apdcat
Autoritat Catalana de Protecció de Dades

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

File identification Resolution
of sanctioning procedure no. PS 19/2018, referring to the Catalan Health Institute.

Background

1.- On 27/10/2017 the Catalan Data Protection Authority received a letter in which a complaint was made by a person against the Catalan Institute of Health (hereafter ICS), on the grounds of 'an alleged breach of data protection regulations. Specifically, the complainant - user of the CAP (...), SAP (...) - stated that unauthorized persons had accessed his medical history without his consent. In order to substantiate the facts reported, the affected person (whose ICS has known the identification in the previous information phase), provided the following documentation:

a) Document entitled "list of accesses from 01/11/2016 to 15/08/2017". This list contains several accesses to the medical history of the person reporting on 27/03/2017, by a person with the professional category of "administrative assistant" who would provide services to the CAP (...). Specifically, they include the following accesses:

• Module “USUFG005 – User and patient maintenance” at 11:07
• Module “USUG068 Labels by User” at 11:07 • Module
“USUG068 Labels by User” at 11:07 • Module
“USUFG005 – User and Patient Maintenance” at 12:48

These four accesses can be reduced to two, as three of them occurred at the same time (11:07).

b) Office dated 31/08/2017, which the EAP (...) addressed to the complainant. In this letter he was informed that it had not been established that the accesses indicated in the previous section "are linked to professional health visits", and that this fact had been brought to the attention of the SAP management (...).

2.- The Authority opened a preliminary information phase (no. IP 340/2017), in accordance with 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 (hereafter, LPAC), in order to determine whether the facts were susceptible to motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances concurrent with each other.

As part of this information phase, by means of orders dated 12/11/2017 and 01/09/2018 (the latter reiterated on 01/17/2018 and 02/21/2018) it was required the ICS to comply with the following:

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

- Identify the person to whom the two controversial accesses to the medical history of the person making the complaint correspond and confirm that on 03/27/2017 this person provided services as an administrative assistant in the CAP (...).
- Confirm whether, as pointed out by the EAP (...) in its office of 08/31/2017, the accesses indicated did not respond to any healthcare reason.
- Report if the ICS had initiated a reserved information on the controversial accesses. If so, provide a copy of the documentation listed there.
- Indicate which health/care reason would justify people with a user profile linked to a certain CAP being able to access the clinical histories of patients who are users of another CAP. In relation to these cases (access by a user linked to a CAP to clinical histories of patients assigned to another CAP) report on the following:

    - If the computer system alerts the user in some way that he/she will access the clinical history of a patient linked to another CAP.
    - If, in order to access the clinical history, the user must necessarily indicate the reasons that would justify this access.
    - If these types of access are expressly analyzed by the security manager and if they are reflected in the monthly report that must be drawn up in accordance with the provisions of article 103.5 of Royal Decree 1720/2007, of December 21, which approves the Regulation implementing Organic Law 15/1999, of December 13, on the protection of personal data (henceforth, RLOPD and LOPD).

- Provide the monthly report drawn up by the security manager, in which the reviews carried out and any problems detected in March 2017 are analysed.

The ICS responded to the above requirements through letters dated 02/01/2018, 16/01/2018 and 23/02/2018, which set out, among others, the following:

- That Ms. (...) (person to whom the user who made the controversial accesses would correspond) provided services on 03/27/2017 as an administrative assistant at the CAP (...).
- That "the accesses are not assistance" and are carried out "from the ECAP profile administrative".
- That the Territorial Administration of Central Catalonia, by means of a letter dated 10/31/2017, requested "authorization to process reserved information, in order to find out if the aforementioned accesses to the clinical history of Mrs. (name of reporting person) are justified (...)". That subsequently the ICS "ordered the realization of reserved information by the Labor and Regulatory Legal Support area of the same Management".

- That "the link that a worker with a non-health user profile of the Administrative ECAP has with a specific CAP is established for the purposes of managing agendas, scheduling visits and other purely administrative tasks".

- That "the healthcare reason why a person with a non-health user profile of the Administrative ECAP linked to a specific CAP can access administrative data of any citizen, even if they do not belong to or have a doctor assigned to it

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

CAP, but which does belong to the Territorial Management itself, is the achievement of a good service to citizens".

- That people with a user profile linked to a certain CAP that does not belong to the same Territorial Management "cannot access (the clinical histories of patients) if the patient's data have not previously been retrieved from the Administrative ECAP. Then the care professional will have access to the clinical data of this patient that are published in the HC3. This fact would occur, for example, when a patient assigned to a Territorial Management acute, for whatever reason, to a visit to another center of another Territorial Management. In the event that this fact does not occur, the professional of the Management center other than the user's assignment would only be able to access a few data (name, surname, DNI, NASSS, CIP, address and telephone), never of type clinical".

