apdcat
Autoritat Catalana de Protecció de Dades

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

File identification

Resolution of sanctioning procedure no. PS 25/2019, referring to the Maresme Health Consortium.

Background

1. On 21/(...)/2018, the complaint filed was received by the Catalan Data Protection Authority, by referral from the General Directorate of the Police (hereinafter DGP) on (...) in a Police station of the Generalitat-Mossos d'Esquadra of the DGP by Mr. (...) against the Consorci Sanitari del Maresme – Hospital de Mataró (hereafter CSM).
The DGP transferred the said complaint to this Authority to the extent that the facts reported could contravene the regulations for the protection of personal data. Specifically, the person making the complaint stated that on (...)/2018, a family member had informed him that "photographs made on a computer screen at the Hospital de Mataró where the TAC's made on his brother and where its number is displayed at the bottom".

The complaint was accompanied by two photographs showing a computer screen showing the (CT) image of a (...), and the name of the patient in the lower bar (brother of the person making the complaint).

2. The Authority opened a preliminary information phase (no. IP 330/2018), in accordance with the provisions of article 7 of Decree 278/1993, of 9 of (...), 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 (from now on, LPAC), for to determine whether the facts were likely to motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances that were involved.

3. On 23/(...)/2018 the CSM notified this Authority of a security breach in which it was reported that an employee of the CSM had accessed a patient's medical history in order to consult a radiological image, which "according to information from third parties" would later have been disseminated to a "social network". It was also reported that an information file had been opened "to clarify and verify the facts with the professionals involved".

4. On 26/(...)/2018 the Authority notified the CSM that the instruction on the actions linked to the notification of the security breach was considered complete, to the extent that a file had been initiated of prior information following the complaint filed.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

5. On 28/(...)/2018 (reiterated on 07/01/2019) the CSM was required to comply with the following:

- Provide a copy of the record of access to the medical history of the reporting person, from the day of his entry until (...)/2018 (inclusive).
- Indicate whether each and every access to the radiological image of the reporting person was justified for a healthcare reason. In the event of a negative answer to this question, please report whether the CSM has implemented some type of periodic control of the information recorded on access to patient data, with the preparation of the corresponding report by the security manager (on the line of what had been provided for in article 103.5 of Royal Decree 1720/2007, of December 21, which approves the Regulation for the deployment of the LOPD); or if this control is carried out once a request/complaint is received from him/her

  patient
- Report on the results of the investigations that the CSM had carried out in order to verify the eventual dissemination on social networks of the controversial images, and in particular, report whether any disciplinary action had been initiated against the person who allegedly would have disclosed the controversial image.
- Indicate whether photo 1 and photo 2, of which it was transferred, would show a computer from the CSM.

6. On 15/01/2019 the CSM responded to this request, in which the following was reported:

- In relation to access to the clinical history of the patient's sibling Complainant (henceforth, HC):
  a) That given the circumstances of the case, it was decided by the CSM to conduct an audit "of all the accesses, not only of radiology" in the clinical history of the patient's sibling of the reporting person (henceforth, HC), carried out between the 16th and 23rd of (...) 2018.

  b) That, as a result of this audit, access to the HC was detected by 28 people. Once these accesses were analyzed, the following was concluded: - That the accesses of 15 of these people were fully justified, "for having participated in relation to the care act and its clinical evolution or administrative management".

  - That 13 professionals accessed the HC without a medical/administrative justification to justify it.
  c) That these 13 people were asked for explanations about access, and accordingly these explanations determined the following:
  - 4 denied having accessed the HC, but admitted to having left the session open. "We consider these accesses unjustified"
  - 9 agreed "to consider the case of clinical interest or declare to have left the session open. We consider that all of them are unauthorized access".

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

- That, in relation to the leakage of the images on a social network (whatsapp), actions were carried out which are summarized below:
  - 18/(...)/18 there are indications of a possible leak of information, without specifying patient and leak details.
  - 21/(...)/18 Information file is opened by the "LOPD Incident Commission"
  - 23/(...)/18 Provisional notification to the APDCAT of a possible security breach i the Data Protection Delegate is informed.
  - Monitoring of the information file between 23/(...)/2018 and 4/(...)/2018
  - Research/Interviews with people directly involved in the possible dissemination of radiological images (10 interviews).
    The following is concluded from the investigation: -
    That on 16/(...)/2018, PERSON 3 (with nursing assistant profile) accessed the radiological image (CT) of the patient, an image that he showed to the person with whom he shared nursing control in the ICU at the time, PERSON 29 (with TCAI profile).

