out by Mrs. (...), but they are HC consultation accesses. Most of them from patients already visited by herself, days before.'* In the statement of objections to the initiation agreement, the ICS added that there were a series of accesses that ' *could not be justified'* , thereby admitting that some of the access to clinical histories carried out by Ms. (...) they had no justification.

It is worth saying that in that previous information phase, the entity's response had not been so forceful, given that it justified the accesses that were not related to any assistance activity such as " *consultation"* . In this regard, it is not superfluous to point out , as the instructor highlighted in the resolution proposal, that a mere consultation does not justify access, since this would mean that any access to clinical history would always be legitimate regardless of the reason for the consultation, when the truth is that access to the medical history must always obey a healthcare or diagnostic reason , as provided for in the health regulations.

All in all, it must be concluded that the accesses made by Ms. (...) detailed in the proven facts section, carried out without the consent of the patients, nor having justified their link to any healthcare activity, constitute unjustified access and contrary to the duty of confidentiality of personal data .

Finally, in the statement of objections, the ICS stated that it had taken actions aimed at improving the traceability and control of professionals' access to clinical histories " *by raising awareness of the use of these tools among users and with the adoption of periodic control access audits"* . In this regard, it is worth saying, as the instructor of the present sanctioning procedure already explained in the resolution proposal, that although any measure tending to improve the traceability and control of access to clinical histories must be evaluated very

positively, this fact does not detract from the imputed facts, nor their legal qualification, consisting in the violation of the principle of data confidentiality.

Finally, it should be noted that, as regards the person responsible for the infringement, although the commission of the imputed infringement would be materially attributable to the person who improperly accessed the medical records, the liability system provided for in the RGPD and particularly in article 70 of Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (hereafter, LOPDGDD), responsibility for violations of the regulations on the protection of data, among others, about those responsible and in charge of the treatments, and not about 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*
> *b) Those in charge of the treatments*
> *(…)"*

For all the above, it must be concluded that the ICS, as the entity responsible for the reported treatment, breached the duty of confidentiality of personal data by having produced the unjustified access detailed in the section on proven facts. However, in view of the number of unjustified accesses carried out (33 in total), it is already advanced here that, in accordance with article 21.2 of Law 32/2010 , this Authority proposes the initiation of disciplinary actions against the person who materially effected the disputed accesses.

3. In relation to the fact described in the proven facts section, relating to the principle of confidentiality, it is necessary to refer to article 5.1.f) of the RGPD, which provides that *"1 . Personal data will be: (...) f) treated in such a way as to guarantee adequate security for personal data, including protection against unauthorized or illegal processing and against its loss, destruction or accidental damage, through the application of appropriate technical and organizational measures ("integrity and confidentiality")".*

This principle of integrity and confidentiality provided for by the RGPD must be supplemented with the duty of confidentiality contained in article 5 LOPDGDD, which establishes:

> *"Article 5. 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 the applicable regulations. 3. The obligations established in the previous sections remain even if the obligee's relationship with the person in charge or person in charge of the treatment has ended."*

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

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

"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 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 clinical history data remain subject to the duty of confidentiality."

In turn, 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 ":

"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 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 is considered constitutive of the violation provided for in article 83. 5.a) of the RGPD, which typifies as such the violation of the *" principles básicos para el tratamiento "* , which includes the principle of confidentiality.

The conduct addressed here has been included as a very serious infraction in article 72.1.i) LOPDGDD, in the following form:

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

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".

By virtue of this faculty, and in view of the amount of unjustified access carried out by Ms. (...) (33 accesses in total, distributed among 16 clinical histories), it is appropriate to propose to the ICS the initiation of disciplinary actions against this person.

On the other hand, it is considered that it is not appropriate to require the ICS to adopt corrective measures to correct the effects of the infringement, given that these are facts that have already been committed, and that the accused entity has stated that it has carried out actions to improve the traceability and control of professionals' access to clinical histories.

For all this, I resolve:

1. Admonish 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. Propose to the Catalan Institute of Health the initiation of disciplinary actions against the person who carried out the improper access detailed in the proven facts section.

3. Notify this resolution to the Catalan Health Institute.

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

5. 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,