Expediente Nº: E/05845/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el HOSPITAL UNIVERSITARIO VIRGEN DE LA ARRIXACA - SERVICIO MURCIANO DE SALUD, y SCANNER MURCIA S.L., en virtud de denuncia presentada por la ASOCIACIÓN DE CONSUMIDORES Y USUARIOS EN ACCION-FACUA y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 5 de septiembre de 2014, tuvo entrada en esta Agencia un escrito remitido por la ASOCIACIÓN DE CONSUMIDORES Y USUARIOS EN ACCION-FACUA en el que declara:

<<PRIMERO.- FACUA ha tenido conocimiento de la cesión de los datos personales y médicos de los pacientes que se encuentran en lista de espera en el citado Hospital Clínico Universitario Virgen de la Arrixaca, de titularidad pública, a la Clínica Scanner Murcia, situada en la (C/.....1) Murcia, de titularidad privada.

SEGUNDO.- Que el objetivo de esta cesión es derivar pacientes a un centro médico privado y aligerar así la lista de espera del centro público de manera irregular, sin consentimiento de los pacientes y con un mensaje falso (que indica que la comunicación se produce en nombre del hospital público), con la intención de confundir a los afectados.

TERCERO.- Que el hospital privado que recibe los datos personales e informes médicos de manera fraudulenta los utiliza para obtener un beneficio económico a través del tratamiento de unos pacientes que no han solicitado sus servicios…

SEXTO.- Que, dado que no existe una ley de rango similar a la Ley Orgánica mencionada anteriormente y que los afectados no han expresado su consentimiento previo a la cesión de los datos, especialmente protegidos de acuerdo a la norma, el hospital arriba mencionado está incumpliendo la ley.

SÉPTIMO.- Que el hospital denunciado también incumple el artículo 9 de dicha ley, sobre la seguridad de los datos, que expresa que "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".

OCTAVO.- Que, asimismo, incumple el artículo 10 de la Ley Orgánica 15/1999, sobre el deber de secreto, que indica 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".

NOVENO.- Que, además, incumple el artículo 44.3.b de la Ley 15/1999

anteriormente mencionada, que recoge que es una infracción grave "tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo".>>

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. De la información y documentación aportada por el HOSPITAL UNIVERSITARIO VIRGEN DE LA ARRIXACA se desprende:

    a. Aporta copia del contrato suscrito entre el Servicio Murciano de Salud y SCANNER.

    Acompaña igualmente copia del PLIEGO DE CLÁUSULAS ADMINISTRATIVAS PARTICULARES QUE HAN DE REGIR EL CONCURSO ABIERTO PARA LA CONTRATACIÓN DE LA GESTIÓN DEL SERVICIO PÚBLICO DE REALIZACIÓN DE PROCEDIMIENTOS DE DIAGNÓSTICO POR IMAGEN "EFIGIE" que, según establece el contrato aportado, rige la contratación.

    En dichas clausulas aparece:

    <<14.8. El adjudicatario se obliga al estricto cumplimiento de la legislación sobre protección de datos de carácter personal, quedando expresa y radicalmente prohibida la revelación, divulgación, publicación, cesión o el simple acceso de terceros a información, informes o bases de datos que se generen o se conozcan por razón del servicio.>>

    Aparece igualmente, en el punto 18.- TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL, en donde se especifica:

    <<La empresa adjudicataria se compromete a tratar los datos personales a los que tenga acceso como consecuencia de la prestación del servicio, observando los principios exigibles por la legislación en materia de protección de datos, en particular los relativos a la calidad de los datos, seguridad de los mismos y deber de secreto, y conforme a las concretas instrucciones recibidas del SERVICIO MURCIANO DE SALUD, no utilizando los datos para ningún otro propósito distinto a la ejecución del contrato.

