Expediente Nº: E/03034/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID - SUBDIRECCION GENERAL DE INSPECCION SANITARIA Y EVALUACION, EL HOSPITAL UNIVERSITARIO DE LA PRINCESA, y la SECCIÓN SINDICAL CC.OO en HOSPITAL LA PRINCESA, en virtud de denuncia presentada por Don ***B.B.B.*** (***Servicio De D.D.D.***), y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 4 de abril de 2017, tuvo entrada en esta Agencia un escrito remitido por Don ***B.B.B.*** en el que expone lo siguiente:

El denunciante es el Jefe del Servicio de ***D.D.D.*** del Hospital Universitario de la Princesa; dicho Servicio ha sido objeto de evaluación por el Área de Evaluación Sanitaria y Evaluación de la Consejería de Sanidad de la Comunidad de Madrid.

La evaluación se inició a raíz de una comunicación, de fecha 5 de septiembre de 2016, de la Sección Sindical de CCOO al Director-Gerente del Hospital, denunciando supuestas deficiencias en la organización y funcionamiento del Servicio.

En el informe de evaluación de octubre de 2016, cuya copia aporta, se pone de manifiesto que:

"*El equipo evaluador ha tenido acceso a escritos presentados por la Sección Sindical de CCOO cuyos anejos contienen documentos internos del hospital, así como información de acceso restringido, objetivándose una vulneración de datos confidenciales de pacientes y de trabajadores, así como de la custodia de documentos*"

Así mismo, en las conclusiones del informe, se incluye la siguiente:

"*En el transcurso de la presente evaluación el equipo evaluador ha tenido acceso a escritos presentados por la Sección Sindical de CCOO, cuyos anexos contienen datos confidenciales que están especialmente protegidos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Por lo tanto, la Dirección-Gerencia debería investigar e identificar la auditoria y procedencia de dichas filtraciones, así como adoptar las medidas necesarias para su corrección y prevención y, en su caso, poner estos hechos en conocimiento de la Agencia Española de Protección de Datos*".

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

- Con fecha 20 de julio de 2017 la Subdirección General de Inspección Sanitaria y Evaluación de la Consejería de Sanidad de la Comunidad de Madrid, remitió a esta Agencia la siguiente documentación:

1. Copia del escrito de la Sección Sindical de CCOO del Hospital de la Princesa,

dirigido al Director Gerente del Hospital, con fecha 5 de septiembre de 2016, que fue facilitado al equipo evaluador, y en el que constan datos de las guardias realizadas por los adjuntos Servicio de D.D.D. del Hospital así como detalle de las historias clínicas de dos pacientes del Servicio de D.D.D. del Hospital: consultas, intervenciones, diagnósticos, tratamientos etc… del año 2016. Con el escrito CCOO aporta copia de varias hojas de citaciones de pacientes (agendas), donde constan los diagnósticos.

- Con fechas 16 y 24 de agosto de 2017, la citada Subdirección General de Inspección Sanitaria y Evaluación ha informado a esta Agencia de que no tienen constancia de que por parte de la Dirección Gerencia del Hospital de la Princesa se hayan llevado a cabo actuaciones con objeto de "investigar e identificar la autoría y procedencia de los datos aportados por CCOO.

- Con fecha 11 de agosto de 2017, la Sección Sindical de CCOO del Hospital Universitario de la Princesa ha remitido a esta Agencia la siguiente información en relación con el origen de los datos aportados en su escrito de fecha 5 de septiembre de 2017:

1. Según manifiestan, desconocen el origen de los datos personales incorporados al escrito de queja que remitieron a la Dirección Gerencia del Hospital, ya que la documentación que se adjunta al mismo fue puesta a disposición de la Sección Sindical, de forma anónima y bajo la puerta del local sindical.
2. Dicha información se puso en conocimiento de la Gerencia al objeto de su verificación, para que en el marco de sus competencias llevara a cabo las actuaciones que considerara convenientes. A este respecto, aportan copia del primer párrafo del escrito que remitieron al Director Gerente del Hospital con fecha 5 de septiembre en el que consta "*Habiendo recibido en esta Sección Sindical de CCOO, numerosas y repetidas quejas sobre el Servicio De D.D.D. de este Hospital, ponemos en su conocimiento algunos de los datos de los que disponemos, solicitando a esta Gerencia que verifique con detenimiento y rigor la organización y funcionamiento de dicho Servicio, con el fin de corregir aspectos que entendemos graves….Para ello, tras algunos de los puntos que se van desarrollando, se aporta documentación adjunta numerada*".

