



Procedimiento N° AP/00005/2013

RESOLUCIÓN: R/01935/2013

En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00005/2013**, instruido por la Agencia Española de Protección de Datos a la entidad **SERVICIO MADRILEÑO DE SALUD-HOSPITAL CLINICO SAN CARLOS**, vista la denuncia presentada por D. **A.A.A.**, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 28 de enero de 2013 tiene entrada en el Registro de esta Agencia Española de Protección de Datos el presente expediente con motivo de la extinción de la Agencia de Protección de Datos de la Comunidad de Madrid prevista en el artículo 61 de la Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas de la Comunidad de Madrid para el año 2013 (B.O.C.M. de 29 de diciembre). Al objeto de garantizar la efectividad del derecho de los ciudadanos a la protección de sus datos de carácter personal, se ha trasladado el expediente a la Agencia Española de Protección de datos en los términos indicados por la Disposición transitoria tercera de la citada Ley 8/2012.

SEGUNDO: D. **A.A.A.** (en lo sucesivo el denunciante), presentó un escrito en el que expone que el día 19 de julio de 2012, fue citado en el hospital Clínico Universitario San Carlos de Madrid, al objeto de practicársele una intervención quirúrgica programada para ese día.

Que al acudir previamente al Servicio de Admisión y Documentación Clínica (Admisión de Hospitalización) del referido Hospital, por el personal de dicho Servicio se le comunica que se ha cancelado dicha intervención a causa del extravío/pérdida de su Historial Clínico. Añade en su escrito que: *“Confío, en que noticias como ésta, hagan reflexionar a las Administraciones implicadas en la responsabilidad que tienen en la custodia y gestión de información tan sensible para los ciudadanos. Es lamentable que, ante una denuncia tan clara como ésta, los gestores del Hospital o del Archivo adscrito al mismo, no salgan a dar una respuesta más clara, y a explicar si se ha debido a un error puntual o a un sistema de trabajo sin los controles de calidad necesarios.”*

TERCERO: A la vista de los hechos denunciados, se solicitó información a la entidad Servicio Madrileño de Salud, Hospital Clínico San Carlos quien, con fecha 10 de septiembre de 2012, informa que los datos de la historia clínica del denunciante figuran en el fichero del Hospital Clínico San Carlos de Madrid denominado “Documentación Clínica” y continúa informando:

“En cada episodio asistencial, la historia clínica que es custodiada por el Archivo, sale del mismo hasta la unidad asistencial que le vaya a atender y retorna una vez concluida. Adjunto hoja con el registro informático de todos los movimientos de esta historia. En ningún momento nos consta la pérdida de esta historia clínica.”

Cuando el paciente acude a la intervención programada, ésta no se puede realizar porque su historia no se puede facilitar al equipo médico ya que no es localizada dentro del Archivo. Tras la investigación interna realizada, se evidencia por nuestra parte, que esa historia ha sido archivada en lugar erróneo e inadecuado al suyo, pues el archivo está ordenado en función del número de historia. Si al incorporarla no se coloca, en su lugar adecuado, luego no se localiza al ir a buscarla precisamente a ese su sitio. He de hacer constar que en el Archivo de nuestro hospital hay alrededor de 2.000.000 de historias y 24.000 metros de estanterías. Movemos diariamente casi 5.000 historias que como la de este caso entran y salen del Archivo y que lamentablemente, existiendo el error humano, en todos los archivos físicos de los hospitales está reconocido un porcentaje de casos de este tipo. Para aplacar estos potenciales errores, cada cierto tiempo se puntea cada uno de los 24.000 metros lineales (aprox.) repasando la perfecta ubicación de cada historia, precisamente para detectar estos casos y reubicarlo subsanando el error.

Precisamente por esto descrito, disponemos de un protocolo de gestión del extravío de la historia clínica, que adjunto a este escrito. En el caso concreto que nos ocupa, amén de ponerlo en marcha, se trató con la provincia de origen y con el servicio médico afecto, de recuperar la documentación, cuestión que nos permite programar a este paciente para el próximo 3 de octubre para ser intervenido. (...)

