Expediente Nº: E/04418/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el HOSPITAL SAN PEDRO DE ALCANTARA, en virtud de denuncia presentada por Don ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 4 de agosto de 2016, tuvo entrada en esta Agencia un escrito remitido por Don ***A.A.A.,*** en el que manifiesta lo siguiente:

"Ha tenido constancia del acceso a su Historia clínica por parte de un médico del Hospital de San Pedro, donde él también presta sus servicios como profesional sanitario, sin autorización expresa ni en condición de interesado.

Los hechos tuvieron lugar con fecha 31 de julio de 2014 y 24 de septiembre de 2015, según la información recibida sobre accesos a documentación clínica electrónica.

Anexa copia del citado Documento de Información sobre accesos."

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 fecha 14 de diciembre de 2016, se recibió escrito del Hospital de San Pedro, que incluye un Informe realizado por el facultativo que accedió a la Historia clínica del denunciante, poniendo de manifiesto que:

   Ambos son profesionales de la sanidad del Hospital San Pedro de Alcántara.

   El denunciante mantiene un conflicto laboral y profesional con el Servicio Extremeño de Salud, haciéndole responsable de dichos problemas.

   Para acceder al sistema (JARA) basta con conocer usuario y contraseña, por lo que con saber primer nombre, primer apellido y fecha de nacimiento, cualquiera podría acceder. Por otra parte cuando se accede al sistema cada mañana, la aplicación queda abierta, por lo que si no se cierra la sesión o se cierra por tiempo transcurrido sin actividad, y no te encuentras el puesto de trabajo, también podría acceder cualquier persona.

   No tiene noción de haber accedido al historial del denunciante. No obstante, no puede negar ni afirmar taxativamente que se haya accedido a la historia del denunciante.

2. Con fecha 7 de marzo de 2017, se recibe escrito de la Gerencia del Área de Salud de Cáceres, con el que adjuntan un Informe de Medidas de Seguridad y Advertencias Legales, manifestando que:

   Según consta en el citado Aviso Legal, al iniciar una sesión por parte de

cualquier usuario del Hospital y antes de realizar la validación mediante usuario y contraseña, el sistema muestra una ventana en la que consta, entre otros, que el usuario es el único responsable de las sesiones iniciadas. Así mismo, advierte de las responsabilidades del usuario al acceder a información para la que no tiene privilegios o no está directamente relacionada con sus funciones.

En cuanto al control realizado sobre los accesos indebidos, cualquier paciente puede solicitar el acceso a su historia y/o quien ha accedido a la misma, en base al artículo 35.3 de la Ley 3/2005, de 8 de julio de Información Sanitaria y de Autonomía del Paciente de Extremadura, facilitando este trámite al paciente, desde el Servicio Extremeño de Salud.

En el caso de que se aprecien accesos indebidos en la historia de un paciente, se procede a la depuración de responsabilidades en las que pudieran haber incurrido los profesionales de esa Gerencia.

Si de la información obtenida se observaran indicios suficientemente razonables de posible incumplimiento, se solicita a la Secretaría General, incoación de expediente disciplinario al responsable.

Por otra parte desde la Gerencia se han impartido cursos de formación al personal en este sentido, así como cursos de la aplicación (Jara) uno sobre Jara en el Hospital y otro sobre Jara en Atención Primaria. Dicho curso es impartido todos los años.

Asimismo, se imparten diferentes cursos de confidencialidad de datos personales y sanitarios, a todo el personal.

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.

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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, 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 clínico asistencial, 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 de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico asistenciales, 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, 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."

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.

V

El RDLOPD, 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.

Analizando las medidas de seguridad cuyo presunto incumplimiento se podría haber cometido por parte del Servicio Extremeño de Salud 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 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 para que puedan acceder a los datos de cualquier paciente al que pueda tener que prestar asistencia, pudiendo entrar a la historia clínica de un paciente por los motivos siguientes: Gestión de paciente, Estudio Investigación, Docencia, Auditoría de Calidad, Estudios de Medicina Preventiva, Contestación de Reclamaciones, Gestión de Historias, y Solicitud DCL.

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).

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 el de los profesionales sanitarios, que pueden acceder al fichero de pacientes, para cumplir con la obligación de prestación de la asistencia sanitaria o justificar el motivo de otros accesos.

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 Servicio Extremeño de Salud dispone de un control de accesos que cumple con lo exigido por el RLOPD por cuanto el mencionado Servicio aportó documentación que acredita tal extremo siendo identificados el usuario, fecha y hora, tipo de acceso, que accedió a la historia clínica del denunciante, identificación posible gracias a la existencia de tarjeta identificativa del profesional, y su identificación como usuario del sistema con contraseña personal. El sistema recogió los accesos del médico denunciado con habilitación de "Gestión del paciente" y

"Asistencial".

Cabe concluir por tanto que en el presente caso el sistema de información utilizado por el Servicio Extremeño de Salud, y que gestiona la historia clínica electrónica cumple 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 listas cerradas de usuarios con acceso a las historias clínicas dado su vinculación asistencial con los titulares de las mismas, y caso de no existir dicho vínculo, la existencia de medida de seguridad que impide el acceso a aquellos usuarios que no tengan dicho vínculo o una actividad programada con el paciente, exigiendo al usuario del sistema que en estos casos, incluya una justificación para el acceso a la historia clínica, justificación de la cual el sistema guarda registro de tal manera que puede comprobarse posteriormente la idoneidad o no de la referida justificación aducida por el profesional para efectuar el acceso a la historia clínica.

Conforme a los anteriores hechos y fundamentos de derecho procede en el presente caso el archivo de las presentes Actuaciones Previas por no apreciarse infracción de lo dispuesto en el artículo 9 de la LOPD, en relación con los artículos 91 y 103 del RLOPD por parte del Servicio Extremeño de Salud.

No obstante, se insta al mencionado Servicio a que audite de forma pormenorizada los accesos efectuados por el médico denunciado a la historia clínica del médico denunciante, por si pudiesen dar lugar a actuaciones disciplinarias. Asimismo, deberán comprobar las claves de acceso que se facilitan a los profesionales sanitarios, si no se deben modificar para evitar su conocimiento por terceros. Por último, deben recordar a todos los usuarios del sistema de acceso a las historias clínicas la obligación de cerrar las sesiones al abandonar el despacho para evitar que accedan terceros no autorizados.

Se traslada esta Resolución al Defensor del Pueblo para el seguimiento de las actuaciones requeridas al servicio Extremeño de Salud.

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 Extremeño de Salud, a Don ***A.A.A.,*** al Hospital San Pedro de Alcántara y al Defensor del Pueblo.

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