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

Identificació de l'expedient

Resolució del procediment sancionador núm. PS 32/2019, referent al Consorci Sanitari Integral

Antecedents

1. En data 19/12/2018 el Consorci Sanitari Integral (en endavant, CSI) va notificar a aquesta Autoritat una violació de seguretat (en endavant, NVS) en la qual s'informava que la Sra. (...) (...), qui presta serveis a l'Hospital Dos de Maig -integrat al Consorci Sanitari Integral (en endavant, CSI), havia accedit, a través del sistema de gestió d'històries clíniques del CSI, 38 vegades (compreses en el període 03/03/2017 fins el 03/12/2018) a la història clínica compartida d'una persona identificada a la NVS, sense que aparentment aquest accés estigués justificat per raons assistencials, ni tampoc comptés amb el consentiment de la persona afectada.

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 361/2019), d'acord amb el que preveu l'article 7 del Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat, i l'article 55.2 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (d'ara endavant, LPAC), per determinar si els fets notificats a l'Autoritat eren susceptibles de motivar la incoació d'un procediment sancionador, la identificació de la persona o persones que en poguessin ser responsables i les circumstàncies rellevants que hi concorrien.

3. En aquesta fase d'informació, en data 15/01/2019 es va requerir el CSI perquè donés compliment al següent:

a) Confirmés que els 38 accessos efectuats per la Sra. (...) a la història clínica de la persona afectada no estaven justificats per cap raó assistencial, ni comptaven tampoc amb el consentiment de la persona afectada.
b) Indiqués si el CSI, en les dates en què es van produir els accessos controvertits, tenia implementat al sistema de gestió d'històries clíniques les mesures apropiades per garantir un nivell de seguretat adequat al risc que inclogués un procés de verificació, avaluació i valoració regulars de l'eficàcia de les mesures de seguretat implementades, com podria ser l'exigència d'efectuar una revisió mensual de la informació registrada sobre els accessos a les dades dels pacients, amb l'elaboració del corresponent informe.
c) Aportés una còpia del registre d'accessos a la història clínica compartida de la persona afectada realitzats a través del sistema de gestió d'històries clíniques del CSI, en el qual constés, en relació amb els 38 accessos controvertits, a banda de la data i hora de l'accés, les pantalles o recursos als quals es va accedir.
d) Indiqués la categoria professional que ostentava la Sra.(...) (...) a la organització.

e) Informés si el CSI havia iniciat algun expedient (d'informació reservada o disciplinari) en relació amb l'actuació de la Sra. (...) i, en cas afirmatiu, aportés una còpia.

4. En data 08/02/2019 el CSI va respondre el requeriment a través d'escrit en què esposava el següent:

- Que *"en el moment dels accessos a través del nostre aplicatiu de la Sra. (...), la persona afectada no tenia cap relació assistencial amb els nostres centres".* Que *"a les entrevistes mantingudes amb la persona afectada, aquesta manifesta que la Sra. (...) no ha tingut el seu consentiment per fer aquests accessos".*
- Que la Sra. (...) *"és infermera del (...)"* .
- Que *"no hi ha cap activitat assistencial a la història clínica de la persona afectada (no cursos clínics, no analítiques, no documents, no tractament...)"*
- Que *"les revisions i auditories d'històries clíniques i accessos indeguts es feien de manera aleatòria sense una sistemàtica definida ni amb la generació d'informes dels registres. Amb l'entrada en vigor del nou reglament europeu, s'ha assignat una persona responsable en protecció de dades per dinamitzar, entre altres temes, aquests controls. Emmarcats en el procés de millora continua, s'ha generat el procediment sistemàtic i programat de revisió i audit (sic) dels accessos a les històries clíniques".*
- Que *"el CSI va obrir actuacions reservades de caràcter intern en verificació i constatació de les actuacions en matèria de protecció de dades en què podia haver incorregut la professional, des del moment en què se'ns van posar en coneixement els fets, havent donat curs a l'obertura d'un expedient informatiu en ordre laboral per resoldre les responsabilitats disciplinàries que* concorrin *al cas, restant en aquest moment a l'espera de les seves conclusions".*

El CSI aportava un extracte del registre d'accessos a la història clínica compartida de la persona afectada, en el qual consten 38 accessos efectuats per la Sra. (...), entre els dies 03/03/2017 i 03/12/2018. La pràctica totalitat d'aquests accessos (35) es van produir a partir del setembre del 2018.

5. En data 25/02/2019 va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit de la persona identificada a la NVS com a titular de la història clínica compartida, en què denunciava al CSI pel mateixos fets que havien estat objecte de la NVS.

A aquesta denúncia se li assignà el núm. IP 56/2019.

6. En data 17/10/2019, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra el CSI, en primer lloc, per una presumpta infracció prevista a l'article 83.5.a), en relació amb l'article 6; i, en segon lloc, per una presumpta infracció prevista a l'article 83.4.a) en relació a l'article 32; tots ells del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27/4, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes (en endavant, RGPD).

Aquest acord d'iniciació es va notificar a l'entitat imputada en data 29/10/2019.

7. A l'acord d'iniciació es concedia a l'entitat imputada un termini de 10 dies hàbils, comptadors a partir de l'endemà de la notificació, per formular al·legacions i proposar la pràctica de proves que considerés convenients per defensar els seus interessos.

El termini s'ha superat amb escreix i no s'han presentat al·legacions.

Fets provats

Del conjunt de les actuacions practicades en aquest procediment, es consideren acreditats els fets que es detallen a continuació:

1. Una professional que presta serveis al CSI com a infermera, va accedir 38 vegades a la història clínica compartida d'una persona, sense que aquests accessos tinguessin relació amb cap actuació assistencial/administrativa, ni tampoc comptessin amb el consentiment de la persona afectada.

Els 38 accessos es van produir entre el 03/03/2017 i el 03/12/2018, si bé gairebé tots (35) varen tenir lloc a partir de setembre de 2018.

2. El CSI no revisa periòdicament la informació de control registrada al registre d'accessos, ni elabora informes sobre les revisions realitzades i els problemes detectats. Aquesta situació s'hauria mantingut almenys fins el novembre-desembre de 2018, quan es van produir els darrers accessos no justificats a la història clínica de la persona afectada.

Fonaments de dret

1. Són d'aplicació a aquest procediment el que preveuen l'LPAC, i l'article 15 del Decret 278/1993, segons el que preveu la DT 2a de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades. De conformitat amb els articles 5 i 8 de la Llei 32/2010, la resolució del procediment sancionador correspon a la directora de l'Autoritat Catalana de Protecció de Dades.

2. D'acord amb l'article 64.2.f) de l'LPAC i de conformitat amb el que s'indica a l'acord d'iniciació d'aquest procediment, escau dictar aquesta resolució sense una proposta de resolució prèvia, atès que l'entitat imputada no ha formulat al·legacions a l'acord d'iniciació. Aquest acord contenia un pronunciament precís sobre la responsabilitat imputada.

3. En relació amb els fets descrits a l'apartat 1 de fets provats, i a la vista de les actuacions que consten en aquest procediment, es considera més ajustat tipificar-los com una

vulneració del principi de confidencialitat de les dades (i no com un tractament il·lícit), recollit a l'article 5.1.f) del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27/4, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes (en endavant, RGPD). Cal precisar que aquest canvi de qualificació no comporta un agreujament del tipus infractor.

L'article 5.1.f) de l'RGPD determina el següent:

> *"Los datos personales serán:*
> *(...)*
> *f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".*

Per la seva banda, l'article 5 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (en endavant, LOPDGDD), determina el següent:

> *"1. Els responsables i encarregats del tractament de dades així com totes les persones que intervinguin en qualsevol fase d'aquest estan subjectes al deure de confidencialitat a què es refereix l'article 5.1.f) del Reglament (UE) 2016/679.*
> *2. L'obligació general que assenyala l'apartat anterior és complementària dels deures de secret professional de conformitat amb la seva normativa aplicable.*
> *3. Les obligacions que estableixen els apartats anteriors es mantenen encara que hagi finalitzat la relació de l'obligat amb el responsable o encarregat del tractament".*

La legislació sanitària, aplicable al cas, regula l'ús de la història clínica en els següents termes:

- Article 11 Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica.

> *Usos de la història clínica*
> *1. La història clínica és un instrument destinat fonamentalment a ajudar a garantir una assistència adequada al pacient. A aquest efecte, els professionals assistencials del centre que estan implicats en el diagnòstic o el tractament del malalt han de tenir accés a la història clínica.*

2. Cada centre ha d'establir el mecanisme que faci possible que, mentre es presta assistència a un pacient concret, els professionals que l'atenen puguin, en tot moment, tenir accés a la història clínica corresponent.
3. Es pot accedir a la història clínica amb finalitats epidemiològiques, d'investigació o docència, amb subjecció al que estableix la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, i la Llei de l'Estat 14/1986, de 25 d'abril, general de sanitat, i les disposicions concordants. L'accés a la història clínica amb aquestes finalitats obliga a preservar les dades d'identificació personal del pacient, separades de les de caràcter clinicoassistencial, llevat que aquest n'hagi donat abans el consentiment.
4. El personal que té cura de les tasques d'administració i gestió dels centres sanitaris pot accedir només a les dades de la història clínica relacionades amb les dites funcions.
5. El personal al servei de l'Administració sanitària que exerceix funcions d'inspecció, degudament acreditat, pot accedir a les històries clíniques, a fi de comprovar la qualitat de l'assistència, el compliment dels drets del pacient o qualsevol altra obligació del centre en relació amb els pacients o l'Administració sanitària.
6. Tot el personal que accedeix en ús de les seves competències a qualsevol classe de dades de la història clínica resta subjecte al deure de guardar-ne el secret.

- Article 16 de la Llei 41/2002, de 14 de novembre, *"básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica"*

"Artículo 16. Usos de la historia clínica.
1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.
2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.
3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.
Asimismo, se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.
Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.
4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.
5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.
6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.
7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso".

Aquesta Autoritat considera que durant la tramitació d'aquest procediment s'ha acreditat degudament el fet descrit al punt 1r de l'apartat de fets provats, constitutiu de la infracció prevista a l'article 83.5.a) de l'RGPD, que tipifica com a tal la vulneració dels *"principios básicos para el tratamiento (…)",* en concret, del principi de confidencialitat de les dades.

La conducta que aquí s'aborda s'ha recollit com a infracció molt greu a l'article 72.1.i) de l'LOPDGDD, en la forma següent:

"i) La vulneració del deure de confidencialitat que estableix l'article 5 d'aquesta Llei orgànica".

4. Pel que fa al fet descrit al punt 2 de l'apartat de fets provats, cal acudir a l'article 32 de l'RGPD, que preveu el següent pel que fa a la seguretat del tractament:

> *"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
> a) *la seudonimización y el cifrado de datos personales;*
> b) *la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
> c) *la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
> d) *un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*
> 2. *Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.*
> *(…)"*

Per la seva banda, l'article 103.5 del Reial decret 1720/2007, de 21 de desembre, de protecció de dades de caràcter personal, aplicable en allò que no s'oposi a l'RGPD, determina el següent en relació al registre d'accessos:

> *"(...)*
> *5. El responsable de seguretat s'ha d'encarregar de revisar almenys una vegada al mes la informació de control registrada i ha d'elaborar un informe de les revisions realitzades i els problemes detectats".*

A més de l'anterior, també a mode de pauta o referència es pot afegir que el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració electrònica, defineix el "registre d'activitat" al seu article 23:

> *"Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la*

información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa".

L'apartat 4.3.8 de l'Annex II ("Mesures de Seguretat") de l'ENS, determina el següent:

"Se registrarán las actividades de los usuarios en el sistema, de forma que: a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información.
b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.
c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados.
d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1]).
Nivel BAJO Se activarán los registros de actividad en los servidores.
Nivel MEDIO Se revisarán informalmente los registros de actividad buscando patrones anormales.
Nivel ALTO Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada".

I l'Annex 1 de l'ENS, relatiu a "*Categories dels sistemes*" determina que:

c) Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:
1.º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
2.º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.
3.º El incumplimiento grave de alguna ley o regulación.
4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5.º Otros de naturaleza análoga.

Cal afegir en relació amb l'ENS que el "Centro Criptológico Nacional" (de l'Estat Espanyol) ha elaborat una "*Guía de implantación del ENS*" (actualitzada a juny 2017) en quin punt 4.3.8 estableix el següent en relació amb el *"Registro de la actividad de los usuarios"*

> *"225. Se realiza una inspección regular de los registros para identificar anomalías en el uso de los sistemas (uso irregular o no previsto)*
> *226. Se utilizan herramientas automáticas para recoger y analizar los registros en busca de actividades fuera de lo normal (por ejemplo: consola de seguridad centralizada, SIEM"*

Durant la tramitació d'aquest procediment s'ha acreditat degudament el fet descrit al punt 2n de l'apartat de fets provats, que és constitutiu de la infracció prevista a l'article 83.4.a) de l'RGPD, que tipifica com a tal la vulneració de *"las obligaciones del responsable y del encargado (...)",* en aquest cas relacionades amb la implementació de mesures de seguretat.

La conducta que aquí s'aborda s'ha recollit com a infracció greu a l'article 73.f) de l'LOPDGDD, en la forma següent:

> *"f) La falta d'adopció de les mesures tècniques i organitzatives que siguin apropiades per garantir un nivell de seguretat adequat al risc del tractament, en els termes que exigeix l'article 32.1 del Reglament (UE) 2016/679".*

5. L'article 77.2 de l'LOPDGDD disposa que, en el cas d'infraccions comeses pels responsables o encarregats enumerats a l'article 77.1 de l'LOPDGDD, l'autoritat de protecció de dades competent:

> *"(...) ha de dictar una resolució que les sancioni amb una amonestació. La resolució ha d'establir així mateix les mesures que escaigui adoptar perquè cessi la conducta o es corregeixin els efectes de la infracció que s'hagi comès.*
> *La resolució s'ha de notificar al responsable o encarregat del tractament, a l'òrgan del qual depengui jeràrquicament, si s'escau, i als afectats que tinguin la condició d'interessat, si s'escau."*

I l'apartat 3r de l'art. 77 LOPDGDD, estableix que:

> *"3. Sense perjudici del que estableix l'apartat anterior, l'autoritat de protecció de dades ha de proposar també la iniciació d'actuacions disciplinàries quan hi hagi indicis suficients per fer-ho. En aquest cas, el procediment i les sancions que s'han d'aplicar són els que estableix la legislació sobre règim disciplinari o sancionador que sigui aplicable.*

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

> *Així mateix, quan les infraccions siguin imputables a autoritats i directius, i s'acrediti l'existència d'informes tècnics o recomanacions per al tractament que no s'hagin atès degudament, en la resolució en què s'imposi la sanció s'ha d'incloure una amonestació amb la denominació del càrrec responsable i se n'ha d'ordenar la publicació al «Butlletí Oficial de l'Estat» o autonòmic que correspongui."*

En termes similars a l'LOPDGDD, l'article 21.2 de la Llei 32/2010, determina el següent:

> *"2. En el cas d'infraccions comeses amb relació a fitxers de titularitat pública, el director o directora de l'Autoritat Catalana de Protecció de Dades ha de dictar una resolució que declari la infracció i estableixi les mesures a adoptar per a corregir-ne els efectes. A més, pot proposar, si escau, la iniciació d'actuacions disciplinàries d'acord amb el que estableix la legislació vigent sobre el règim disciplinari del personal al servei de les administracions públiques. Aquesta resolució s'ha de notificar a la persona responsable del fitxer o del tractament, a l'encarregada del tractament, si escau, a l'òrgan del qual depenguin i a les persones afectades, si n'hi ha".*

5.1.- Pel que fa al fet provat 1r i ateses les circumstàncies concurrents, no es considera procedent requerir l'adopció de mesures correctores, ja que es tractaria d'uns fets puntuals ja consumats.

5.2.- Pel que fa al fet provat 2n, es requereix al CSI per tal que al més aviat possible i en tot cas en el termini màxim d'un mes a comptar del dia següent al de la notificació d'aquesta resolució, implementi en els seus sistemes d'informació les mesures apropiades per garantir un nivell de seguretat adequat al risc, que permeti garantir la confidencialitat de les dades, i que inclogui un procés de verificació, avaluació i valoració regulars de l'eficàcia de les mesures de seguretat implementades (art. 32.1.d de l'RGPD), com podria ser l'exigència d'efectuar una revisió mensual de la informació registrada sobre els accessos a les dades dels pacients, amb l'elaboració del corresponent informe, en la línia del previst a l'art. 103.5 de l'RLOPD.

Un cop s'hagi adoptat la mesura correctora descrita en el termini assenyalat, en el termini dels 10 dies següents l'ICS n'ha d'informar l'Autoritat, sense perjudici de la facultat d'inspecció d'aquesta Autoritat per efectuar les verificacions corresponents.

5.3.- D'altra banda, cal assenyalar que l'article 21.2 de la Llei 32/2010, en consonància amb el que disposa l'article 77.3 de l'LOPDGDD, preveu la possibilitat que la directora de l'Autoritat proposi la iniciació d'actuacions disciplinàries, d'acord amb el que estableix la legislació vigent sobre el règim disciplinari del personal al servei de les administracions públiques. En el cas aquí analitzat aquesta Autoritat considera que no procedeix la

proposició d'actuacions disciplinàries en la mesura que el CSI ha informat a aquesta Autoritat (antecedent 4t) que va iniciar una informació reservada en relació amb els accessos injustificats que han donat origen a aquest procediment.

Resolució

Per tot això, resolc:

1. Amonestar al Consorci Sanitari Integral com a responsable, en primer lloc, d'una infracció prevista a l'article 83.5.a) en relació amb l'article 5; i en segon lloc, d'una infracció prevista a l'article 83.4.a) en relació amb l'article 32, tots ells de l'RGPD.

2. Requerir el Consorci Sanitari Integral perquè adopti les mesures correctores assenyalades a l'apartat 5.2 del fonament de dret 5è en el termini assenyalat a l'efecte, i acrediti davant d'aquesta Autoritat les actuacions dutes a terme per complir-les.

3. Notificar aquesta resolució al Consorci Sanitari Integral.

4. Ordenar que es publiqui aquesta resolució al web de l'Autoritat (apdcat.gencat.cat), de conformitat amb l'article 17 de la Llei 32/2010, de l'1 d'octubre.

Contra aquesta resolució, que posa fi a la via administrativa d'acord amb els articles 26.2 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, i 14.3 del Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades, l'entitat imputada pot interposar, amb caràcter potestatiu, un recurs de reposició davant la directora de l'Autoritat Catalana de Protecció de Dades, en el termini d'un mes a comptar des de l'endemà de la seva notificació, d'acord amb el que preveuen l'article 123 i següents de l'LPAC. També pot interposar directament un recurs contenciós administratiu davant els jutjats contenciosos administratius, en el termini de dos mesos a comptar des de l'endemà de la seva notificació, d'acord amb els articles 8, 14 i 46 de la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa.

Si l'entitat imputada manifesta a l'Autoritat la seva intenció d'interposar un recurs contenciós administratiu contra la resolució ferma en via administrativa, la resolució se suspendrà cautelarment en els termes previstos a l'article 90.3 de l'LPAC.

Igualment, l'entitat imputada pot interposar qualsevol altre recurs que consideri convenient per defensar els seus interessos.

La directora,