3- Efectivamente tengo conocimiento de la reclamación presentada por el paciente. No se le ha contestado por escrito pues al estar citado el 5 de septiembre en la consulta y al estar nosotros tratando por todos los medios de resolver el error de ubicación, esperábamos darle la información en ese momento. Y de esta manera el 5 de septiembre con la oftalmóloga se le confirmó que aunque seguía extraviada dentro del Archivo, se había reconstruido la documentación necesaria y ya estaba apto, programándose fecha de intervención con él.

Es política de este hospital el velar por la satisfacción de los pacientes y por responder a sus reclamaciones lo antes posible en tiempo y forma. No obstante, en este caso concreto, la reclamación presentada por el paciente ha sido trasladada al Servicio de Responsabilidad Patrimonial del SERMAS, al objeto de que siga el trámite legal correspondiente.

4- Por último, enfatizar por nuestra parte, que la historia clínica no estaba perdida, pues consta registro de entrada en el Archivo, sino mal colocada y no localizable, por lo que no consideramos que se haya producido vulneración alguna en materia de Protección de Datos del Paciente."

CUARTO: Con fecha 17 de abril de 2013, el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas al SERVICIO MADRILEÑO DE SALUD-HOSPITAL CLINICO SAN CARLOS por la presunta infracción del artículo 9.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificada como grave en el artículo 44.3.h) de dicha norma.

QUINTO: Notificado el citado acuerdo de inicio de procedimiento de declaración de

infracción de Administraciones Públicas, el SERVICIO MADRILEÑO DE SALUD-HOSPITAL CLINICO SAN CARLOS presentó escrito de alegaciones en el que, en síntesis, manifestaba que:

“SEGUNDA Que hemos de informar que la historia clínica del paciente fue localizada en un breve espacio de tiempo, dado que no se había producido la pérdida de la misma, sino una ubicación errónea en las propias instalaciones del Archivo, De esta forma, la historia clínica ha quedado debidamente ubicada y a disposición de la asistencia sanitaria precisa.

A este respecto, cabe destacar, que nuestro archivo cuenta con aproximadamente 2.000.000 de historias clínicas y 24.000 metros de estanterías, lo que unido a los 5.000 movimientos diarios de documentación clínica, justifica que pueda producirse de manera excepcional un error humano en el archivo de las misma, tal y como ha tenido lugar en el caso que nos ocupa.

No obstante, esta circunstancia no determina, en ningún caso, que se hayan incumplido las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos, por lo que no cabe inferir vulneración alguna en materia de protección de datos.

TERCERA. Que si bien inicialmente hubo de suspenderse la intervención quirúrgica oftalmológica programada para el día 19 de julio de 2012, desde el primer momento se realizaron cuantas actuaciones resultaron necesarias para la reconstrucción de la documentación clínica, a fin de que el paciente pudiera ser intervenido a la mayor brevedad, tal y como pudo llevarse a efecto sin incidencias.

CUARTA. Que en la actualidad, se instruye por parte del Servicio Madrileño de Salud expediente de responsabilidad patrimonial, con motivo de la reclamación interpuesta por D. A.A.A., fundamentada en los mismos hechos que conforman el expediente que nos ocupa.

Asimismo y conforme obra en el citado procedimiento de responsabilidad patrimonial, según informe clínico emitido por el Servicio de Oftalmología de este hospital, el aplazamiento de la intervención quirúrgica no influyó de ninguna manera en la patología del paciente ni en su evolución, por lo que el paciente no sufró perjuicio alguno respecto a su situación clínica,

QUINTA. Que resulta preciso señalar que este hospital dispone de las medidas de seguridad previstas según la normativa que, en materia de protección de datos, se exige a las historias clínicas como ficheros no automatizados.

Dejando a salvo la incidencia acaecida tras la ausencia temporal de localización de la documentación clínica del paciente, destacar que no se ha producido alteración, pérdida, tratamiento o acceso no autorizado de la misma, tal y como preceptúa el citado art. 9. 1 de la LOPD, por lo que cabe concluir que se han cumplido estrictamente las medidas necesarias para garantizar la seguridad de los datos de carácter personal del paciente”.

SEXTO: Con fecha 21 de mayo de 2013 se acordó por el Instructor del procedimiento la

apertura de un período de práctica de pruebas, acordándose practicar las siguientes:

1. Se dan por reproducidos a efectos probatorios la denuncia interpuesta por D. **A.A.A.** y su documentación, los documentos obtenidos y generados por los Servicios de Inspección ante el **SERVICIO MADRILEÑO DE SALUD-HOSPITAL CLINICO SAN CARLOS**, y el Informe de actuaciones previas de Inspección que forman parte del expediente.
2. Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio AP/00005/2013 presentadas por el **SERVICIO MADRILEÑO DE SALUD-HOSPITAL CLINICO SAN CARLOS**, y la documentación que a ellas acompaña.

SÉPTIMO: Con fecha 2 de julio de 2013, el Instructor del procedimiento emitió Propuesta de Resolución, en el sentido de que por el Director de la Agencia Española de Protección de Datos se declare que el **SERVICIO MADRILEÑO DE SALUD-HOSPITAL CLINICO SAN CARLOS** ha infringido lo dispuesto en el artículo 9.1 de la LOPD, lo que supone una infracción tipificada como grave en el artículo 44.3.h) de la citada norma, así como que se requiera la adopción de las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 9.1 de la mencionada Ley.

De acuerdo con lo establecido en el artículo 19.1 del Real Decreto 1398/1993 de 4 de agosto, Reglamento del procedimiento para el ejercicio de la potestad sancionadora, en dicha propuesta de resolución se concedió un plazo de QUINCE DÍAS hábiles para que las partes interesadas en el procedimiento pudieran alegar cuanto considerasen para su defensa y presentasen los documentos e informaciones que estimasen pertinentes, así como se detallaba, en un anexo adjunto a esa propuesta de resolución, la relación de documentos obrantes en el procedimiento, a fin de que las partes interesadas en el procedimiento pudieran obtener copia de los que estimasen convenientes.

OCTAVO: La Propuesta de Resolución fue notificada a la entidad denunciada el día 5 de julio de 2013.

HECHOS PROBADOS

PRIMERO: El día 19 de julio de 2012, el denunciante fue citado en el hospital Clínico Universitario San Carlos de Madrid, para una intervención quirúrgica programada para ese día. En el Servicio de Admisión y Documentación Clínica del Hospital (Admisión de Hospitalización), le comunicaron que se había cancelado dicha intervención a causa del extravío/pérdida de su Historial Clínico.

SEGUNDO: La entidad denunciada ha informado que los datos de la historia clínica del denunciante figuran en el fichero del Hospital Clínico San Carlos de Madrid denominado

“Documentación Clínica” y continúa informando:

“En cada episodio asistencial, la historia clínica que es custodiada por el Archivo, sale del mismo hasta la unidad asistencial que le vaya a atender y retorna una vez concluida. Adjunto hoja con el registro informático de todos los movimientos de esta historia. En ningún momento nos consta la pérdida de esta historia clínica.

Cuando el paciente acude a la intervención programada, ésta no se puede realizar porque su historia no se puede facilitar al equipo médico ya que no es localizada dentro del Archivo. Tras la investigación interna realizada, se evidencia por nuestra parte, que esa historia ha sido archivada en lugar erróneo e inadecuado al suyo, pues el archivo está ordenado en función del número de historia. Si al incorporarla no se coloca, en su lugar adecuado, luego no se localiza al ir a buscarla precisamente a ese su sitio.”

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 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 17, 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](#)”*.

El artículo 19 de la citada Ley 41/2002 indica: *“Derechos relacionados con la custodia de la historia clínica. El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el [artículo 16 de la presente Ley](#)”*.

El Servicio Madrileño de Salud-Hospital Clínico San Carlos ha alegado al acuerdo de inicio del presente procedimiento que *“nuestro archivo cuenta con aproximadamente 2.000.000 de historias clínicas y 24.000 metros de estanterías, lo que unido a los 5.000 movimientos diarios de documentación clínica, justifica que pueda producirse de manera excepcional un error humano en el archivo de las misma, tal y*

como ha tenido lugar en el caso que nos ocupa.”

Según queda expuesto, frente a esta alegación cabe decir que los centros sanitarios están obligados a una custodia activa y diligente de las historias clínicas de sus pacientes y que en la documentación clínica hay que aplicar 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](#), según establece la Ley 41/2002, de 14 de noviembre, por la que se aprueba la Ley básica, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

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. 3 de la LOPD establece las definiciones de responsable de fichero o tratamiento, de encargado de tratamiento y de cesión de datos:

“d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

i) Cesión o comunicación de datos: toda revelación de datos realizada a la persona distinta del interesado.”

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 transcrito artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen tal seguridad, así como para impedir el acceso no autorizado a los mismos por ningún tercero.

Para poder delimitar cuáles son 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 al concepto de “fichero” el artículo 3.b) de la LOPD lo define como “*todo conjunto organizado de datos de carácter personal*”, con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la “*comunicación*” o “*consulta*” de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Para completar el sistema de protección de datos de carácter personal, el

artículo 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 citadas 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, regulado en normas reglamentarias.

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 del artículo 9 de la LOPD tipificada como grave en el artículo 44.3.h) de la citada Ley.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, define en su artículo 5.2 ñ) el *“Soporte”* como el *“objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos”*.

Por su parte el artículo 81.1 del mismo Reglamento 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.

En los hechos de este procedimiento, consta probado que el día 19 de julio de 2012, el denunciante fue citado en el hospital Clínico Universitario San Carlos de Madrid, para una intervención quirúrgica programada para ese día que hubo de suspenderse porque desde el Servicio de Admisión y Documentación Clínica del Hospital le comunicaron que su Historial Clínico se había extraviado.

El Servicio Madrileño de Salud, Hospital Clínico San Carlos, en su calidad de responsable del tratamiento de los datos de salud contenidos en las historias clínicas de sus pacientes, debió adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración y pérdida. Tales medidas no fueron

adoptadas totalmente en el presente caso, como lo acredita el hecho de que la historia clínica del denunciante se extravió.

Con relación a los criterios de archivo el Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la LOPD, en su artículo 106 establece:

“El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.”

En las alegaciones al acuerdo de inicio la entidad denunciada ha manifestado *“Que si bien inicialmente hubo de suspenderse la intervención quirúrgica oftalmológica programada para el día 19 de julio de 2012, desde el primer momento se realizaron cuantas actuaciones resultaron necesarias para la reconstrucción de la documentación clínica, a fin de que el paciente pudiera ser intervenido a la mayor brevedad, tal y como pudo llevarse a efecto sin incidencias”.*

En este mismo sentido, en las actuaciones previas de inspección se informó al respecto que: *“el 5 de septiembre con la oftalmóloga se le confirmó que aunque seguía extraviada dentro del Archivo, se había reconstruido la documentación necesaria y ya estaba apto, programándose fecha de intervención con él.(...) Por último, enfatizar por nuestra parte, que la historia clínica no estaba perdida, pues consta registro de entrada en el Archivo, sino mal colocada y no localizable, por lo que no consideramos que se haya producido vulneración alguna en materia de Protección de Datos del Paciente.”*

En las actuaciones previas de inspección se aportó copia del “Procedimiento de recuperación de documentación clínica” así como el “Listado de seguimiento de préstamos” referido a la historia clínica del denunciante. En la información aportada, previo a la iniciación del presente procedimiento, se manifiesta: *“Precisamente por esto descrito, disponemos de un protocolo de gestión del extravío de la historia clínica, que adjunto a este escrito. En el caso concreto que nos ocupa, amén de ponerlo en marcha, se trató con la provincia de origen y con el servicio médico afecto, de recuperar la documentación, cuestión que nos permite programar a este paciente para el próximo 3 de octubre para ser intervenido. (...) En cada episodio asistencial, la historia clínica que es custodiada por el Archivo, sale del mismo hasta la unidad asistencial que le vaya a atender y retorna una vez concluida. Adjunto hoja con el registro informático de todos los movimientos de esta historia. En ningún momento nos consta la pérdida de esta historia clínica.*

Cuando el paciente acude a la intervención programada, ésta no se puede realizar porque su historia no se puede facilitar al equipo médico ya que no es localizada dentro del Archivo. Tras la investigación interna realizada, se evidencia por nuestra parte, que esa historia ha sido archivada en lugar erróneo e inadecuado al suyo, pues el archivo está ordenado en función del número de historia. Si al incorporarla no se coloca, en su lugar adecuado, luego no se localiza al ir a buscarla precisamente a ese su sitio”.

En efecto, tal como se informa por la entidad imputada, en el listado de movimientos de la historia del denunciante que se aporta, no consta recogida la incidencia ocurrida el día 19 de julio de 2012 por lo que se puede afirmar que no les consta la pérdida de esa historia clínica. Los últimos movimientos anotados en la historia son de 21 de junio de 2012 y el siguiente y último movimiento recogido es de 3 de septiembre de 2012. No figura en dicho listado de movimientos la solicitud al Archivo de la historia del denunciante en la fecha de la operación programada o bien alguna incidencia con motivo de dicha solicitud.

Por otra parte el procedimiento de recuperación de documentación clínica que se ha aportado está reflejado en un diagrama de flujo de actividades entre las que se recoge una con el siguiente literal: *“¿Se encuentra la documentación clínica adecuadamente archivada?”*.

En el presente caso no cabe estimar lo alegado respecto a que la historia clínica no estaba perdida sino mal colocada y no localizable, porque la falta de esta documentación provocó que la operación programada tuviera que suspenderse porque la documentación clínica no estaba adecuadamente archivada de manera que no pudo utilizarse para el fin para el que estaba prevista la misma, la asistencia sanitaria del paciente.

Esta necesidad de especial diligencia en la custodia de la documentación por el responsable del tratamiento ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11 de diciembre de 2008 (recurso 36/08), fundamento cuarto: *“Como ha dicho esta Sala en múltiples sentencias...se impone, en consecuencia, una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros...la recurrente es, por disposición legal una deudora de seguridad en materia de datos”*.

El artículo 5.1.g) del Reglamento de la LOPD dispone que se entenderá por *“datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.”*

No hay duda de que la pérdida de la historia clínica del denunciante lleva a concluir que el encargado del tratamiento no ha adoptado las medidas que garantizan la seguridad de los datos de carácter personal relacionados con la salud.

El Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el sujeto infractor no se comporta con la diligencia exigible. Diligencia cuyo grado de exigencia se determinará en atención a las circunstancias concurrentes, tales como el especial valor del bien jurídico protegido, la profesionalidad exigible al infractor. En este sentido la Sentencia de 5 de junio de 1998 exige a los profesionales del sector *“... un deber de conocer especialmente las normas aplicables”*.

En definitiva, el SERVICIO MADRILEÑO DE SALUD-HOSPITAL CLINICO SAN CARLOS, no actuó con la diligencia debida al no adoptar las medidas de seguridad necesarias y suficientes para garantizar la seguridad de los datos de carácter personal, por ello, debe considerarse que ha vulnerado la LOPD.

Aplicando la anterior doctrina, la Audiencia Nacional, en varias sentencias, entre otras las de fechas 14 de febrero y 20 de septiembre de 2002 y 13 de abril de 2005, 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 Servicio Madrileño de Salud-Hospital Clínico San Carlos carece de las medidas de seguridad que la Ley exige al responsable del fichero, dado que hubo de suspenderse una intervención quirúrgica programada del denunciante de este procedimiento porque su historia clínica se había extraviado.

De acuerdo con los fundamentos anteriores, se deduce que por parte del Servicio Madrileño de Salud-Hospital Clínico San Carlos se ha producido una vulneración del principio de seguridad de los datos, que ha tenido como consecuencia que los datos personales de un paciente, su historia clínica, se perdieran, 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:

«1. 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”.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DECLARAR que el SERVICIO MADRILEÑO DE SALUD-HOSPITAL CLINICO SAN CARLOS ha infringido lo dispuesto en el artículo 9.1 de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

SEGUNDO: Debido a la naturaleza de la infracción no se insta por parte de la Agencia la adopción de una concreta medida correctora. No obstante se solicita se comuniquen las que de forma autónoma decida adoptar.

TERCERO: NOTIFICAR la presente resolución al SERVICIO MADRILEÑO DE SALUD-HOSPITAL CLINICO SAN CARLOS y a D. **A.A.A.**

CUARTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 46.4 de la LOPD.

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 Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se podrá interponer potestativamente recurso de reposición ante el Director 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 lo sucesivo 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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la 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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos