Expediente Nº: E/05952/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

Examinado el escrito presentado por el HOSPITAL UNIVERSITARIO CENTRAL DE ASTURIAS, relativo a la ejecución del requerimiento de la resolución de referencia R/02795/2017 dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento de declaración de Infracción de Administraciones Públicas AP/00041/2017, seguido en su contra, y en virtud de los siguientes

ANTECEDENTES DE HECHO

PRIMERO: En esta Agencia Española de Protección de Datos se tramitó el procedimiento de declaración de Infracción de Administraciones Públicas, de referencia AP/00041/2017, a instancia de Doña ***A.A.A.***, con Resolución de la Directora de la Agencia Española de Protección de Datos por infracción del artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (en lo sucesivo LOPD). Dicho procedimiento concluyó mediante resolución R/02795/2017, de fecha 20 de octubre de 2017 por la que se resolvía *" **REQUERIR** al Hospital Universitario Central de Asturias, dependiente del Servicio de Salud de Principado de Asturias, de acuerdo con lo establecido en el apartado 3 del artículo 46 de la Ley 15/1999, para que acredite en el plazo de un mes desde este acto de notificación las medidas de orden interno adoptadas que impidan que se produzca en el futuro una nueva infracción, como la denunciada, a la normativa de protección de datos.*
*Asimismo, deberán informar del resultado de las actuaciones llevadas a cabo para verificar la autorización o no de los accesos efectuados a la historia clínica de la denunciante por parte de Doña **B.B.B.**; medidas correctoras concretas tomadas, tanto generales como con la persona denunciada, debiéndo acreditarlo ante esta Agencia en el plazo de **UN MES** desde este acto de notificación, para lo que se abre expediente de actuaciones previas E/05952/2017, advirtiéndole que en caso contrario se procederá a acordar la apertura de un procedimiento sancionador*."

Con objeto de realizar el seguimiento de las medidas a adoptar la Directora de la Agencia Española de Protección de Datos insto a la Subdirección General de Inspección de Datos la apertura del expediente de actuaciones previas de referencia E/05952/2017.

SEGUNDO: Con motivo de lo instado en la resolución, el denunciado remitió a esta Agencia con fecha de entrada 28 de octubre de 2017, escrito en el que informaba a esta Agencia en los siguientes términos: que los antecedentes de los accesos a la historia clínica de la denunciante se trasladaron, en fecha 4 de julio de 2017, al Servicio de Inspección de la Dirección de Atención y Evaluación Sanitaria del Servicio de Salud del Principado de Asturias, quien ha iniciado un procedimiento de información previa al posible inicio de un expediente disciplinario o en su caso denuncia ante la autoridad judicial. Añaden que el acceso a las historias clínicas electrónicas era universal para los profesionales sanitarios, no existía la posibilidad de denegar el acceso a una historia clínica concreta; no obstante, la situación ha sido subsanada y es posible denegar accesos determinados a una historia clínica a un profesional.

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 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."

Por otra parte, el artículo 17 de la misma Ley, dedicado por completo a la conservación de la documentación clínica, establece en su punto primero que *"Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial" y* 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 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

La LOPD traspuso al ordenamiento interno el contenido de la Directiva 95/46, y en su artículo 1 dispone que *"la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*

El artículo 2.1 de la misma Ley Orgánica establece: *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados".*

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."

En los hechos de este procedimiento, consta probado que la denunciante es usuaria del sistema público de salud del Principado de Asturias y que tuvo conocimiento de los accesos reiterados por parte de una profesional que no tiene encomendada su asistencia sanitaria. La denunciante ha aportado con su denuncia, certificado de 7 de julio de 2016, del Servicio de Salud del Principado de Asturias de la relación de accesos realizados a su historia clínica desde el 26 de junio de 2014 hasta el 7 de julio de 2016, donde se observa que 10 accesos fueron realizados por la DUE que no es titular de su atención sanitaria.

Consta también probado que en junio de 2017 solicitó que se actuase a la unidad de atención al paciente, sin que hayamos recibido ninguna información al respecto.

La LOPD regula en su artículo 4 el principio de calidad de datos que resulta aplicable al supuesto de hecho que se analiza. Este artículo debe interpretarse de forma conjunta y sistemática. El artículo 4.1 y 2 de la LOPD, señala lo siguiente:

"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".

El artículo 4.2 prohíbe que los datos puedan usarse para una finalidad incompatible con aquella para la que fueron recogidos.

En este caso la finalidad de los datos personales contenidos en la historia clínica de los pacientes es la de la asistencia sanitaria de los mismos, y los accesos realizados por la DUE que no es el titular del cuidado sanitario de la denunciante, no parecen tener justificación clínico asistencial. Esto lleva a afirmar que la DUE autora de los numerosos accesos a la historia clínica en cuestión, trató los datos de la denunciante con una finalidad diferente de aquella para la que se han recogido y sin que en ningún caso conste acreditado que la afectada hubiera prestado su consentimiento para el nuevo tratamiento realizado

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."

Esta es la concreta medida de seguridad de las legalmente previstas en la que se observa la falta del deber de cuidado en esta ocasión, dado que el "Registro de accesos" no ha permitido detectar el problema de la cantidad de accesos injustificados a la historia clínica de la denunciante y así poder corregir la anomalía.

En conclusión, en el presente caso ha quedado acreditado que 10 accesos a fueron realizados por un profesional DUE que no tenía encargada la asistencia sanitaria de la denunciante. La entidad imputada contestó a la denunciante, en fecha 16 de junio de 2017, que su reclamación la pasaba al Jefe de Seguridad e Informática. Cuando se notificó el Acuerdo de inicio de este procedimiento, el día 11 de agosto de 2017, habían transcurrido dos meses desde el citado traslado y el HUCA no ha alegado nada acerca de la posible investigación y resultados obtenidos.

Se confirma así la existencia de accesos injustificados a la historia clínica de la

denunciante sin que la entidad responsable del fichero haya detectado esos accesos injustificados y haya adoptado alguna medida para corregir el problema.

Todo ello lleva a considerar que por parte de la entidad denunciada se carece de un efectivo control de los accesos a la información recogida en el fichero de historias clínicas de sus pacientes, para el cumplimiento del principio de seguridad de los datos, consagrado en el artículo 9 de la LOPD. Un sistema que permita, no solo conocer los registros de todos los accesos que se realizan a cada una de las historias clínicas de sus pacientes, sino también que permita, por medio de la revisión periódica de esa información, la detección de problemas tales como los accesos injustificados. Con ello se garantizaría la seguridad de los datos de carácter personal y se evitaría su alteración, pérdida, tratamiento o acceso no autorizado, en definitiva, unas medidas de seguridad adecuadas que garanticen el derecho fundamental a la protección de datos personales.

Por todo lo expuesto, se concluye que, en el presente caso si bien se dispone de un registro de accesos a las historias clínicas, este no se ha utilizado para detectar y depurar los accesos injustificados que se han denunciado en esta Agencia.

La Audiencia Nacional, en varias sentencias, exige a las entidades que operan en el mercado de datos una especial diligencia a la hora de llevar a cabo el uso o tratamiento de tales datos o su cesión a terceros, visto que se trata de la protección de un derecho fundamental de las personas a las que se refieren los datos, por lo que los depositarios de éstos deben ser especialmente diligentes y cuidadosos a la hora de realizar operaciones con los mismos y deben optar siempre por la interpretación más favorable a la protección de los bienes jurídicos protegidos por la norma.

V

El artículo 44.3.h) tipifica como infracción grave la siguiente:

"*Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

En el presente caso ha quedado acreditado que el HUCA, dependiente del Servicio de Salud del Principado de Asturias, carece de las medidas de seguridad que la Ley exige al responsable del fichero, dado que se ha constatado que se han producido de accesos injustificados a la historia clínica de la denunciante de este procedimiento.

De acuerdo con los fundamentos anteriores, se deduce que por parte del HUCA, dependiente del Servicio de Salud del Principado de Asturias, se ha producido una vulneración del principio de seguridad de los datos, que ha tenido como consecuencia que los datos personales de una paciente pertenecientes a su historia clínica, fueran objeto de acceso por parte de un profesional que carece de justificación clínico asistencial, infracción que procede calificar como grave, sin que pueda exonerarse su responsabilidad tal como se ha demostrado en este procedimiento, por lo que procede su imputación, elemento necesario en el derecho administrativo sancionador tal como establece la STS de 27/5/99: *"Para la imposición de una sanción y las consecuencias derivadas del ilícito administrativo, no basta que la infracción esté tipificada y sancionada sino que es necesario que se aprecie en el sujeto infractor el elemento o categoría denominado culpabilidad. La culpabilidad es el reproche que se hace a una persona, porque ésta debió haber actuado de modo distinto de cómo lo hizo".*

VI

Por último, el artículo 46 de la LOPD, "Infracciones de las Administraciones Públicas", dispone que:

<<. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores".>>

VII

En supuesto presente, del examen de las medidas adoptadas por el HOSPITAL UNIVERSITARIO CENTRAL DE ASTURIAS, se constata que han efectuado modificaciones en el control de accesos a las historias clínicas electrónicas por parte de los profesionales sanitarios, impidiendo el acceso universal a las mismas.

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución al HOSPITAL UNIVERSITARIO CENTRAL DE ASTURIAS**,** 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