



Expediente Nº: E/02822/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el **SERVICIO CANARIO DE SALUD**, en virtud de denuncia presentada por Doña **A.A.A.**, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 30 de abril de 2018, tuvo entrada en esta Agencia un escrito remitido por Doña **A.A.A.**, en el que expone lo siguiente:

Al solicitar el Acceso a su Historia clínica, detectó accesos desde dos Centros de Salud con los que no tiene vinculación alguna; en concreto, un médico, en fecha 2 de octubre de 2016 y una enfermera, el día 1 de diciembre de 2014.

Solicitó información al Servicio Canario de Salud, que le indicó, con fecha 26 de marzo de 2018, mediante escrito, que procedían a solicitar un Informe de los hechos. No obstante, hasta la fecha en la que presenta esta denuncia, no ha recibido respuesta.

Anexa, entre otra, la siguiente documentación:

Copia de su reclamación ante el Hospital.

Copia del escrito de contestación de fecha 26 de marzo de 2018.

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:

1. Con fechas 6 y 12 de julio de 2018, tienen entrada en esta Agencia dos escritos del Servicio Canario de Salud (Gerencia de Servicios Sanitarios-Área de Salud de Lanzarote), en los que se pone de manifiesto que:
 - 1.1. Tras la reclamación presentada por la denunciante, la Gerencia de Servicios Sanitarios solicitó, con fecha 13 de marzo de 2018, Informe a la Oficina de Seguridad de la Información sobre los registros generados en la Historia clínica de la denunciante el día 2 de octubre de 2016, con indicación de los profesionales que accedieron y el tiempo de acceso.
 - 1.2. Con fecha 13 de abril, se remite informe desde la Oficina de Seguridad de la Información, en el que se pone de manifiesto, entre otros:
 - 1.2.1. *... se emite Informe de los accesos realizados el 02 de octubre de 2016, desde Atención Primaria.*
 - 1.2.2. *No se han detectado accesos a su Historia clínica desde Atención Especializada en la fecha indicada.*



- 1.2.3. *Así mismo, no constan cesiones a terceros*
- 1.3. A la vista del citado Informe, que refleja que la persona identificada por la reclamante accedió a la historia clínica, se están realizando las comprobaciones pertinentes con el fin de verificar si se trata de un acceso justificado, amparado por la normativa legal o, por el contrario, un acceso indebido a la historia clínica.
- 1.4. El responsable de los datos de Historias clínicas de los pacientes es la Dirección del Servicio Canario de Salud.
2. Con fecha 7 de agosto de 2018, se recibe escrito de la Gerencia de Servicios Sanitarios del Área de Salud de Lanzarote, en el que se pone de manifiesto que:
- 2.1. Con relación a los accesos realizados a la Historia Clínica de Atención Primaria de la denunciante, la Gerencia de Servicios Sanitarios inició tramitación de expediente de información previa y reservada, mediante Resolución 1380/2018 de 2 de mayo de 2018, que fue archivado mediante Resolución número 2295/2018, de 13 de julio de 2018. A la vista de las Diligencias se puede concluir lo siguiente:
- 2.1.1. *Se encuentra acreditado el acceso por parte de D. **B.B.B.** a la Historia Clínica de Atención Primaria de Doña **A.A.A.** el día 2 de octubre de 2016.*
- 2.1.2. *Se encuentra acreditado que con fecha 2 de octubre de 2016, D. **B.B.B.** estaba adscrito a la Gerencia de Servicios Sanitarios del Área de Salud de Lanzarote mediante nombramiento como personal estatuario temporal interino con la categoría de Médico de Familia del Servicio de Urgencias Extrahospitalarias.*
- 2.1.3. *Se encuentra acreditado que D. **B.B.B.** realiza el acceso en su turno de trabajo.*
- 2.1.4. *No constan cesiones a terceros.*
- 2.2. En estos términos fue informada la reclamante, en virtud de escrito a esa Gerencia de Servicios Sanitarios de fecha 16 de julio de 2018, con registro de salida 17 de julio de 2018, y fue notificado con fecha 26 de julio de 2018.

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

El objeto de la denuncia es verificar el acceso efectuado a la historia clínica de la denunciante por parte de un médico el día 2 de octubre de 2016. El acceso anterior al que se refiere en su escrito es del año 2014.



En primer lugar y acerca de la finalidad de la historia clínica, 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.”

Por otra parte, el artículo 17 de la misma Ley, en su apartado 6 determina lo siguiente: *“Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal”.*

III

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*”.

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de “*fichero*” y “*tratamiento*” contenidas en la LOPD.

En lo que respecta a los ficheros el art. 3.b) los define como “*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*”.

Por su parte la letra c) del mismo artículo permite considerar tratamiento de datos a las “*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*.”

Para completar el sistema de protección en lo que a la seguridad afecta, el art. 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros “*...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen*”.

Sintetizando las previsiones legales puede afirmarse que:

- a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.
- b) Los ficheros que contengan un conjunto organizado de datos de carácter personal, así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.
- c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.
- d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, 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.”*

Con relación al “Registro de accesos”, el Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la LOPD, en su artículo 103 establece:

“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 período 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.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

- a) Que el responsable del fichero o del tratamiento sea una persona física.*
- b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.*

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.”

El Servicio Canario de Salud tiene registro de accesos a las historias clínicas con la finalidad de verificar la legitimidad de los mismos. Tras hacer un análisis de los accesos efectuados a la historia clínica de la denunciante, el Servicio Canario de



Salud ha informado a esta Agencia que está acreditado el acceso por parte de Dr. Don **B.B.B.** a la Historia Clínica de Atención Primaria de Doña **A.A.A.** el día 2 de octubre de 2016. Don **B.B.B.** estaba adscrito a la Gerencia de Servicios Sanitarios del Área de Salud de Lanzarote mediante nombramiento como personal estatuario temporal interino con la categoría de Médico de Familia del Servicio de Urgencias Extrahospitalarias y realizó el acceso en su turno de trabajo.

En consecuencia, no se ha acreditado incumplimiento de las medidas de seguridad.

IV

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 **SERVICIO CANARIO DE SALUD-GERENCIA DE SERVICIOS SANITARIOS AREA DE SALUD DE LANZAROTE** 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.

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