Expediente Nº: E/00467/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el HOSPITAL MÉDICO QUIRURGICO DE JAÉN (SERVICIO ONCOLÓGICO), dependiente del Servicio Andaluz de la Salud, en virtud de denuncia presentada por Doña ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 19 de enero de 2018, tuvo entrada en esta Agencia escrito remitido por Doña ***A.A.A.,*** en el que expone lo siguiente:

Está siendo tratada en el Complejo Hospitalario de Jaén, concretamente en el Servicio de Oncología Médica del Hospital Médico-Quirúrgico de Jaén.

Que tiene conocimiento de que personal del citado Servicio, está filtrando sus datos médicos, porque dicha información ha llegado a sus oídos.

Al parecer, la información que está difundiendo el personal del Servicio Andaluz de la Salud del citado hospital, es de personal que no pertenece a la unidad en la que está siendo tratada.

Con fecha 13 de febrero de 2018, a requerimiento de la Agencia, la denunciante aporta copia la reclamación presentada por los mismos hechos ante la Delegación territorial de Jaén del Servicio Andaluz de la Salud, en la que hace constar los mismos hechos que en la denuncia presentada ante la Agencia.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Con fecha 28 de febrero de 2018, se solicita información al Complejo Hospitalario de Jaén, en relación con los hechos denunciados y, con fecha 8 de mayo de 2018, se recibe en la Agencia la siguiente información:

1. La información clínica del Complejo se gestiona desde la aplicación DIRAYA que tiene dos módulos principales:
    a. Módulo asistencial: al que accede personal sanitario.
    b. Módulo de gestión: para modificación de datos de gestión interna y datos administrativos.
2. El registro de los accesos que se realizan a la aplicación no está disponible en el Centro, solo es accesible desde los Servicios Centrales del SAS (Servicio Andaluz de Salud).
3. No tienen constancia de que se haya difundido a terceros no autorizados ninguna información respecto a la asistencia prestada en el Centro a la denunciante.

4. Con carácter general, todo el personal del Centro, está obligado a la confidencialidad respecto a los datos de pacientes, disponiendo de un protocolo para el acceso a la información, que en ningún caso se facilita a terceros no autorizados ni se procede a la difusión de los mismos.

Con fecha 4 de junio de 2018, el Servicio Andaluz de Salud, ha remitido a esta Agencia la siguiente información, en relación con los hechos denunciados:

1. Aportan copia de la reclamación interpuesta por la denunciante, de fecha 16 de enero de 2018, que coincide con la aportada a esta Agencia por la propia denunciante.
2. Con fecha 12 de febrero de 2018, solicitaron informe a la Subdirección de Tecnologías de la Información y Comunicación del SAS, sobre los accesos a la historia clínica de la denunciante. Aportan copia de la solicitud.
3. Con fecha 6 de marzo de 2018, recibieron la información sobre los accesos que se habían realizado a la citada historia clínica, cuya copia aportan.
4. Con fecha 22 de marzo de 2018, el inspector actuante del Equipo Provincial de la Inspección de Centros y Servicios Sanitarios, realiza un informe en relación con la reclamación interpuesta por la denunciante, del que aportan copia, y en el que se pone de manifiesto que: del estudio del informe realizado sobre los accesos a la historia clínica de la denunciante, se concluye que:
    a. Entre los efectuados desde HSDU y “Atención primaria” (Centro de Salud de Mancha Real, todos ellos corresponden a consultas, imágenes de RX, informes y accesos por parte del médico de familia, oncólogo y enfermero.
    b. De los accesos realizados desde el CAE “Hospital de Jaén”, corresponden a episodios de urgencia y Cuidados Paliativos.
    c. Desde el CAE “Virgen de las Nieves” los accesos corresponden a atención prestada en urgencias.
    d. Desde el COMPLEJO HOSPITALARIO DE JAEN, se han producido 524 accesos desde el 29 de septiembre de 2015 al 26 de febrero de 2018. Los 142 accesos de 2017 corresponden a 39 procesos de atención, y los 50 accesos de 2018 corresponden a 10 procesos de atención.

       Los profesionales que accedieron pertenecen en su mayoría al Servicio de Oncología, aunque también a Digestivo, Ginecología y Documentación (para la codificación de los episodios). Alguno de los accesos corresponde a un médico investigador debidamente autorizado.
    e. Desde citaciones se han producido 48 accesos en 2017 y 19 en 2018 (hasta febrero).
    f. El informe indica que todos los accesos a la historia clínica de la denunciante se corresponden con episodios de atención prestada a la paciente tanto en Atención Primaria como Especializada.
    g. Respecto a las historias clínicas en papel, el informe indica que no se utilizan desde hace un año con excepción del Materno-Infantil y que

para poder utilizarlas hay que solicitarlas mediante una aplicación informática.

5. El informe realizado por el inspector actuante de la Junta de Andalucía tiene las siguientes CONCLUSIONES:

    a. Según la información sobre los accesos producidos en la historia clínica de la denunciante, todos los profesionales que han accedido pertenecen a la plantilla de los Servicios Hospitalarios y de Atención Primaria relacionados con la asistencia recibida, con la excepción del médico de un proyecto de investigación debidamente autorizado por el Servicio de Oncología.

    b. Todos los accesos se corresponden con episodios de atención en hospitalización, consultas y urgencias.

6. Con fecha 23 de marzo de 2018, se dio contestación a la reclamación de la denunciante, mediante escrito, cuya copia adjunta, en el que se le da traslado de las conclusiones del informe de la Inspección de Servicios.

7. Con fecha 2 de mayo de 2018, reciben un nuevo escrito de la denunciante en el que manifiesta que ha recibido la contestación a su reclamación y que solicita que se proceda a determinar quién de los profesionales que han accedido a su historia clínica ha procedido a difundir datos de la misma.

8. Con fecha 14 de mayo de 2018, se da contestación al escrito de la denunciante de 2 de mayo, informándole de que para poder acceder a su petición es imprescindible que aporte los documentos, relaciones de testigos o cualquier otra prueba que obre en su poder, en definitiva, los elementos materiales y personales necesarios para demostrar que los hechos que denuncia han sucedido, así como la identidad del presunto o presuntos autores de los mismos sobre los que poder dirigir la correspondiente actuación inspectora. Así mismo, le informan de que en caso de no aportar lo que se solicita, su reclamación será archivada con carácter definitivo.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

La Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, en su artículo 16 dedicado a los usos de la historia clínica, dispone:

“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. (…)

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."

III

El artículo 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"*Seguridad de los datos:*

Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados."

El artículo 17.1 de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

IV

El artículo 9 de la LOPD dispone lo siguiente:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento,

deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

El art. 9 de la LOPD *establece* el principio de *"seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquélla, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado".*

El RLOPD, en su artículo 81.1 señala que "*Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico*". Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104. El artículo 88, en su punto 3, se refiere al documento de seguridad.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. En el caso que nos ocupa como establece el artículo 81.3.a) del Reglamento de desarrollo de la LOPD, además de las medidas de nivel básico y medio, deberán adoptarse las medidas de nivel alto a los ficheros o tratamientos de datos de carácter personal que se refieran a datos de salud.

El artículo 88, en sus puntos 3 y 4, referido al documento de seguridad, establece lo siguiente:

"3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento."

El artículo 91 establece:

"Artículo 91 Control de acceso

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio."

El presente procedimiento trae causa de la denuncia formulada por Doña ***A.A.A.*** por las presuntas filtraciones referidas a la enfermedad que padece. Apunta a posibles accesos indebidos a su historia clínica por parte de personal ajeno a los profesionales que están atendiéndola.

Tras el exhaustivo y detallado análisis de los accesos realizados a la historia clínica de la reclamante, 524 accesos desde el día 29 de septiembre de 2015 hasta el día 26 de febrero de 2018, se ha acreditado que se corresponden con episodios de atención prestada a la paciente, en Atención Primaria y Especializada; con la excepción de algún acceso realizado por un médico investigador autorizado para ello.

Analizando las medidas de seguridad cuyo presunto incumplimiento podría haberse producido, cabe señalar que el artículo 91 del RDLOPD bajo la denominación *"Control de acceso",* dispone:

"1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones."

"2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos."

"3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados."

"4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero."

"5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio."

Los profesionales sanitarios tienen acceso al sistema operativo DIRAYA para el desarrollo de sus funciones que son garantizar la asistencia sanitaria y protección de la vida, de tal modo que el sistema se está configurado con roles adecuados para que puedan acceder a los datos de cualquier paciente al que pueda tener que prestar asistencia.

Establecidas por tanto estas medidas de seguridad como condiciones necesarias de acceso al sistema, la justificación del acceso queda bajo la estricta responsabilidad del profesional sanitario autorizado (o habilitado).

Según dispone el apartado 3 del citado art. 91 RLOPD todos los usuarios se ajustan a un perfil diferente de acceso. Dentro de estos perfiles se ha definido cuáles pueden y deben acceder exclusivamente a listas cerradas de pacientes y cuáles han de disponer de la posibilidad de acceder a otros pacientes en caso de surgir un vínculo asistencial no previsto o programado con ellos.

Por tanto debe concluirse que no se aprecia incumplimiento de las medidas se seguridad exigidas por el referido artículo 91 RLOPD por cuanto no se acredita que existan usuarios que puedan acceder a recursos con derechos distintos de los autorizados habida cuenta que el sistema establece perfiles determinados entre los que se encuentran aquellos que puedan acceder únicamente a listas cerradas de pacientes, y aquellos otros, que caso de surgir un vínculo asistencial no previsto puedan disponer de la posibilidad de acceder para cumplir con la obligación de prestación de la asistencia sanitaria.

Por otra parte en relación con el cumplimiento de lo dispuesto en el artículo 103 del RDLOPD, bajo la denominación "Registro de accesos", se establece lo siguiente":

"1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado."

"2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido."

"3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos."

"4. El periodo mínimo de conservación de los datos registrados será de dos años."

"5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados."

Ha quedado acreditado que el sistema DIRAYA dispone de un control de accesos que cumple con lo exigido por tanto por el RLOPD por cuanto el Servicio Andaluz de Salud aportó en el procedimiento documentación que acredita tal extremo siendo identificados los usuarios, fecha y hora, tipo de acceso y su autorización, que accedieron a la historia clínica de la denunciante, identificación posible gracias a la existencia de tarjeta identificativa del profesional, su firma electrónica reconocida, y su identificación como usuario del sistema con contraseña personal. Todos los accesos efectuados durante dos años y medio están legitimados por las funciones que han realizado los profesionales que accedieron.

Cabe concluir, por tanto, que en el presente caso que se han cumplido con las medidas de seguridad exigidas por el art. 93 (control de accesos) y 103 (registro de accesos) del RLOPD, tendentes a evitar accesos no autorizados (art. 9 de la LOPD) al acreditarse que se dispone de un control y un registro de accesos a las historias clínicas, así como de perfiles diferentes para el acceso a las historias clínicas según su vinculación asistencial con los titulares de las mismas.

Conforme a los anteriores hechos y fundamentos de derecho procede en el presente caso el archivo del presente procedimiento por no apreciarse infracción de lo dispuesto en el artículo 9 de la LOPD, en relación con los artículos 91 y 103 del RLOPD.

V

Por otro lado, la reclamante se refiere a que se ha vulnerado la confidencialidad y que terceros conocen su patología. El artículo 10 de la LOPD establece que *"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."*

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento. Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española. En efecto, este precepto en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30/11, contiene un *"…instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos". "Este derecho fundamental a la*

protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino" que impida que se produzcan situaciones atentatorias con la dignidad de la persona, "es decir, el poder de resguardar su vida privada de una publicidad no querida."

El deber de secreto profesional que incumbe a los responsables de los ficheros y a quienes intervienen en cualquier fase del tratamiento, recogido en el artículo 10 de la LOPD, comporta que el responsable de los datos almacenados o tratados no pueda revelar ni dar a conocer su contenido, teniendo el *"deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo*". Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la protección de datos a que se refiere la citada Sentencia del Tribunal Constitucional 292/2000, y por lo que ahora interesa, comporta que los datos personales no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

En el presente caso, se denuncia a trabajadores del Hospital de Jaén de una vulneración de dicho deber de guardar secreto, al filtrar informaciones médicas de la reclamante.

VI

El artículo 28.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece:

"*Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa*".

De las actuaciones previas de investigación llevadas a cabo por esta Agencia y por la Junta de Andalucía no se derivan elementos probatorios de los que se infiera que trabajadores del Centro denunciado resulten responsables de los hechos constitutivos de infracción.

En este sentido, debe tenerse en cuenta que en el ámbito administrativo sancionador son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, teniendo plena virtualidad el principio de presunción de inocencia, que debe regir en el ordenamiento sancionador y ha de ser respetado en la imposición de cualesquiera sanciones. Esto, porque el ejercicio del *ius puniendi*, en sus diversas manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

En este sentido se ha pronunciado reiteradamente el Tribunal Constitucional, entre otras en SSTC 120/1994 y 76/1990, señalando en esta última que *"… la presunción de inocencia rige sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, sean penales, sean administrativas en general o tributarias en particular".*

Expone también el Tribunal Constitucional en la Sentencia 76/1990 que el derecho a la presunción de inocencia comporta *"que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio".*

Por otra parte, la Sentencia del Tribunal Constitucional de 20/02/1989 afirma que *"Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate."*

Así mismo, se debe tener en cuenta lo que establece el artículo 53.2 la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas: "*Además de los derechos previstos en el apartado anterior, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables, tendrán los siguientes derechos: (…) b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario*".

En el presente caso, en aplicación del principio de presunción de inocencia, que impide imponer una sanción en el caso de que exista una falta de pruebas respecto de un hecho concreto y determinante, no procede activar un procedimiento sancionador, al no estar acreditada la comisión de las infracciones imputadas.

Como ya se indicó, en el informe de conclusiones de los Inspectores de la Junta de Andalucía, los profesionales que accedieron a la historia clínica de la denunciante pertenecen a la plantilla de los Servicios Hospitalarios y de Atención Primaria relacionados con la asistencia recibida, con la excepción del médico de un proyecto de investigación debidamente autorizado por el Servicio de Oncología. Todos los accesos se corresponden con episodios de atención en hospitalización, consultas y urgencias.

No resulta posible, por ello, imputar las conductas típicas y antijurídicas que establece el artículo 44.3 de la LOPD al Hospital de Jaén, dependiente del Servicio Andaluz de Salud, siendo la solución procedente en derecho el archivo de las actuaciones.

VII

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución al HOSPITAL MÉDICO QUIRURGICO DE JAÉN (SERVICIO ONCOLÓGICO), al Servicio Andaluz de la Salud y a Doña ***A.A.A.***.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la LJCA, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos