apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 56/2021, referring to the Sant Francesc d'Assisi Foundation.

Background

1. Between the months of April and May 2021, the Catalan Data Protection Authority received twenty-four complaints made by different people against the Sant Francesc d'Assis Foundation (hereinafter, FSFA), with reason for an alleged breach of the regulations on the protection of personal data. These complaints were assigned nos. 133, 134, 135, 137, 138, 139, 140, 142, 143, 144, 145, 146, 147, 148, 149, 151, 156, 158, 165, 170, 186. 187, 188 and 202.

The complainants - all employees of the FSFA - complained of unwarranted access to their shared medical history (HC3) carried out by a person or persons employed by the Center of (...), managed by the FSFA. All the complainants indicated that these accesses would not be justified to the extent that they were not patients/users of said centre.

In order to substantiate the facts reported, each of the reporting persons provided a copy of the log of access to their HC3 -extracted from the "My Health" portal (hereafter, LMS) of the Department of Health- in which the accesses were listed carried out from the Center (...). All the accesses that were included in the LMS lists provided by the complainants had been made between 2019 and 2020, with the details that will be indicated in the proven facts.

2. The Authority opened a preliminary information phase in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, of the common administrative procedure of public administrations (from now on, LPAC), to determine if the facts were likely to motivate the initiation of a sanctioning procedure.

3. In this information phase, on 11/06/2021 a list containing the reported accesses referred to twenty-four employees of your entity was transferred to the FSFA, and I required you to comply with the following:

- Provide a copy of the log of accesses to each of the HC3 of the reporting persons, in which the accesses made from the Center (...) of the FSFA between 28/10/2019 and 31/05/2021 .

- Report if the FSFA, on the dates when the controversial accesses occurred, had implemented in the clinical history management and consultation system, the appropriate measures to guarantee a level of security appropriate to the risk that included a verification process ,

regular evaluation and assessment of the effectiveness of the security measures adopted, such as the requirement to carry out a monthly review of the information recorded on the accesses to the HC3 by the personnel serving the FSFA, with the preparation of the corresponding report.

4. On 07/02/2021, the FSFA responded to the aforementioned request in writing in which it set out the following:

- With regard to the log of access to the HC3 of each of the complainants, they reported that they did not have said log given the following:
"During this period, the FSFA had two methods of access to the HC3:
- From the platform for sharing the clinical data of Barcelonès Nord and Maresme de Badalona BSA Care Services (this platform was created by the Catalan Health Service and all the public compatible clinical history management applications). Since 03/11/2009 the FSFA has been registered in the model agreement to implement the Shared Clinical History in Catalonia and access was carried out as described in the agreement, with an application device certificate (CDA) issued by the Catalan Certification Agency (CATCert) to BSA. We attach the signed agreement as Annex 1 and the incorporation form as Annex 2. Access was carried out through the BSA web portal, without our organization having any record of these accesses.

- From the GENOMI care program. From 18/10/2019, HC3 could be accessed from within the Program with a connection via URL Viewer authorized by the HC3 support area of TICSalut of the Department of Health of the Generalitat. All accesses made from this method are registered within the GENOMI program, identifying the user who makes the consultation, the date and time it was carried out, the CIP of the patient consulted and the identifier of the Clinical History (NHC) that was attempted to be accessed.
In the register of accesses of the GENOMI care program, none of the accesses referred to in the annex to the request appear, therefore the accesses subject to the complaint have only been made from the platform for sharing the clinical data of the Barcelonès Nord and the Maresme de Badalona Care Services and for this reason BSA cannot provide the requested information.

Currently, access through BSA is completely unused and inoperative".
- Regarding the identification of the person or persons who made the access, report that:
"We have no records to know the user who made the requested queries, access to the BSA platform required a user with a password and also having the digital certificate installed on the computer, which only people authorized by the FSFA, belonging to the medical service (doctors), rehabilitation, psychology and user care, had access. This certificate was only installed on specific computers located in our facilities, and within these computers only authorized people had access to it since it was only enabled in their user sessions.

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

The rest of the workers did not have this certificate. This certificate was the same for all users, provided by BSA and was in the name of "CSS (...)_(...)", and for this reason the person who made these inquiries cannot be identified.