    - That PERSON 29 took two photographs with her mobile phone on the computer screen showing the CT scan (images identified as photo 1 and photo 2).
    - That PERSON 29 shared said images with two WhatsApp groups (according to their own statements "Group of clowns" and "Group of friends", one of which was a person known/relative to the patient
  - That, as stated, "an access audit and the its justification (28 people involved)".
  - "Carry out the disciplinary file. Once the facts have been reviewed, the interviews and access audits, it is decided:
    - 21/(...)/2018. Sanction of suspension of work and salary of 2 days to PERSON 3 and 7 days a PERSON 29 and additionally:
      - ☐ Obligation to take the GDPR course
      - ☐ Obligation to return the signed "Manual of good practices in use" document of ICT's and in the access and processing of data"
    - (...)/2019. Warning to 13 people, for improper or unjustified access:
      - ☐ Obligation to take GDPR course
      - ☐ Obligation to return the signed "Manual of good practices in use" document of ICT's and in the access and processing of data"
  - (...)/2019 We inform the patient of the facts by certified letter".

- What:
  - "CSM has implemented a type of periodic control of registration of access to patient data, as stated in the action protocol to carry out access audits approved by the management team of the CSM l' (...)/3/16 (...). These audits are both pro-active and reactive depending on whether there has been any suspicion or complaint through user support, and in the case of unwarranted access and its severity we have applied penalties. In 2018, around 14 audits were carried out, and in one case it resulted in a penalty of 2 months of work and salary, due to the repeated access of inappropriate access to clinical histories.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

• CSM also has a system for protecting the patient's clinical history in 2 levels, at the request of the patient:
- Access notification by email to the patient. When this has been requested by the patient, every time a worker/user accesses their clinical history, an email is automatically sent to the patient (...),
- Email access protection and PIN access protection, which only the patient knows. This PIN is inhibited in the event that the patient enters the emergency room and/or hospitalization.

• CSM to guarantee security measures:
- Every employee has a unique user code and we have an automatic user registration and deregistration system according to the validity of the employment contract
- We have an inventory of all the equipment to determine its exact location.

- We have an HCE or Care Manager that records the details of all access produced by the users of the system".

- That, although photo 1 and photo 2 sent by the Authority together with its request are blurry, the images agree "with [the ones] PERSON 29 shared and which correspond to the computer screen of the CSM with IP, indicated in the access register by PERSON 3".

Along with its written response, the CSM provided various documentation, among others:

- Document entitled "Good practices in the use of ICTs and in the access and treatment of the information", version "(...) 2018 V2.5"
- Registration of accesses to the controversial HC. The accesses to the HC carried out by the people identified with the following numbers are listed as unjustified: 2, 3, 4, 5, 9, 13, 16, 17, 19, 23, 24, 25 and 27.

7. On 09/09/2019, the director of the Catalan Data Protection Authority agreed to initiate a disciplinary procedure against the CSM, firstly, for an alleged infringement provided for in article 83.5.a), in relation to articles 6 and 9; and, secondly, for an alleged infringement also provided for in 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 27/4, 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 Ms. (...), employee of the Catalan Data Protection Authority.

This initiation agreement was notified to the imputed entity on 09/10/2019.

8. In the initiation agreement, the accused entity was granted a period of 10 working days, counting from the day after the notification, to formulate allegations and propose the practice of evidence that it considered appropriate to defend their interests.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

9. On 09/25/2019, the CSM presented a letter in which it acknowledges its responsibility for the alleged facts, and expressly requests that "the case proceed directly to the resolution phase, making the proposal procedure unnecessary resolution".

In this same letter, the CSM showed that the entity "acted quickly and effectively, adopting corrective measures, consisting of determining the extent of the events, the material responsible, penalizing the most serious behaviors, establishing training measures and strengthening awareness of the privacy of the data and its treatment in the staff, and acting on the interested person facilitating the satisfaction of the damages caused. And finally, measures have been reviewed and adapted to the needs detected from the case suffered".

proven facts

Of all the actions taken in this procedure, the facts detailed below are considered accredited:

1. Through the user numbers linked to different people who provide service at the CSM (a total of 13), health data contained in the medical history of the reporting person's brother was accessed, without these accesses being related to any assistance/administrative action. The details of improper access are as follows (each user is assigned the number indicated by the CSM in the written response to the Authority):

- Several accesses made on 16/(...)/2018 by the user belonging to PERSON 2 - with the professional category of nurse, in several modules, among others "Radiology data", "Emergency data", "viewer reports", "Attendance history".
- Several accesses made on 16/(...)/2018 by the user belonging to PERSON 3 - with professional category Aux. from nurse, to various modules, among others, "Clinical course", "Radiology data" "Reports list", "Reports viewer".
- Several accesses made between the 16th and the 18th of (...) 2018, by the user belonging to PERSON 4 -with the professional category of nurse-, to various modules, among others: "Data of Radiology" "Reports list", "Reports viewer", "Attendance history", "actions.HC3".

- Accesses made on (...), by the user belonging to PERSON 5 -with professional category of nurse-, to the modules: "Reports list", "Attendance history", "actions.HC3.SEM" .

- Several accesses made on the 20th and 22nd of (...) 2018, by the user belonging to PERSON 9 -with the professional category of nurse-, to various modules, among others: "Radiology data" "Reports list", "Reports viewer", "Attendance history".
- Accesses made on (...)/2018, by the user belonging to PERSON 13 - with professional category doctor - to the modules "Clinical Course", "HC3 Actions", "Radiology Data" "Reports list For".

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

- Accesses made on (...)/2018, by the user belonging to PERSON 16 -with professional category nurse-, to the modules, among others: "Reports list", "Attendance history", " Clinical course".

- Accesses made on 16/(...)/2018, by the user belonging to PERSON 17 -with professional category doctor-, to the modules "Clinical Course", "Radiology Data", "list Reports For" .

- Accesses made on 18/(...)/2018, by the user belonging to PERSON 19 -with professional category doctor-, to the modules "Clinical Course", "Radiology Data", "list Reports For" .

- Accesses made on (...)/2018, by the user belonging to PERSON 23 - with professional category nursing assistants to the modules "Clinical Course", "Radiology Data", "List Reports For", " attendance history"
- Various accesses made on 16/(...)/2018, by the user belonging to PERSON 24 -with professional category of nurse-, to various modules, among others: "Radiology data" , "List Reports For", "Emergency data".
- Accesses made on 21/(...)/2018, by the user belonging to PERSON 25 -with professional category nurse in the "Clinical Course", "HC3 Actions" modules.
- Several accesses made between the 16th and the 21st of (...) 2018, by the user belonging to PERSON 27 -with the professional category of nurse-, to various modules, among others: "Data of Radiology" "list Reports For", "Radiology Data" "laboratory", "attendance history", "clinical course", "HC3 actions".

2. PERSON 3 (with nursing assistant profile), who, as indicated in the previous section, accessed the HC without justification, on 16/(...)/2018 disclosed data of health of the patient to PERSON 29 (with TCAI profile), since he showed him a computer screen on which appeared a radiological image (TAC) of a (...), together with the name of said patient. Then, PERSON 29 took two photographs (photo 1 and photo 2) of the computer screen showing the patient's data, and spread them in two WhatsApp groups for private use, on an undetermined date but comprised between 16/(...)/2018 and (...) (date on which the complaint was filed before the DGP (1st precedent)

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 the 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 85.1 of the LPAC and in accordance with what is indicated in the agreement to initiate this procedure, this resolution should be issued without a previous resolution proposal, given that the imputed entity has acknowledged its responsibility and that implies the termination of the procedure.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

3. In relation to the facts described in section 1 of proven facts, in view of the actions contained in this procedure, and in accordance with the provisions of article 90.2 of the LPAC. it is considered more appropriate to classify these facts as a violation of the principle of data confidentiality, contained in article 5.1.f) of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27/4, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereafter, RGPD), which provides for the following:

> "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»).

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

- Article (...) 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.
>
> 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 (...)986, 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.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

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 14 of (...), "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 the Law (...) 986, of April 25, General of Health, and other applicable rules 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 33/20(...), of October 4, General of Public Health, may access patient identification data 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 only you can access the clinical history data related to your own functions.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

> 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".

This Authority considers it proven that the users linked to the people indicated in proven fact 1 - who provide service at the CSM - accessed data contained in the medical history of the reporting person's brother, without these accesses being related to no assistance/administrative action. This is expressly admitted by the CSM in its letter dated 09/25/2019. At this point it is appropriate to point out that some of these people, during the investigation launched by the CSM, stated in their defense that they had not accessed the controversial clinical history, but that "they had left the session open", thus giving the opportunity for unidentified people to access it with their user (precedent 6th). In this regard, it is necessary to make a point and point out that in such a case (the session remains open for a sufficient time to allow access to a user other than the authorized one), it would be evident that the person in charge of the treatment would not have established the security measures relevant in order to prevent its staff from accessing unauthorized resources, and this fact could constitute a different infringement typified in article 83.4.a of the RGPD. In any case, in the event that this lack of security measures had occurred, the fact is that said lack would have allowed unauthorized persons to consult the controversial clinical history, which would entail a violation of the duty of confidentiality which is the offense charged in this resolution.

In short, as has been said, it is proven in this procedure that several accesses were made to the clinical history of a patient of the CSM, without their explicit consent, and without it being justified by any assistance purpose, a fact that is constitutive of the infringement provided for in article 83.5.a) of the RGPD, which typifies as such the violation of the "principios básicos para el tratamiento (…)", specifically, the principle of confidentiality of the data.

4. With regard to the fact described in point 2 of the proven facts section, the improper dissemination of confidential personal data has also been proven, which also constitutes a violation of the principle of data confidentiality in article 5.1. f) of the RGPD, constitutive of the offense classified in article 83.5.a) of the RGPD, both articles already transcribed in the previous section.

5. Article 83.7 of the RGPD provides that each Member State may establish rules on whether administrative fines can be imposed on authorities and public bodies, without prejudice to the corrective powers of the control authority under art. 58.2 of the GDPR. And add the article

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

84.1 of the RGPD that member states must establish rules regarding other sanctions applicable to violations of this Regulation, in particular those that are not sanctioned with administrative fines in accordance with article 83.

In this regard, 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 this same sense, the art. 46 of the LOPD (valid until the entry into force of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights -LOPDGDD-), provided the following:

> "1. When the infractions referred to in article 44 are committed in files of public ownership or in relation to treatments whose responsibility would be files of this nature, the sanctioning body must issue a resolution in which it establishes the measures that should be adopted so that the effects of the infringement cease or are corrected. This resolution must be notified to the person in charge of the file, to the body to which it depends hierarchically and to those affected if there are any.
>
> 2. The sanctioning body can also propose the initiation of disciplinary actions, if appropriate. The procedure and the sanctions to be applied are those established by the legislation on the disciplinary regime of public administrations (...)".

In the present case, given the concurrent circumstances, it is not considered appropriate to require the adoption of corrective measures by the CSM, since it would be a matter of specific facts already accomplished. In addition, it is necessary to demonstrate that the CSM has informed this Authority that it has carried out a series of organizational actions and personnel training in order to avoid actions such as those that have led to the initiation of this procedure.

On the other hand, as has been said, article 21.2 of Law 32/2010, in accordance with the provisions of article 46 of LOPD, provides for the possibility that the director of the Authority proposes the initiation of disciplinary actions, in accordance with what is established by the current legislation on the disciplinary regime of personnel in the service of public administrations. In this sense, it is not considered necessary to propose the initiation of the aforementioned actions, given that the CSM has reported having initiated information files against the professionals who had improperly accessed the medical history of the person making the complaint here and/or had disseminated the your health data.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

resolution

For all this, I resolve:

1. Admonish the Consorci Sanitari del Maresme as responsible for two violations provided for in article 83.5.a), in relation to article 5.1.f), all of them 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 5th legal basis.

2. Notify this resolution to the Consorci Sanitari del Maresme

3. Communicate the resolution issued 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 (www.apd.cat), from _____ 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 what they provide
article (...)3 and following 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,