- Con fecha 13 de septiembre de 2017, el Hospital Universitario de la Princesa, ha remitido a esta Agencia la siguiente información:

1. Con fecha 29 de marzo de 2017, el Director Gerente del Hospital dejo de prestar sus servicios como tal, siendo asumida la Dirección por el Director Médico hasta el nombramiento de un nuevo Director.
2. No obstante, con fecha 3 de mayo de 2017, el Director Médico requirió información sobre los accesos realizados a las dos historias clínicas que figuran en el escrito de CCOO. (Aportan copia del escrito de solicitud de la información).
3. Con fecha 5 de mayo de 2017, se remitió un escrito a la Dirección General de Inspección y Ordenación haciendo referencia en su último párrafo de lo siguiente: "*Esta Dirección Médica, al haber asumido la representación legal del Hospital por vacante de la Dirección Gerencia el pasado día 18 de abril, ha iniciado las investigaciones relativas a la procedencia de la filtración de datos protegido*s."
4. Han procedido al análisis de los datos correspondientes a los accesos realizados a las dos historias clínicas, cuya copia aportan en CD, y según manifiestan ha

resultado extremadamente complicado establecer una relación entre dichos accesos y la obtención de datos confidenciales por parte de la Sección Sindical de CCOO.

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 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."

III

El objeto de la denuncia era verificar los accesos efectuados a las historias clínicas de dos pacientes del servicio de otorrinolaringología del Hospital de la Princesa que fueron facilitados a la sección sindical de CCOO en dicho Centro Hospitalario y ésta Sección lo puso en conocimiento del Director-Gerente del Hospital.

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".*

IV

El artículo 9 de la LOPD dispone lo siguiente:

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

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

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

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

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 Hospital de la Princesa 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 las historias clínicas que facilitó CCOO a la Gerencia del Hospital, no ha podido verificarse que haya relación de CCOO con tales accesos. Los representantes de la Sección Sindical de CCOO en el Hospital de la Princesa indicaron que los datos se los facilitaron de forma anónima e introduciéndolos bajo la puerta del local sindical.

En consecuencia no se ha acreditado incumplimiento de las medidas de seguridad por parte de CCOO.

V

El denunciante indica que asimismo se ha producido una vulneración del deber de secreto de datos confidenciales.

El artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal establece que*: "El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."*

El deber de secreto profesional que incumbe a los responsables de los ficheros y a quienes intervienen en cualquier fase del tratamiento, recogido en el artículo 10 de la LOPD, comporta que el responsable de los datos almacenados o tratados no pueda revelar ni dar a conocer su contenido teniendo el *"deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, y, por lo que ahora interesa, comporta que los datos personales no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, en el caso

de que no prevalezcan otros derechos como la libertad de información, pues en eso consiste precisamente el secreto.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riego para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española. En efecto, este precepto contiene, en palabras del Tribunal Constitucional en la citada Sentencia 292/2000, un *"instituto de garantía de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos"*. Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino que impida que se produzcan situaciones atentatorias con la dignidad de la persona, es decir, el poder de resguardar su vida privada de una publicidad no querida.

En este supuesto no se ha vulnerado ningún secreto, ya que este deber de secreto se concreta en que los datos no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley.

El artículo 7 de la LOPD regula los datos especialmente protegidos, refiriéndose en el apartado 3 y 6 a los datos de salud:

"3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento."

El deber de secreto incumbía a la persona que facilitó los datos de salud a CCOO y no se ha podido averiguar su procedencia. CCOO facilito la información al Director-Gerente del Hospital, que puede acceder a las historias clínicas para la gestión de servicios sanitarios, según establece el artículo 7.6 de la LOPD arriba recogido. Para esa finalidad lo utilizo al haber pedido una evaluación de un servicio del Hospital cuyo funcionamiento había sido cuestionado.

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 a la CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID - SUBDIRECCION GENERAL DE INSPECCION SANITARIA Y EVALUACION, HOSPITAL UNIVERSITARIO DE LA PRINCESA, a la SECCIÓN SINDICAL CC.OO en HOSPITAL LA PRINCESA, y a Don ***B.B.B.*** (***Servicio De D.D.D.***),***).***

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