We can only identify the accesses made during the year 2020, which have been carried out by the staff of the center (...), with the knowledge of (...). (...), (...) of the FSFA and carried out for the reasons and context set out in point 1.b."

- Regarding the justification of the accesses, the following was reported:

"We do not have evidence of the reason for the accesses made during 28/10/2019, 17/09/2020 and 01/12/2020 since it has not been possible to identify the person who made them to justify them to us.

The accesses on 04/14, 04/21, 05/01, 09/17 and 12/01 of the year 2020 were carried out by monitoring for close contact with possible/ probable or confirmed cases of COVID19, in the context of the increase in cases the different waves of the pandemic, since we did not have reliable information about the worker affected in each case.

Of the rest of the accesses, carried out in the month of May 2020, they have to do with the following situation: in the months of April and May 2020, the impact of the first wave of the COVID19 pandemic on entities such as ours was very relevant (...).

All our users are very fragile people and therefore at high risk of a possible infection by COVID (...). On those dates, the non-governmental organization OPEN ARMS contacted our organization, and among others (...) offered to carry out a PCR screening for all the users and professionals of our organization. Samples were collected on Sunday, May 10, 2020, and they were referred to two laboratories (...) The need to know the results with the utmost urgency, in the context of infections and deaths mentioned above and faced with the emergency of adopting decisions, either in relation to users or in relation to professionals, to slow down the spread of infections, it meant that the General Directorate assessed the need to access HC3, with the sole purpose of knowing the results of the PCR's analyzed (...) and thus avoiding the growth of infections and deaths".

- That *"on the dates requested, there was no access verification process implemented, since, as previously mentioned, access could not be controlled from the platform for sharing the clinical data of Barcelonès Nord and the Maresme de Badalona BSA Assistance Services (only limit the users who had access which was already done by installing only the certificate in the user sessions of the authorized persons, and giving each one their own user and password).*

With the implementation of the GENOMI assistance program, we do have access to the register of all the accesses made to the HC3, but until the beginning of 2021, when possible improper accesses were detected, no regular assessments of the effectiveness of security measures".

The reported entity attached various documents to the letter, among others:

a) *"Standard agreement to implement shared clinical history in Catalonia"* of 9 July 2009.

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

In the fifth point of this agreement, referring to *"Access to the HCCC in each centre",* the following text appears:

"1. In accordance with what is established in the health and data protection regulations, only authorized persons may have access to the information contained in the HCC.
The entity that subscribes to this agreement undertakes to provide individualized identification and authentication systems for its healthcare professionals who, in accordance with points three and four of this agreement, can access the HCCC (...) .
2. (...) This center is responsible for informing the members of its authorized staff with authorized access that each assumes responsibility for protecting the data or the identification and authentication systems and that making use of them implies acceptance and knowledge of rights and duties in relation to access to the HCCC".

And in Annex 6, Section A of this agreement, regarding the *"standard measures applied" ,* the following is included:

"In the same way that logical protection of data access is required, physical protection is also required, that is to say, only authorized professionals must have access to clinical data".

b) *"Program of Shared Clinical History in Catalonia (HCCC). Specifications for connecting centers to the system.*

In section 4.4, referring to the *"CATCert Certificate",* it is indicated that *"The web server must have a certificate issued by CATCert. It will use it to prove its identity in SSL communication with the central platform HCCCSs"*

c) *"Program of shared clinical history in Catalonia (HCCC). Incorporation form",* formalized between the Department of Health and the FSFA on 3/11/2009.

In this document it is indicated that the Social Health Center (...) is incorporated into the HC3 program, and that *"For access to the services provided by the HCCC, application device certificates will be used (CDA) issued by the Catalan Certification Agency - CATCert with the following identification data: Organization. BSA".*

d) *"HC3 access registration report no. RI-2021-001"* issued by the FSFA on 03/12/2021, in which there is an annotation on 02/17/2021 with the following text: *The IT Manager blocks access to the folder \CONNEXIONES\HCCC where there is the original certificate, the password to install it and the credentials to access the HC3 through the BSA".*

e) *"Shared clinical history access protocol in Catalonia (HC3) - FSFA Security Document"* drawn up by the data protection delegate of the FSFA in February 2021. In this document, among other issues, the conditions for access the HC3; and in this

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

meaning it is determined that *"to access it you need a unique user and password that will only be provided to the users described in the section "Authorized managers with access to the HC3"; the users created and the person to whom they are assigned are noted in the appendix of the Security Document: DS_Annex_17.1 HC3 and SIRE Access Users."*

5. On 08/07/2021 the Department of Health, as responsible for the HC3 file, was required to provide a copy of the HC3 access log for each of the reporting persons (which list attached to the office), from 28/10/2019 to 31/05/2021, and that it included those accesses made from the Sociosanitary Center (...), dependent on the FSFA.

6. On 22/07/2021 and 30/07/2021 the Department of Health complied with this requirement by providing a copy of the HC3 access registers of the reporting persons in the indicated period. In these records it is observed that all the accesses to said stories had been made with *(...)"(...)".*

7. On 05/10/2021 and still within the framework of this preliminary information phase, the records of access to the HC3 of the complainants that the Department of Health had provided to this were transferred to the FSFA Authority, and in relation to which the following information was requested:

- That, in view of the records provided by the Department of Health which state that all the accesses to the HC3 of the complainants were made by (...), complete, if necessary, the information provided to this Authority in letter of 02/07/2021, in relation to the justification of the accesses.
- To report whether the FSFA had a single user / password to access the BSA platform to consult the HC3 register; or, if each person with access to said platform had a personal user/password.

8. On 15/10/2021, the FSFA complied with this requirement by means of a letter stating the following:

- That, in relation to the justification of the accesses, they cannot provide more information than the one that was already provided.
- That the platform for sharing the clinical data of the Barcelonès Nord and Maresme de Badalona Services Assistencianals ÿBSAÿ *"was created by the Catalan Health Service and allowed access to the HC3 to those providers of the public network of health that did not have compatible clinical history management applications, an application that we did not manage directly from the Foundation".*
- That *"access to the BSA platform required a user with a password and also having the digital certificate installed on the computer, which only people authorized by the FSFA had access to. The Foundation had only one user for all the staff authorized to access the BSA platform".*

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

9. On 30/11/2021, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the FSFA for three alleged infringements: an infringement provided for in article 83.5.a) in relation to article 5.f); and two violations provided for in article 83.4.a) in relation to article 32; all of them from Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 11/30/2021.

10. 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.

11. On 12/13/2021 the FSFA requested the extension of the deadline for making allegations, which was granted by agreement of the instructor of the procedure dated 12/14/2021, notified that same day.

12. On 22/12/2021 he received a letter from the FSFA in which he did not question the facts imputed to the procedure nor their legal qualification, on the contrary, he acknowledged his responsibility. In the same letter, the entity reiterated what it had already stated in the framework of the previous information in relation to the circumstances that had led to the access to the clinical histories of its workers carried out between the months of April and May 2020 ; and, it detailed the measures that had been taken in order to prevent events such as those that had given rise to the present sanctioning procedure from occurring in the future. In the last one, the FAMT enunciated those mitigating circumstances that in his opinion were present in the present case so that they were taken into account when establishing the amount of the penalty.

13. On 01/03/2022, the instructor of this procedure formulated a resolution proposal, by which she proposed that the director of the Catalan Data Protection Authority impose two sanctions consisting of two fines on the FSFA administrative, one of 8,000 euros (eight thousand euros), as responsible for an infringement provided for in article 85.5.a), in relation to article 5.1.a); and, a fine of 2,000 euros (two thousand euros) for the infringement provided for in article 85.4.a), in relation to article 32, all of them of the RGPD.

This resolution proposal was notified on 02/03/2022 and a period of 10 days was granted to formulate allegations.

14. The deadline has been exceeded and no objections have been submitted to the proposed resolution.

15. On 03/04/2022, the accused entity paid 6,000 euros (six thousand euros) in advance, corresponding to the sum of the pecuniary sanctions proposed by the instructor in the resolution proposal, once the reductions provided for in article 85 of the Law have been applied

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

39/2015. At this point it should be remembered that in the letter of 22/12/2021 (antecedent 12) the entity recognized its responsibility for the alleged facts.

proven facts

1. Through the digital certificate linked to (...). (...) - which allowed access to the HC3 file of the Department of Health through the BSA platform - an unidentified person or persons accessed the HC3 of the complainants - all of them workers of the entity-, without the accesses being justified for an assistance or administrative reason. The list of improper accesses is as follows:

HOLDER HC3	Date and time of access	Consulted Information
(133) (...)	28-10-2019 12:06	Summary clinical history information
	28-10-2019 12:08	Information Integrated clinical course
	10-28-2019 12:11	Information clinical reports
(134) (...)	28-10-2019 12:16	Summary clinical history information
	10-28-2019 12:17	Integrated clinical course information
	10-28-2019 12:19	Information clinical reports
	10-28-2019 12:19	Summary clinical history information
	05-15-2020 09:12	Summary clinical history information
(135) (...)	05-15-2020 09:12	Summary clinical history information
(137) (...)	05-15-2020 10:16	Summary clinical history information
(138) (...)	05-14-2020 18:27	Summary clinical history information
	05-15-2020 09:03	Summary clinical history information
(139) (...)	04-14-2020 18:14	Summary clinical history information
	04-14-2020 18:16	Information clinical reports
	04-14-2020 18:19	Summary clinical history information
	04-14-2020 18:19	Information clinical reports
	05-15-2020 08:43	Summary clinical history information
(140) (...)	10-28-2019 12:27	Information Integrated clinical course
	10-28-2019 12:27	Summary clinical history information
	10-28-2019 12:29	Summary clinical history information
	05-15-2020 09:48	Summary clinical history information
(142) (...)	05-15-2020 10:25	Summary clinical history information
(143) (...)	05-15-2020 09:30	Summary clinical history information
(144) (...)	10-28-2019 12:13	Information clinical reports
	10-28-2019 12:13	Summary clinical history information
	10-28-2019 12:14	Information Integrated clinical course
	05-15-2020 08:38	Summary clinical history information
	05-15-2020 08:41	Summary clinical history information
	05-15-2020 09:51	Summary clinical history information

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

(145) (...)	05-15-2020 08:59	Summary clinical history information
(146) (...)	28/10/2019 12:24	Summary clinical history information
	28/10/2019 12:24	Information Integrated clinical course
	28/10/2019 12:24	Information Integrated clinical course
	15/05/2020 09:27	Summary clinical history information
	18/05/2020 17:19	Summary clinical history information
	18/05/2020 17:21	Summary clinical history information
(147) (...)	05-15-2020 10:44	Summary clinical history information
	12-01-2020 15:10	Summary clinical history information
(148) (...)	05-15-2020 10:23	Summary clinical history information
	05-15-2020 11:50	Summary clinical history information
(149) (...)	05-15-2020 09:06	Summary clinical history information
(151) (...)	05-15-2020 08:48	Summary clinical history information
(156) (...)	01-05-2020 11:00	Summary clinical history information
	15-05-2020 08:56	Summary clinical history information
(158) (...)	05-15-2020 09:52	Summary clinical history information
	05-20-2020 13:12	Summary clinical history information
	09-17-2020 07:41	Summary clinical history information
(165) (...)	05-15-2020 08:52	Summary clinical history information
(170) (...)	04-14-2020 18:20	Summary clinical history information
	04-14-2020 18:20	Information clinical reports
	04-21-2020 14:14	Summary clinical history information
	04-21-2020 14:14	Information Integrated Clinical Course
	05-15-2020 16:46	Summary clinical history information
(186) (...)	05-15-2020 10:00	Summary clinical history information
(187) (...)	28-10-2019 12:20	Summary clinical history information
	10-28-2019 12:21	Information Integrated Clinical Course
	10-28-2019 12:22	Information clinical reports
	05-15-2020 09:46	Summary clinical history information
(188) (...)	04-14-2020 18:33	Summary clinical history information
	04-14-2020 18:33	Information clinical reports
	05-15-2020 10:16	Summary clinical history information
(202) (...)	05-15-2020 09:14	Summary clinical history information

2. The digital certificate linked to (...). (...) of the FSFA - which, as stated in the previous point, allowed access to the HC3 file through the BSA platform - was installed on several computers to which different people, also working in the entity Thus, to the extent that

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

all these people could use the same certificate to access the HC3 database, it was not possible to guarantee the unequivocal and personalized identification of the person who effectively accessed it, nor, consequently, to analyze the justification of these
accesses

This situation would have remained at least until 17/02/2021, the date on which, according to the report drawn up by the FSFA and provided to this Authority, access to the HC3 database through the BSA platform was blocked (letter d/antecedent 4t).

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. The facts that are the subject of this procedure fall within the competence of the Authority by virtue of article 3.f) of Law 32/2010.

2. In accordance with article 85.3 of the LPAC, both the recognition of responsibility and the voluntary advanced payment of the proposed monetary penalty lead to the application of reductions. The effectiveness of these reductions is conditioned on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction. For both cases, sections 1 and 2 of article 85 of the LPAC provide for the termination of the procedure.

The accused entity did not make any objections to the initiation agreement and did not do so before the resolution proposal, and it accepted both options to reduce the amount of the penalty. However, it is considered appropriate to reiterate the assessments made by the instructor regarding the circumstances that, according to the FSFA, would have led to the accesses that occurred between April and May 2020 to the medical records of the complainants (antecedent 4th), in essence, the need to know as soon as possible the result of the PCR tests to which the workers of the center had undergone, in view of the vulnerability of its users.

In this regard, it is worth saying that this Authority is fully aware of the very high care pressure that health and socio-health centers suffered on the dates when many of the accesses that are considered illegal took place (April-May 2020); but this exceptional situation cannot in any way protect the violation of the data protection regulations, in this case, the access to the clinical histories of the working people, histories which needless to say include information that is not limited to the result of certain tests, but it covers much more clinical information, which is likely to be known by the person who accesses according to their profile. In addition, it should also be emphasized that not only

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

there was access to certain clinical histories in 2020, that is, in a pandemic situation, but also in 2019, therefore prior to this situation.

3. In relation to the fact described in section 1 of proved facts, relating to the principle of legality, it is necessary to refer to article 6 of the RGPD, which provides for the following:

> *"1. The treatment will only be lawful if at least one of the following conditions is met:*
> *a) the interested party gives his consent for the treatment of his personal data for one or several specific purposes; b) the treatment is necessary for the execution of a contract in which the interested party is a party or for the application at the request of this pre-contractual measures; c) the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment;*
>
> *d) the treatment is necessary to protect the vital interests of the interested party or another natural person; e) the treatment is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment; f) the treatment is necessary for the satisfaction of legitimate interests pursued by the person responsible for the treatment or by a third party, provided that these interests do not prevail over the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a child.*
>
> *The provisions in letter f) of the first paragraph shall not apply to the processing carried out by public authorities in the exercise of their functions.*
>
> *2. Member States may maintain or introduce more specific provisions in order to adapt the application of the rules of this Regulation with respect to treatment in compliance with paragraph 1, letters c) and e), setting more precisely specific treatment requirements and other measures that guarantee legal and equitable treatment, including other specific situations of treatment pursuant to Chapter IX.*
>
> *3. The basis of the treatment indicated in section 1, letters c) and e), must be established by:*
> *a) the Law of the Union, or)*
> *the Law of the Member States that applies to the person responsible for the treatment (…)".*

For its part, article 9 of the RGPD, relating to the treatment of special categories of data -as the health data would be-, determines the following:

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

"1. The processing of personal data that reveal ethnic or racial origin, political opinions, religious or philosophical convictions, or trade union affiliation is prohibited, and the processing of genetic data, biometric data aimed at uniquely identifying a natural person, data relating to health or data relating to the sexual life or sexual orientation of a natural person.