    Asimismo, la empresa se compromete a observar el secreto profesional respecto de los datos personales objeto de tratamiento, manteniendo absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, no comunicando a ningún tercero, ni siquiera para su conservación, los datos facilitados por el SERVICIO MURCIANO DE SALUD como responsable del fichero. Esta obligación subsistirá aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

    La empresa asegurará y se responsabilizara de que sus empleados y o

colaboradores, reciban los datos únicamente en la medida en que sea necesario su conocimiento para la prestación del suministro o servicio pactado

La empresa se compromete a crear y mantener un registro actualizado de usuarios de la empresa que manejan ficheros sometidos a este acuerdo de confidencialidad y a asegurarse del cumplimiento de las medidas de seguridad de nivel alto establecidas en el Real Decreto 994/ 1999.

La empresa, se compromete a observar las medidas de seguridad correspondientes al tratamiento de los datos personales del SERVICIO MURCIANO DE SALUD a los que tiene acceso, de acuerdo al nivel de protección establecido en el Reglamento de medidas de seguridad de ficheros automatizados que contengan datos de carácter personal contenido en el Real Decreto 994/ 1999 o en cualquier otra norma que lo sustituya o modifique.

En el supuesto de que la empresa, destine los datos a finalidad distinta de la estipulada, los comunique o utilice incumpliendo las instrucciones fijadas en el presente contrato, será considerada también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido.

El Servicio Murciano de Salud se reserva el derecho de comprobar e inspeccionar en cualquier momento, durante la vigencia del contrato, el cumplimiento de lo aquí expuesto siempre que medie un preaviso de 15 días. La Empresa se compromete a facilitar la inspección, poniendo a disposición de SERVICIO MURCIANO DE SALUD sus instalaciones y/o todos aquellos datos, información, documentación que sea necesaria para la realización de la misma. Si fruto de dicha comprobación fuese necesario implantar medidas de seguridad adicionales a las previamente acordadas, la Empresa estará obligada a la implantación de dichas medidas a su cargo.

La empresa se compromete a devolver al SERVICIO MURCIANO DE SALUD los datos objeto de tratamiento, soportes o documentos en que estos consten, así como a destruir aquellos según las instrucciones del responsable del tratamiento, una vez cumplida la prestación contractual.>>

b. Las peticiones de scanners son realizadas por facultativos del Área de salud y remitidas al servicio de radiología del centro, donde son valoradas por radiólogos que determinan tanto la idoneidad de realización de las mismas, como si éstas se van a realizar en el propio centro o si van a derivadas a centros concertados para su realización.

Las que han de ser derivadas son registradas por personal administrativo del servicio de radiología en el programa informático SELENE (Historia clínica digital).

Los pacientes registrados como derivables en la aplicación informática SELENE son volcados a su vez diariamente a la aplicación informática SIGILE.

Desde los servicios centrales del Servicio Murciano de Salud autorizan y distribuyen los pacientes a los centros concertados.

Los centros concertados tienen acceso a SIGILE y a través de él comunican la realización de la prueba que automáticamente es dada de baja en lista de espera, y cuelgan en el registro una copia de la petición, un justificante de realización firmado por el paciente y un informe con los resultados de la misma.

Los accesos tanto a SELENE como a SIGILE están restringidos, es necesario tener una clave de usuario y una contraseña.

La información contenida en estas aplicaciones no puede ser visionada por todos los usuarios; cada usuario sólo puede consultar aquella parte del programa que tenga autorizada en su perfil.

Los centros concertados son considerados encargados del tratamiento de los datos.

c. No se solicita consentimiento informado para la derivación de pacientes. Indica el HOSPITAL UNIVERSITARIO VIRGEN DE LA ARRIXACA que, según se recoge reiteradamente por esta Agencia en distintos informes (5 de agosto de 2009; 600/2009), *"En consecuencia, aun no formando parte integrante del sistema Nacional de Salud, los centros concertados desarrollan acciones asistenciales directamente vinculadas con el sistema, pudiendo incluso entenderse que las mismas constituyen, en cuanto sea objeto de concierto, servicios propios del mencionado Sistema."*

Por consiguiente, en opinión de la entidad informante, la incorporación a la historia clínica electrónica de los datos originados como consecuencia de una asistencia prestada al paciente en el marco del concierto que mantiene con el Servicio de Salud de la comunidad autónoma, constituiría una cesión de datos que resulta conforme con la Ley Orgánica 15/1999 por encontrarse amparada en el artículo 56 de la Ley 16/2002, de Cohesión y calidad del Sistema Nacional de Salud.

d. Adjunta copia del Documento de Seguridad.

e. Respecto de la obtención del consentimiento para la derivación de pacientes, aporta el HOSPITAL UNIVERSITARIO VIRGEN DE LA ARRIXACA una Comunicación Interior de la Consejería de Sanidad, con registro de entrada de fecha 24/04/2015, en el que se dejan en suspenso las normas anteriormente vigente que en el caso de derivación de procedimientos diagnósticos o diagnóstico-terapéuticos establecía

<<Se informará al paciente sobre la posibilidad de que puede ser derivada a centros concertados con el fin de disminuir los tiempos de espera. En este caso, para garantizar la continuidad asistencial, previa aceptación firmada del paciente, se cederán al centro al que se derive los datos de carácter personal que sean imprescindibles".>>

2. De la información y documentación aportada por el Servicio Murciano de Salud se desprende:

a. La aplicación SELENE es el sistema de información principal de los hospitales del Servicio Murciano de Salud.

Se trata de una aplicación web, tuyos servidores de base de datos y de aplicaciones están ubicados en los CPDs de cada uno de los hospitales del SMS. Estos servidores no son accesibles desde el exterior del CPD. El servidor de aplicaciones sólo puede acceder través de los protocolos y puertos establecidos para ello. El servidor de base de datos sólo es accesible por los servidores de aplicaciones y los administradores de bases de datos.

Ambos servidores se encuentran protegidos por los cortafuegos perimetrales del Servicio Murciano de Salud y han sido configurados siguiendo las recomendaciones de CIS (Center of Internet Security).

La aplicación Selene dispone de gestión de perfiles para que cada tipo de usuario acceda exclusivamente a los datos que le corresponden por su puesto de trabajo. Tiene incorporado un registro de accesos completo, conforme a lo establecido en la normativa sobre protección de datos personales.

b. La aplicación SIGILE es el sistema que se encarga de gestionar las derivaciones de ciertos procedimientos y pruebas a centros privados. Estos centros son aquellos que previamente han firmado un concierto con el Servicio Murciano de Salud para realizar el tipo de procedimientos que les son derivados.

c. Respecto del circuito de derivación de pacientes:

- Cuando en un hospital se determina que un paciente puede ser derivado, esta circunstancia se indica en el programa SELENE y, si así se determina en el hospital y el paciente se incluye en la lista de espera correspondiente, mediante mensajería HL7 (estándar de intercambio electrónico de información clínica) se envían los datos a la aplicación SIGILE, ubicada en el CPD de los servicios centrales del Servicio Murciano de Salud.

- Estas peticiones llegan a la base de datos de SIGILE y desde la aplicación (a la que se accede con usuario y contraseña) se autorizan en SSCC y se firman (por el Subdirector General de Prestaciones) con certificado electrónico.

- Una vez firmadas, el centro concertado recibe las peticiones de pruebas en la web habilitada para ello (mediante protocolo cifrado https) a la que se accede mediante certificado digital reconocido.

- Cuando el centro concertado realiza la actividad o finaliza la derivación por un motivo distinto a la realización de la prueba, introduce la información en la misma web segura explicada anteriormente y de forma interna información se comunica a SELENE, para realizar las acciones convenientes.

d. La aplicación SIGILE dispone de gestión de perfiles para que cada tipo de usuario acceda exclusivamente a los datos que le corresponden por su puesto de trabajo. Tiene incorporado un registro de accesos completo,

conforme a lo establecido en la normativa sobre protección de datos personales.

e. El Servicio Murciano de Salud da una descripción de la arquitectura de seguridad del sistema, que incluye protección perimetral mediante cortafuegos, autenticación mediante certificados digitales reconocidos y conexiones cifradas mediante VPN.

f. Respecto de las medidas de seguridad establecidas para el tráfico de datos con SCANNER:

- El HOSPITAL UNIVERSITARIO VIRGEN DE LA ARRIXACA no mantiene un tráfico de datos directo con Scanner Murcia.
- Scanner Murcia tiene acceso a los datos a través de una web segura, a la que se conecta el personal autorizado de SCANNER usando un certificado reconocido, y accede exclusivamente a los datos de los procesos que han sido asignados explícitamente a SCANNER previamente. El personal de SCANNER que use la web debe haber sido identificado y registrado previamente.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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 denuncia de FACUA se concreta en la cesión de datos de pacientes del Hospital Virgen de la Arrixaca, de titularidad pública, a un Centro privado denominado Scanner Murcia, S.L., ubicado en Murcia, para aligerar la lista de espera del centro público, sin el consentimiento de los afectados.

Hay que señalar que FACUA no acompaña ninguna prueba de las acusaciones formuladas.

En esta Resolución se analizarán distintas cuestiones, bajo la perspectiva de la normativa de protección de datos.

En primer lugar, referente al consentimiento por parte de los pacientes, el artículo 6.1 de la LOPD dispone que *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa"*.

El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre (F. J. 7 primer párrafo) *"consiste en un poder de disposición y de control sobre los datos personales que faculta*

a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...).”

Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

El artículo 7 de la LOPD dispone que el tratamiento de los datos especialmente protegidos, como son los relativos a la salud, solo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

Este artículo 7 de la LOPD establece un régimen específicamente protector diseñado por el Legislador para aquellos datos personales que proporcionan una información de las esferas más íntimas del individuo, a los que se califica en el citado artículo como “Datos especialmente protegidos”. Para las diversas categorías de éstos, el precepto citado establece específicas medidas para su protección. En el supuesto de los datos de salud, el Legislador español, siguiendo al Consejo de Europa (artículo 6 del Convenio 108/81, de 28 de enero, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal) y al Derecho Comunitario (artículo 8 Directiva 95/46/CEE, del Parlamento y del Consejo, de 24 de octubre 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), los considera como especialmente protegidos y prevé que sólo puedan ser recabados, tratados y cedidos, cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente. Ello quiere decir que, solamente en estos supuestos específicos, dichos datos podrán ser tratados.

El artículo 7.3 señala, para el tratamiento de los datos de salud, la exigencia de consentimiento expreso del afectado, pero no la relativa a que deba constar por escrito. Cabe, en consecuencia, admitir la posibilidad de que la manifestación del consentimiento expreso no conste por escrito. Sin embargo, esta posibilidad debe ponerse en relación con los elementos que integran la definición de consentimiento recogida en el artículo 3. h) de la LOPD, que dispone que lo será “*Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*”.

Por último, indicar que el artículo 8 de la LOPD, relativo exclusivamente a los datos de salud, establece lo siguiente: *“Sin perjuicio de lo que dispone el artículo 11 respecto a la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.”*

III

La LOPD además de sentar el anterior principio de consentimiento, regula en su artículo 4 el principio de calidad de datos. El apartado 2 del citado artículo 4, dispone: *"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."* Las *"finalidades"* a las que alude este apartado 2 han de ligarse o conectarse siempre con el principio de pertinencia o limitación en la recogida de datos regulado en el artículo 4.1 de la misma Ley. Conforme a dicho precepto los datos sólo podrán tratarse 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."* En consecuencia, si el tratamiento del dato ha de ser "pertinente" al fin perseguido y la finalidad ha de estar "determinada", difícilmente se puede encontrar un uso del dato para una finalidad *"distinta"* sin incurrir en la prohibición del artículo 4.2 aunque emplee el término *"incompatible".*

La citada Sentencia del Tribunal Constitucional 292/2000, se ha pronunciado sobre la vinculación entre el consentimiento y la finalidad para el tratamiento de los datos personales, en los siguientes términos: *"el derecho a consentir la recogida y el tratamiento de los datos personales (Art. 6 LOPD) no implica en modo alguno consentir la cesión de tales datos a terceros, pues constituye una facultad específica que también forma parte del contenido del derecho fundamental a la protección de datos. Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aún cuando puedan ser compatibles con estos (Art. 4.2 LOPD), supone una nueva posesión y uso que requiere el consentimiento del interesado. Una facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional y, por tanto, esté justificada, sea proporcionada y, además, se establezca por ley, pues el derecho fundamental a la protección de datos personales no admite otros límites. De otro lado, es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales. Para lo que no basta que conozca que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta. Pues en otro caso sería fácil al responsable del fichero soslayar el consentimiento del interesado mediante la genérica información de que sus datos pueden ser cedidos. De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (Art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia."*

De lo expuesto cabe concluir que la vigente LOPD ha acentuado las garantías precisas para el tratamiento de los datos personales en lo relativo a los requisitos del consentimiento, de la información previa a éste y de las finalidades para las que los datos pueden ser recabados y tratados.

En definitiva, los datos no pueden ser tratados para fines distintos a los que motivaron su recogida, pues esto supondría un nuevo uso que requiere el consentimiento del interesado.

IV

En fecha 28 de febrero de 2010, el Gabinete Jurídico de la Agencia Española de Protección de Datos, emitió un informe, solicitado por un centro hospitalario público, sobre la necesidad del consentimiento de los pacientes en el caso de ser atendidos en un centro privado, con el que mantenía un concierto para asistencia a los beneficiarios de la Seguridad Social. El informe nº 600/2009, indica lo siguiente:

"Se plantea en primer lugar, si el consultante, centro médico privado que mantiene un concierto con la Administración de la Comunidad autónoma para asistencia a beneficiarios de la Seguridad Social, debe solicitar en cumplimiento de lo dispuesto en el apartado 6 de la Ley Orgánica 15/1999 el consentimiento inequívoco de sus pacientes para el tratamiento de sus datos tanto en la actividad pública como privada.

El tratamiento y comunicación de datos de carácter personal, cuyo régimen aparece recogido con carácter general en los artículos 6 y 11 de la Ley Orgánica 15/1999, se encuentra, por vía de excepción, sometido a particulares restricciones en lo que a los datos de salud respecta, por el artículo 7 de la citada Ley Orgánica, cuyo apartado 3 establece como regla general que "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". Esta regla únicamente es matizada por la Ley Orgánica en sus artículos 7.6 y 8.

La especial protección conferida a los datos relacionados con la salud de las personas no es arbitraria, sino que resulta de lo dispuesto en las normas Internacionales y Comunitarias reguladoras del tratamiento automatizado de datos de carácter personal. En este contexto, tanto el artículo 8 de la Directiva 95/46/CE del Parlamento y del Consejo, así como el artículo 6 del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, ratificado por España en fecha 27 de enero de 1984, hacen referencia a los datos de salud como sujetos a un régimen especial de protección.

En este sentido, el artículo 8 de la Directiva 95/46/CE limita el tratamiento de datos a supuestos y finalidades concretos en los que será preciso el consentimiento, que además deberá ser expreso, del afectado o la necesidad del tratamiento con fines de asistencia sanitaria o atención de un interés vital del afectado. Esta cuestión ha sido especialmente analizada por el Grupo de Autoridades de Protección de Datos creado por el artículo 29 de la citada Directiva en su Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (Documento EP131), en el que se indica expresamente que "todos los datos contenidos en documentos médicos, en historiales médicos electrónicos y en sistemas de HME son "datos personales sensibles". Por tanto, no sólo están sujetos a todas las normas generales sobre protección de datos personales de la Directiva, sino también a las normas sobre protección de datos especiales que rigen el tratamiento de la información sensible, contenidas en el artículo 8 de la Directiva".

En el Derecho español, establecida ya por el artículo 7.3 la regla general del consentimiento expreso para el tratamiento de los datos de salud, el artículo 7.6 establece en su párrafo primero que "podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 (datos de salud) 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".

Igualmente, conforme al párrafo segundo del propio artículo 7.6, "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".

Por otra parte, el artículo 8 de la Ley Orgánica 15/1999 establece respecto a los datos de salud que "Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad".

Por consiguiente, debe entenderse que el tratamiento de datos personales relativo a la salud será posible cuando exista consentimiento del interesado o en los supuestos a que hacen referencia los citados artículos 7.6 y 8 de la Ley Orgánica 15/1999.

Ahora bien, debe tenerse en cuenta, como señala el citado el Grupo de Trabajo del artículo 29 en el aludido documento, en relación con el artículo 8 de la directiva, que tratándose de una excepción a la prohibición general de tratar datos sensibles, esta excepción deberá interpretarse de forma restrictiva". De este modo, señala que dichas excepciones "cubre solamente el tratamiento de datos personales para el propósito específico de proporcionar servicios relativos a la salud de carácter preventivo, de diagnóstico, terapéutico o de convalecencia, y a efectos de la gestión de estos servicios sanitarios, como por ejemplo facturación, contabilidad o estadísticas. No se cubre el tratamiento posterior que no sea necesario para la prestación directa de tales servicios, como la investigación médica, el reembolso de gastos por un seguro de enfermedad, o la interposición de demandas pecuniarias. También quedan fuera del alcance de la aplicación del apartado 3 del artículo 8 otros tratamientos en áreas como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad (…)"

II

Plantea el centro médico consultante, en segundo lugar, si necesita autorización del paciente para integrar en el sistema informático del servicio de salud de su comunidad autónoma, los datos sanitarios del paciente atendido en éste, que han sido originados como consecuencia de una asistencia privada prestada en su centro, al estar incorporados a una única historia clínica.

El tratamiento de datos de las historias clínicas se encuentra regulado en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, cuyo artículo 14.1 consagra el principio de máxima integración de la misma, al disponer que "La historia clínica comprende el conjunto de los documentos relativos a los procesos

asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro".

En cuanto a su finalidad, el artículo 15.2 dispone que "La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud".

Por su parte, los apartados 4 y 5 del artículo 17 vienen a reflejar la delimitación del responsable del fichero de historias clínicas, correspondiendo esta condición al centro sanitario en el que se produzca la asistencia sanitaria o al médico que ejerza la profesión de manera individual. Así, se dispone que:

"4. La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario.

"5. Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen."

Por consiguiente, el centro sanitario consultante tiene, en relación con los pacientes que acuden al mismo, la condición de responsable del tratamiento de los datos que sean incorporados a sus historias clínicas, por lo que la comunicación de los datos de la historia clínica al Servicio de Salud de su comunidad autónoma constituirá una cesión de datos de carácter personal definida en el artículo 3 i) de la Ley Orgánica 15/1999 como "Toda revelación de datos realizada a una persona distinta del interesado", que solo cabe, por tratarse de datos de salud, como especifica el artículo 7.3 de la misma ley cuando "así lo disponga una Ley o el afectado consienta expresamente".

Debe así tenerse en cuenta que el párrafo primero del artículo 56 de la Ley 16/2003, de 28 mayo, de cohesión y calidad del Sistema Nacional de Salud, dispone que "Con el fin de que los ciudadanos reciban la mejor atención sanitaria posible en cualquier centro o servicio del Sistema Nacional de Salud, el Ministerio de Sanidad y Consumo coordinará los mecanismos de intercambio electrónico de información clínica y de salud individual, previamente acordados con las comunidades autónomas, para permitir tanto al interesado como a los profesionales que participan en la asistencia sanitaria el acceso a la historia clínica en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información, cualquiera que fuese la Administración que la proporcione."

En este mismo sentido, el 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, recoge expresamente, sobre la base de la citada ley especial, la cesión de datos de salud en este supuesto en su artículo 10.5 disponiendo que "Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre"

En particular, no será necesario el consentimiento del interesado para la

comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

En el presente supuesto nos hallamos ante un centro privado concertado que no forma parte integrante del Sistema Nacional de Salud, aunque se encuentre vinculado con el mismo, así el artículo 44 de la Ley 14/1986, de 25 abril, General de Sanidad señala que "todas las estructuras y servicios públicos al servicio de la salud integrarán el Sistema Nacional de Salud", añadiendo que "el Sistema Nacional de Salud es el conjunto de los Servicios de Salud de la Administración del Estado y de los Servicios de Salud de las Comunidades Autónomas en los términos establecidos en la presente Ley".

No obstante, el artículo 45 de la misma Ley 14/1986 establece que "el Sistema Nacional de Salud integra todas las funciones y prestaciones sanitarias que, de acuerdo con lo previsto en la presente Ley, son responsabilidad de los poderes públicos para el debido cumplimiento del derecho a la protección de la salud" y el artículo 90 habilita la celebración de conciertos con entidades sanitarias para la prestación de servicios.

Sobre estas bases, esta Agencia ha concluido en informe de 5 de agosto de 2009 que "En consecuencia, aun no formando parte integrante del sistema Nacional de Salud, los centros concertados desarrollan acciones asistenciales directamente vinculadas con el sistema, pudiendo incluso entenderse que las mismas constituyen, en cuanto sea objeto de concierto, servicios propios del mencionado Sistema."

Por consiguiente, la incorporación a la historia clínica electrónica de los datos originados como consecuencia de una asistencia prestada al paciente en el marco del concierto que mantiene con el Servicio de Salud de la comunidad autónoma, constituiría una cesión de datos que resulta conforme con la Ley Orgánica 15/1999 por encontrarse amparada en el artículo 56 de la Ley 16/2002.

En este sentido se pronuncia el Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica, de la Comunidad de Galicia que dispone en su artículo 3 "La historia clínica electrónica incorporará la información correspondiente al contenido previsto en el artículo 15 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y deberes en materia de información y documentación clínica, y en el artículo 16 de la Ley gallega 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes.

Asimismo, incorporará la información clínica generada en aquellas actuaciones sanitarias derivadas de programas de salud pública, bajo el principio de integrar toda aquella información que pueda ser relevante para una mejor asistencia futura."

Igualmente, el mismo decreto establece en su artículo 5 que "En particular, no será necesario el consentimiento de la persona interesada para la comunicación de datos personales sobre la salud a través de medios electrónicos, entre organismos, centros, servicios y establecimientos de la Consellería de Sanidad, el Servicio Gallego de Salud y el sistema nacional de salud, cuando se realice para llevar a cabo la atención sanitaria de las personas, tanto se realice con medios propios o concertados."

En consecuencia la normativa estudiada determina la incorporación al sistema de intercambio electrónico de información clínica de los datos relativos a las asistencias prestadas a los pacientes en el marco de los servicios concertados, pero no extiende

dicha obligación a los datos relativos a las asistencias privadas prestadas a sus pacientes por los centros concertados, sin perjuicio del cumplimiento de los deberes que respecto a la unidad de la historia clínica impone al centro médico consultante la Ley 41/2002."

V

Durante las actuaciones previas de investigación se ha constatado que el Sistema Sanitario Público de la Comunidad Autónoma de Murcia publicó, el 4 de junio de 2007, un Pliego de cláusulas administrativas particulares que han de regir el concurso abierto para la contratación de la gestión del servicio público de realización de procedimientos de diagnóstico por imagen "EFIGIE" a beneficiarios del Servicio Murciano de Salud.

En dicho pliego aparece la Cláusula 18: Tratamiento de Datos de Carácter Personal Protección de Datos, en la que se establecen las obligaciones del adjudicatario respecto al tratamiento de datos personales.

El artículo 12 de la LOPD *"acceso a datos por cuenta de terceros",* establece lo siguiente:

"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".

El citado artículo 12.1 de la LOPD permite que el responsable del fichero habilite el acceso a datos de carácter personal por parte de la entidad que va a prestarle un servicio –encargado del tratamiento- sin que, por mandato expreso de la ley, pueda considerarse dicho acceso como una cesión de datos. La LOPD exige que el acceso a datos por cuenta de terceros figure reflejado en un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido, y prevé unos contenidos mínimos, tales como seguir las instrucciones del responsable del tratamiento, no utilizar los datos para un fin distinto, no comunicarlos a otras personas, estipular las medidas de

seguridad del artículo 9 y, cumplida la prestación, destruir los datos o proceder a su devolución al responsable del tratamiento.

En el presente caso, ha quedado constatado que existe formalizado contrato entre el Servicio Murciano de Salud y Scanner Murcia, S.L. En el Pliego de Cláusulas Administrativas se recogen las exigencias establecidas por la normativa de protección de datos para el tipo de datos que van a ser objeto de tratamiento: medidas de seguridad, integridad de la información, confidencialidad…

El día 30 de abril de 2008, se firmó el Contrato administrativo de gestión del servicio público e realización de procedimientos de diagnóstico por imagen "EFIGIE" a beneficiarios del Servicio Murciano de Salud.

En el supuesto del Sistema Sanitario Público existe habilitación legal para concertar la realización de determinadas intervenciones o pruebas diagnósticas con centros sanitarios privados. La finalidad del tratamiento de los datos de los pacientes es efectuar un diagnóstico médico, por lo que no es necesario que presten el consentimiento para dicho tratamiento de datos, en este caso concreto por parte de la Scanner Murcia, S.L.

El Hospital Virgen de la Arrixaca se ha comprometido a informar a los pacientes de la posibilidad de derivarles a un centro privado y si aceptan se cederán los datos imprescindibles.

En consecuencia, no se ha producido vulneración de la normativa de protección de datos en relación con el tratamiento de los datos de los pacientes del Hospital San Pedro por parte del Centro privado.

VI

En relación al posible incumplimiento de las medidas de seguridad y del l deber de secreto, por parte del Hospital Virgen de la Arrixaca al facilitar el acceso a los datos de los pacientes del hospital público a un centro privado, hay que señalar lo siguiente:

En relación al cumplimiento de las medidas de seguridad por parte del Hospital San Pedro, el artículo 9 de la LOPD establece:

"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 citado 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 aquélla, con la finalidad de evitar, entre otros

aspectos, el acceso no autorizado por parte de ningún tercero.

Sintetizando las previsiones legales citadas puede afirmarse que:

- 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.

- 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.

- La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se establecen en normas reglamentarias, de modo que se eviten accesos no autorizados.

- 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 Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, establece de manera pormenorizada las medidas de seguridad que han de tener incorporadas en sus ficheros los responsables del tratamiento de datos personales. Los ficheros que contengan datos de salud han de tener implantadas las medidas de seguridad de nivel alto.

El artículo 104 de dicho Reglamento aplicable a los ficheros con nivel de seguridad alto, como es el caso del que contiene historias clínicas, indica lo siguiente:

"Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros."

El Hospital Virgen de la Arrixaca tiene incorporadas tales medidas de seguridad, ya que los ficheros se envían por correo electrónico encriptado.

En resumen, se trata de un acceso a datos de pacientes en el marco de la prestación de servicios, que no incumple las medidas de seguridad ni supone una vulneración del deber de guardar secreto por parte del Hospital público denunciado.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

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

2. **NOTIFICAR** la presente Resolución a HOSPITAL UNIVERSITARIO VIRGEN DE LA ARRIXACA - SERVICIO MURCIANO DE SALUD, a SCANNER MURCIA S.L., y a la ASOCIACIÓN DE CONSUMIDORES Y USUARIOS EN ACCION-FACUA**.**

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, los interesados podrán 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 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.

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