- That the system does not give any alert in the event of accessing a patient's medical history linked to another CAP, but that "the user sees it because the patient does not have a doctor assigned in the center they are in" .
- That "it is not considered necessary" for the user to access one's medical history patient linked to another CAP, indicate the reasons for said access.
- That this type of access is not expressly analyzed by the security officer and therefore "is not reflected in any report".

3.- On 18/07/2018, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the ICS, firstly, for an alleged serious infringement provided for in article 44.3.d) in relation to article 10 of the LOPD; and, secondly, for an alleged also serious infringement provided for in article 44.3.h) in relation to article 9 of the LOPD. Likewise, he appointed Mrs. (...), an employee of the Catalan Data Protection Authority, as the person instructing the file.

5.- This initiation agreement was notified to the imputed entity on 07/23/2018.

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

7.- On 25/07/2018, the ICS made objections to the initiation agreement. In its allegations, focused solely on the first of the facts that are declared to be proven in this procedure, the ICS asserted that the disputed accesses were justified by "organizational reasons", and added that only "administrative data" would have been accessed , non-assistance".

8.- In view of the allegations made, by Agreement dated 04/10/2018 the instructor ordered the opening of a trial period, in order to practice within 10 days from the day following the notification, the evidence consisting of:

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

- That the ICS report on the result of the reserved investigation that, according to the letter formulated by this entity on 16/01/2018 before this Authority, the ICS had initiated in relation to the access carried out by Ms. . (...) in the medical history of the reporting person on 03/27/2017; and provide a copy of the actions included in the aforementioned information file.

- That the ICS inform if the person making the complaint was treated as a patient in the CAP (...) on the dates immediately before or after 03/27/2017. And in the event that the reporting person had not been visited in that health center, the "organizational reasons" that in the specific case would explain the two controversial accesses should be indicated.
- Provide a screen printout of the following ECAP modules corresponding to the reporting person's medical history:
  • "USUFG068-User Labels"
  • "USUFG005-User and patient maintenance".

This trial agreement was notified on 04/10/2018 to the ICS and was given a period of 10 days to comply with what had been agreed there.

9.- On 29/10/2018 the ICS complied with the trial agreement, and provided the following information:

- That "it was seen that the access was not justified".
- That "reserved information has been made on the accesses of Ms. (...). At this moment it is being investigated by the instructor, in order to be able to conclude and propose a sanction, if necessary"

- That "The person (complainant) was not visited at the CAP (...), the past visits of this user have been consulted and no visit is recorded. The "organizational reasons" are unknown.

Likewise, the ICS contributed a screen print of the "USUFG005-User and patient maintenance" module.

10.- On 05/11/2018, the person instructing this procedure formulated a proposed resolution, which proposed that the director of the Catalan Data Protection Authority declare that the ICS had committed the following violations:

10.1. First, a serious infringement provided for in article 44.3.d), in relation to article 10 of the LOPD.

10.2. Secondly, a serious infringement provided for in article 44.3.h), in relation to article 9 of the LOPD.

This resolution proposal was notified on 06/11/2018 and granted a period of 10 days to formulate allegations. This deadline has passed and they have not been submitted allegations

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

proven facts

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

1.- A person who provided services as an administrative assistant at the CAP (...) - dependent on the Catalan Institute of Health - accessed the person's medical history on two occasions on 03/27/2017 here reporting (1st case), through the ECAP (computerized primary care clinical history program). These accesses were carried out without being justified by any assistance or administrative action.

2.- The Catalan Institute of Health does not periodically review the control information recorded in the access register, nor does it prepare reports on the reviews carried out and the problems detected, but is only reviewed following specific requests from patients.

Fundamentals of law

1.- The provisions of Law 39/2015, of October 1, on the common administrative procedure of public administrations (henceforth, LPAC), and article 15 of the Decree apply to this procedure 278/1993, of November 9, on the sanctioning procedure applied to the areas of competence of the Generalitat, according to what it provides
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.

As a preliminary consideration, it should be indicated that at the time this act was issued, the precept containing the infringing rate applied here has been repealed by Royal Decree-Law 5/2018, of 27/7, on urgent measures for the adaptation of Spanish law to the regulations of the European Union in the matter of data protection. But since it is a sanctioning procedure started before the validity of this rule - or in which the previous actions that had preceded it had started before -, it must be governed by the previous regulation. (DT 1st RDL 5/2018).

Also, in this act, the eventual application to the present case of what is provided for in Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27/4, regarding the protection of natural persons, has also been taken into account regarding the processing of personal data and the free movement thereof (RGPD). And as a result of this analysis, it is concluded that the eventual application of the RGPD would not alter the legal classification that is made here, and in particular would not favor the presumed person responsible for the infringement. In any case, it is worth saying that the facts imputed in application of the LOPD would also be so if the RGPD were applied to the case.

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

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 more relevant than the motivated response of the instructing person to these allegations.

In its statement of objections to the initiation agreement, focused solely on the first of the facts that are declared proven here, relating to access to the medical history, the ICS stated that "in this case not there has been no breach of the duty of confidentiality since Mrs (...) provided services as an administrative assistant at the CAP (...) and in the exercise of her duties she accessed administrative data, not healthcare data, from the administrative ecap.
We understand that they conveniently justified the reason for the access and its justification for managing agendas, scheduling visits and other administrative tasks. The fact that he is an administrator of a center where the patient does not have a doctor assigned to him can be explained by organizational reasons, as we alleged, since he is from the same territorial management".

As has been recorded in the background, in view of the allegations made, the instructor agreed to the test practice in order for the ICS to provide certain information in order to clarify the circumstances that in her case could have justify imputed accesses. Well, in the practice of the aforementioned test the ICS expressly admitted that these accesses were not justified,

On the other hand, in the same statement of objections, the ICS stated that no "care" data was accessed, but only "administrative" data. From this imprecise statement, it could be inferred that the ICS comes to maintain that through the controversial accesses, health data would not have been accessed, but solely administrative data. Well, in this respect it is worth saying that the type of offense declared here (violation of the principle of confidentiality) would also be consummated even in the event that the modules accessed by the administrative assistant did not contain any data relating to the health of the person here reporting.

3.- In relation to the facts described in the first point of the proven facts section, relating to the principle of confidentiality, it is necessary to refer to article 10 of the LOPD, which provides for the following:

> "The person in charge of the file and those who intervene in any phase of the processing of personal data are obliged to professional secrecy with regard to the data and the duty to save them, obligations that remain even after the end of their relations with the holder of the file or, where applicable, with its manager".

As indicated by the instructing person, during the processing of this procedure it has been duly certified that Ms. (...), administrative assistant who would provide services to the CAP (...), through her user code that allowed her to access the ECAP application, accessed data relating to the reporting person contained in her history clinic, without this access being justified for any healthcare or administrative reason. To this one

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

in this respect, it should be noted that the health legislation, when it regulates the uses of the clinical history, in relation to health professionals only contemplates access by those who assist the patient or who are involved in his diagnosis (art. 11 Law 21 /2000 and 16 Law 41/2002), a circumstance that would not occur here in the accesses referred to in the section on proven facts, which therefore violated the principle of confidentiality, action which in turn is considered to constitute a serious infringement provided for in article 44.3.d) of the LOPD, which typifies as such:

> "The violation of the duty to keep secret about the processing of personal data referred to in article 10 of this Law."

4.- With regard to the fact described in point 2 of the proven facts section, regarding which the ICS has not made any allegation in this procedure, it is necessary to refer to article 9 of the LOPD, which had the following:

> "The person in charge of the file and, where applicable, the person in charge of the treatment must adopt the necessary technical and organizational measures that guarantee the security of personal data and prevent their alteration, loss, treatment or unauthorized access, taking into account the state of technology, the nature of the data stored and the risks to which they are exposed, whether they come from human action or from the physical or natural environment."

This regulatory development regarding the security measures to be adopted was carried out through the RLOPD, and specifically with its Title VIII. In accordance with article 7.3 of the LOPD, data relating to health were specially protected data, and as such were subject to basic, medium and high level security measures (art. 81.3.a RLOPD). Among the high-level measures was the one provided for in section 5 of art. 103 of the RLOPD referring to the control obligations of the security manager, which in relation to the access register, stipulates the following:

> "The security manager must be responsible for reviewing at least once a month the control information recorded and must prepare a report of the reviews carried out and the problems detected".

It is worth saying that before the entry into force and full application of the RGPD, and in particular what is provided for in its art. 32 on the security of the treatment, the RLOPD would no longer be a directly enforceable norm, but this circumstance does not prevent it from continuing to be considered as a valid guideline or reference regarding the implementation of measures that guarantee an adequate level of security in the processing of personal data.

In addition to the above, also by way of guideline or reference it can be added that Royal Decree 3/2010, of January 8, which regulates the National Security Scheme (ENS) in the field of Electronic administration, defines the "activity register" in its article 23:

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

"With the exclusive purpose of achieving the fulfillment of the object of this royal decree, with full guarantees of the right to honor, personal and family privacy and the own image of those affected, and in accordance with the regulations on personal data protection, of public or labor function, and other provisions that result from application, the activities of the users will be recorded, retaining the necessary information to monitor, analyze, investigate and document improper or unauthorized activities, allowing the person who acts to be identified at any time ".

Section 4.3.8 of Annex II ("Security Measures") of the ENS, determines the following:

"User activities will be recorded in the system, so that: a) The record will indicate who performs the activity, when it is performed and on what information. b) It will include the activity of users and, especially, that of operators and administrators when they can access the configuration and act in the maintenance of the system. c) Successful activities and failed attempts must be recorded. d) The determination of which activities must be registered and with what levels of detail will be adopted in view of the risk analysis carried out on the system ([op.pl.1]).

LOW level The activity records on the servers will be activated.
MEDIUM Level Activity records will be informally reviewed looking for abnormal patterns.
HIGH level An automatic system for collecting records and correlating events will be available; that is, a centralized security console".

And Annex 1 of the ENS, relating to "Categories of systems" determines that:

c) HIGH level. It will be used when the consequences of a security incident affecting one of the security dimensions pose a very serious detriment to the functions of the organization, its assets or the individuals affected.

It will be understood as very serious
damage: 1.º The annulment of the organization's capacity to attend to some of its fundamental obligations and that these continue to be carried out. 2. The suffering of very serious, and even irreparable, damage to the organization's assets.

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

3.º Serious breach of any law or regulation.
4.º Causing serious damage to some individual, difficult or impossible to repair. 5. Others of a similar nature.

It should be added in relation to the ENS that the "Centro Criptológico Nacional" (of the Spanish State) has drawn up an "Guide for the implementation of the ENS" (updated in June 2017) in which point 4.3.8 establishes the following in relation to the "Registry of the activity of the users"

"225. A regular inspection of the records is carried out to identify anomalies in the use of the systems (irregular or unplanned use)
226. Automatic tools are used to collect and analyze records in search of unusual activities (for example: centralized security console, SIEM"

This Authority considers the fact recorded in point 2 of the proven facts section to be proven, which constitutes a serious violation of article 44.3.h) of the LOPD, which typifies as such:

"Maintain files, premises, programs or equipment that contain personal data without the proper security conditions determined by regulation."

5.- Article 21 of Law 32/2010, in line with article 46 of the LOPD, provides that when the offenses are committed by a public administration, the resolution declaring the commission of an offense must establish the measures to be taken so that the effects cease or are corrected. In relation to this question, and as the instructor explained in the proposal, the following should be noted:

5.1.- With regard to the fact proven 1st and given the concurrent circumstances, it is not considered appropriate to require the adoption of corrective measures, since it would be a matter of specific facts already accomplished.

5.2.- With regard to the 2nd proven fact, the ICS is required so that as soon as possible and in any case within a maximum period of one month from the day following the notification of this resolution, implement in the ECAP system the appropriate measures to guarantee a level of security appropriate to the risk, which allows to guarantee the confidentiality of the data, and which includes a process of regular verification, evaluation and assessment of the effectiveness of the security measures implemented (art. 32.1.d RGPD), such as the requirement to carry out a monthly review of the information recorded on access to patient data, with the preparation of the corresponding report, along the lines of had foreseen in the art. 103.5 of the RLOPD.

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

Once the corrective measure described has been adopted within the period indicated, within the next 10 days the ICS must inform the Authority, without prejudice to the Authority's inspection powers to carry out the corresponding checks.

5.3.- On the other hand, it should be noted that article 21.2 of Law 32/2010, in accordance with the provisions of article 46.2 of the LOPD, foresees the possibility that the director of the Authority proposes the initiation of disciplinary actions, in accordance with what is established by the legislation in force on the disciplinary regime of personnel in the service of public administrations. In the case analyzed here, this Authority considers that the proposal for disciplinary action is not appropriate to the extent that the ICS has informed this Authority (precedent 9th) that it has initiated a reserved information in relation to the unjustified accesses that have given rise to this procedure.

resolution

For all this, I resolve:

1.- Declare that the Catalan Institute of Health has committed, in the first place, a serious infringement provided for in article 44.3.d) in relation to article 10; and secondly, a serious infringement provided for in article 44.3.h), in relation to article 9, all of them of the LOPD.

2.- Require the ICS to adopt the corrective measure indicated in the 5th legal basis (section 2) and accredit before this Authority the actions carried out to comply with them.

3.- Notify this resolution to the Catalan Health Institute.

4.- Communicate this resolution to the Complaints Ombudsman and transfer it to him literally, as specified in the third agreement of the Collaboration Agreement between the Complaints Ombudsman of Catalonia and the Catalan Data Protection Agency, of date June 23, 2006.

5.- Order that this resolution be published on the Authority's website (www.apd.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 what they provide
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.

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

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.

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

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

The director

M. Àngels Barbarà and Fondevila

Barcelona, (on the date of the electronic signature)