2. Section 1 will not apply when one of them applies following circumstances:
a) the interested party gives his explicit consent for the treatment of said personal data with one or more of the specified purposes, except when the Law of the Union or Member States establishes that the prohibition mentioned in section 1 cannot be lifted by the interested party;
b) the treatment is necessary for the fulfillment of obligations and the exercise of specific rights of the person responsible for the treatment or of the interested party in the field of labor law and of social security and protection, to the extent that this is authorized by the Law of the Union of the Member States or a collective agreement in accordance with the Law of the Member States that establishes adequate guarantees of respect for the fundamental rights and interests of the interested party;

c) the treatment is necessary to protect the vital interests of the interested party or another natural person, in the event that the interested party is not physically or legally able to give their consent;
d) the treatment is carried out, within the scope of its legitimate activities and with due guarantees, by a foundation, an association or any other non-profit organization, whose purpose is political, philosophical, religious or trade union, provided that the treatment refers exclusively to current or former members of such organizations or persons who maintain regular contact with them in relation to their purposes and provided that the data

personal information is not communicated outside of them without the consent of the interested parties;
e) the treatment refers to personal data that the interested party has made manifestly public;
f) the treatment is necessary for the formulation, exercise or defense of claims or when the courts act in the exercise of their judicial function;
g) the treatment is necessary for reasons of an essential public interest, on the basis of the Law of the Union or of the Member States, which must be proportional to the objective pursued, essentially respect the right to data protection and establish measures adequate and specific to protect the fundamental interests and rights of the interested party;

h) the treatment is necessary for the purposes of preventive or occupational medicine, evaluation of the worker's labor capacity, medical diagnosis, provision of health or social assistance or treatment, or management of health and social care systems and services, on the basis of law

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

of the Union or of the Member States or by virtue of a contract with a health professional and without prejudice to the conditions and guarantees contemplated in section 3;

i) the treatment is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health, or to guarantee high levels of quality and safety of health care and medicines or sanitary products, on the basis of the Law of the Union or of the Member States that establishes appropriate and specific measures to protect the rights and freedoms of the interested party, in particular professional secrecy,

j) the treatment is necessary for archival purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with article 89, paragraph 1, on the basis of the Law of the Union or of the Member States, which must be proportional to the objective pursued, essentially respect the right to data protection and establish appropriate and specific measures to protect the fundamental interests and rights of the interested

3. The personal data referred to in section 1 may be processed for the purposes mentioned in section 2, letter h), when its treatment is carried out by a professional subject to the obligation of professional secrecy, or under his responsibility, in agreement with the Law of the Union or of the Member States or with the rules established by the competent national organisms, or by any other person also subject to the obligation of secrecy in accordance with the Law of the Union or of the Member States or of the rules established by the competent national bodies.

4. Member States may maintain or introduce additional conditions, including limitations, with respect to the treatment of genetic data, biometric data or health-related data.

And article 9 of Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (hereafter, LOPDGDD), referring to the special categories of data, among which are the data of health, determines in its section 2 the following:

2. The data treatments provided for in letters g), h) ii) of article 9.2 of Regulation (EU) 2016/679 based on Spanish law must be covered by a rule with the rank of law, which may establish additional requirements regarding its security and confidentiality. In particular, this rule can protect the processing of data in the field of health when this is required by the management of health and social assistance systems and services, public and private, or the execution of a contract insurance of which the affected person is a party.

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

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

- 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.

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.

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

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 the data and documents of the clinical history 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 point 1 of the proven facts section, which is considered constitutive of the violation provided for in article 83.5.a) of the RGPD, which typifies as thus the violation of *"the basic principles for the treatment",* among which the principle of lawfulness is at the top.

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

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

> *"The processing of personal data of the categories referred to in article 9 of Regulation (EU) 2016/679, without any of the circumstances provided for in the aforementioned precept and article 9 of this Organic Law"*

4. With regard to the fact described in point 2 of the proven facts section, relating to data security, it is necessary to refer to article 32 of the RGPD, which provides that:

> *"1. Taking into account the state of the art, the costs of application, and the nature, scope, context and purposes of the treatment, as well as risks of variable probability and severity for the rights and freedoms of natural persons, the person responsible and the person in charge of the treatment will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk, which in its case includes, among others:* a) *the pseudonymization and encryption of personal data, b) the ability to guarantee the confidentiality, integrity, availability and quickly verification, evaluation and assessment of the effectiveness of the technical and organizational measures to guarantee the security of the treatment.* 2.
>
> *the ability to restore availability and access to data*
>
> *When evaluating the adequacy of the level of security, particular consideration will be given to the risks presented by data processing, in particular as a result of the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the unauthorized communication or access to said data.* 3.
>
> *Adherence to a code of conduct approved in accordance with article 40 or a certification mechanism approved in accordance with article 42 may serve as an element to demonstrate compliance with the requirements established in section 1 of this article.* 4.
>
> *The person in charge and the data controller will take measures to ensure that any person who acts under the authority of the data controller or the data controller and has access to personal data can only process said data following the instructions of the data controller, unless they are required to do so by virtue of law of the Union or of the Member States".*

Also article 9.4 of the aforementioned Law 21/2000, determines that *"health centers must take the appropriate technical and organizational measures to protect personal data*

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

collected and avoid its destruction or accidental loss, and also access, alteration, communication or any other processing that is not authorized".

Regarding the conduct described in point 2 of the proven facts section, it is considered that the FSFA has violated the security of the data since, on the one hand, the credentials linked to an employee of the entity, which allowed the access to the HC3 through the BSA platform, were used indiscriminately by other people working in the organization, so it was impossible to identify which specific person would have carried out certain access or activities in relation to the HC3. And on the other hand, the use of the same credentials by different people would have meant, in turn, that the FSFA could not analyze the justification of access to the HC3 made by its staff.

In accordance with what has been explained, the conduct described in point 2 of the section on proven facts constitutes an infringement provided for in article 83.4.a) of the RGPD, which typifies as such the violation of " the *obligations of the person in charge and of the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43",* among which there is the obligation described in article 32 referring to the security of the treatment.

In turn, this conduct has been included as a serious infraction in article 73.f) of the LOPDGDD, in the following form:

"f) The lack of adoption of technical and organizational measures that are appropriate to guarantee a level of security adequate to the risk of the treatment, in the terms required by article 32.1 of Regulation (EU) 2016/679"

5. As the FSFA does not fit into any of the subjects provided for in article 77.1 of the LODGDD, the general sanctioning regime provided for in article 83 of the GDPR applies.

Article 83 of the RGPD foresees for the infractions provided for in its section 4, they are sanctioned with an administrative fine of 10,000,000 euros at the most, or in the case of a company, an equivalent amount to a maximum of 2% of the overall total annual business volume of the previous financial year, opting for the higher amount. For its part, section 5 of the same precept provides for the infractions provided for there to be sanctioned with administrative fines of 20,000 euros at the most, or in the case of a company, an amount equivalent to 4% at the most of the overall total annual business volume of the previous financial year, opting for the higher amount. This, without prejudice to the fact that, as an additional or substitute, the measures provided for in clauses a) ah) ij) of Article 58.2 RGPD may be applied.

In the present case, as explained by the instructor in the resolution proposal, the possibility of replacing the administrative fine with the reprimand provided for in Article 58.2.b) RGPD should be ruled out, given that the imputed infractions are linked to treatments of health data (which are part of the so-called special categories of data).

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

Once it has been ruled out that the administrative fine should be replaced by a warning, the amount of the administrative fine to be imposed must be determined. According to the provisions of article 83.2 of the RGPD, and also in accordance with the principle of proportionality enshrined in article 29 of Law 40/2015, as indicated by the instructor in the resolution proposal, the sanctions should be imposed of administrative fines indicated below based on the weighting between the aggravating and mitigating criteria detailed below:

5.1. With regard to proven fact 1, relating to the principle of legality, 8,000 euros (eight thousand euros).

5.2. Regarding proven fact 2, related to the breach of data security: 2,000 euros (two thousand euros).

The quantification of the fines is based on the weighting between the aggravating and mitigating criteria indicated below:

On the one hand, we appreciate the following circumstances that operate as mitigating criteria in the grading of the fines linked to the two facts proven:

- FSFA's adherence to the code of conduct of the Catalan Hospitals Union (art. 83.2.j RGPD).
- The lack of profits obtained as a result of the commission of the infringement (art. 83.2.k RGPD and art. 76.2.c LOPDGDD).
- That the FSFA is a non-profit organization (art. 83.2.k).

Apart from these mitigating factors which, as has been said, have been taken into account in the graduation of the two fines that are proposed to be imposed, the following mitigating criterion linked to the proven fact 1 must be taken into consideration.

- Lack of intentionality (art. 83.2.b RGPD).

And, the following mitigating factor linked to the 2nd proven fact:

- According to the actions, FSFA had blocked access to HC3 through the BSA platform before it was aware of the start of inspection actions by this Authority (art. 83.2.k RGPD) .

Regarding the analysis of the mitigating circumstances that have been related and that have been taken into consideration when setting the amount of the fines, it should be noted that most of them have been invoked by the FSFA. On the contrary, this Authority cannot take into account as a mitigating circumstance - invoked by the entity - the exceptional pandemic situation that occurred from March 2020 and which would have led to access to the medical histories of its workers. As we have already advanced to the 2nd legal basis, the situation is certainly complicated

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

exceptional that occurred at that time in the social and health centers could in no way protect access to the clinical histories of the affected people. Apart from the fact that, as has also been said, some of the accesses were prior to that period.

In contrast to the mitigating factors set out, a series of criteria from article 83.2 of the RGPD operate in an aggravating sense, and which have been taken into account to set the amount of the two fines:

- Linking the activity of the FSFA with the processing of personal data (art. 83.2.k of the RGPD and 76.2.b/ of the LOPDGDD).
- The continuing nature of the offense (art. 83.2.ki 76.2.a LOPDGDD).
- The nature, gravity and duration of the infringement, taking into account the nature, scope and purpose of the treatment operation in question, as well as the number of interested persons affected (art. 83.2.a/). The number of workers affected by unauthorized access (24), as well as the number of accesses carried out, is taken into consideration here.

6. On the other hand, in accordance with article 85.3 of the LPAC and as advanced in the initiation agreement and also in the resolution proposal, if before the resolution of the sanctioning procedure the entity accused acknowledges his responsibility or makes voluntary payment of the pecuniary penalty, a 20% reduction should be applied on the amount of the provisionally quantified penalty. If the two aforementioned cases occur, the reduction is applied cumulatively (40%).

As has been advanced, the effectiveness of the aforementioned reductions is conditional on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction (art. 85.3 of the LPAC, *in fine).*

Well, as indicated in the antecedents, the accused entity has recognized its responsibility and on 03/04/2022 has paid 6,000 euros (six thousand euros) in advance, corresponding to the sum of the amounts of the penalties resulting once the cumulative reduction of 40% has been applied (4,800 + 1,200).

7. Given the findings of the violations provided for in art. 83 of the RGPD in relation to privately owned files or treatments, article 21.3 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, empowers the director of the Authority for the resolution declaring the infringement to establish the appropriate measures so that its effects cease or are corrected. By virtue of this power, it is necessary to say the following:

7.1.- In relation to proven fact 1 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.

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

7.2. In relation to proven fact 2, specifically, regarding the use of the same credentials by several people to access the HC3 through the BSA platform, it is also not considered appropriate to require the adoption of any measures since as it has progressed, FSFA has already blocked access to HC3 through said platform.

7.3. At the very least, it is proposed to require the FSFA to implement in the GENOMI system (the application through which the FSFA currently has access to clinical records) the appropriate measures to ensure 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 the clinical histories, with the preparation of the corresponding report.

Once the corrective measure described in section 7.3 above has been adopted within the specified period, the FSFA must inform the Authority within the following 10 days, without prejudice to the inspection faculty of this Authority to carry out the corresponding checks.

For all this, I resolve:

1. To impose on the Sant Francesc d'Assis Foundation two sanctions consisting of two administrative fines, one of 8,000 euros (eight thousand euros), as responsible for an infringement provided for in article 85.5.a), in relation to the Article 5.1.a); and, a fine of 2,000 euros (two thousand euros) for the infringement provided for in article 85.4.a), in relation to article 32, all of them of the RGPD.

2. Declare that the Sant Francesc d'Assisi Foundation has made effective the advance payment of 6,000 euros (six thousand euros), which corresponds to the total amount of the two penalties imposed, once the percentage of deduction of 40% corresponding to the reductions provided for in article 85 of the LPAC has been applied.

3. Request the Sant Francesc d'Assisi Foundation to adopt the indicated corrective measure in section 7.3 of the 7th legal foundation and certify before this Authority the actions carried out to comply with it.

4. Notify this resolution to the Sant Francesc d'Assisi Foundation.

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.

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

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,