

Dictamen en relación con la consulta de un centro sanitario sobre el acuerdo de encargado del tratamiento con las empresas que monitorizan ensayos clínicos

Se presenta ante la Autoridad Catalana de Protección de Datos una consulta de un centro sanitario (en adelante, el Hospital) sobre el acceso por parte del monitor externo de ensayos clínicos a datos personales de los sujetos que participan en los ensayos.

En concreto, la consulta pregunta si el acceso a datos personales por parte del monitor externo de ensayos clínicos estaría legitimado indirectamente en virtud de la hoja de información y el consentimiento informado que firman las personas que participan en el ensayo. En este caso, la consulta pregunta si el Hospital podría dejar de exigir la firma de un contrato de encargado de tratamiento entre el Hospital y el monitor externo y si, en este caso, habría que establecer algún tipo de salvaguardia adicional.

Analizada la petición, que no se acompaña de otra documentación, vistos la normativa vigente aplicable y el informe de la Asesoría Jurídica, se dictamina lo siguiente.

I

(...)

II

La consulta explica que el Hospital lleva a cabo en sus instalaciones ensayos clínicos con medicamentos, regulados por el Real decreto 1090/2015, de 4 de diciembre, a petición de las entidades o empresas promotoras (en adelante, el Promotor).

Según la consulta, el Promotor designa al monitor del ensayo, quien, para poder realizar sus funciones, tiene que acceder a datos personales identificados de los sujetos del ensayo que están bajo el control del Hospital. Según la consulta, el Promotor puede designar a un monitor interno (del personal del Promotor del ensayo) o externo (en adelante, Monitor externo).

En relación con la designación de un Monitor externo, según la consulta, *“el Hospital exige la firma de un contrato de tratamiento de datos entre el Hospital y el Monitor externo en los términos del artículo 28 del RGPD”*.

En este contexto, el Hospital formula las **siguientes preguntas**:

“1.- ¿Podría el Hospital entender que el acceso del Monitor externo a los datos personales identificados de los sujetos del ensayo bajo control del Hospital está legitimado indirectamente en virtud de la HIP/CI que legitima el acceso directo del Promotor a estos datos?”

2.- Si la respuesta a la pregunta anterior es afirmativa, ¿podría el Hospital dejar de exigir la firma de un contrato de tratamiento entre el Hospital y el Monitor externo?”

3.- Si la respuesta a la pregunta anterior es afirmativa, ¿debería establecer el Hospital algún tipo de salvaguardia adicional antes de permitir el acceso del Monitor externo a datos personales bajo el control del Hospital?”

III

Según el Reglamento (UE) 2016/679 del Parlamento y del Consejo Europeo, de 27 de abril de 2016, general de protección de datos (en adelante, RGPD), son datos personales: “*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona»* (art. 4.1 RGPD).

El tratamiento de datos (art. 4.2 RGPD) de las personas físicas que participan en ensayos clínicos que lleva a cabo el Hospital a petición de los promotores, se encuentra sometido a los principios y garantizas de la normativa de protección de datos personales (RGPD, así como la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD)).

La participación en ensayos clínicos implica el tratamiento de datos de salud (art. 4.15 RGPD) de los pacientes (“*personas interesadas*”, ex art. 4.1 RGPD) y, por lo tanto, hay que tener en cuenta que la información relativa a la salud de las personas físicas es objeto de una especial protección.

Así, el artículo 9 del RGPD regula la prohibición general del tratamiento de datos personales de varias categorías, entre otros, de los datos relativos a la salud (apartado 1). El apartado 2 del mismo artículo 9 dispone que esta prohibición general no será de aplicación cuando concurra una de las siguientes circunstancias:

*“a) el interesado dio su **consentimiento** explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;*

*h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, **prestación de asistencia o tratamiento de tipo sanitario o social, (...);***

(...)

*j) el tratamiento es necesario con fines de archivo en interés público, **fines de investigación científica** o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado”.*

Según dispone el artículo 89.1 del RGPD:

*“1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para **garantizar el respeto del principio de minimización** de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo”.*

La historia clínica (en adelante, HC) se encuentra regulada y protegida por una normativa específica (Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, la documentación clínica y 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. El artículo 16.3 de la Ley 41/2002 (modificado por la disposición final novena de la LOPDGDD) prevé el acceso a la HC, entre otras, para finalidades de investigación, en los siguientes términos:

*“3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, **de investigación** o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que, **como regla general**, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.*

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley orgánica de protección de datos personales y garantía de los derechos digitales.

(...). El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

(...).”

Según el apartado 2 de dicha disposición adicional 17.a de la LOPDGDD:

*“2. El tratamiento de datos en la investigación en salud se regirá por los siguientes **criterios**:*

a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para

finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

(...).

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

(...)"

Finalmente, la disposición final quinta de la LOPDGDD ha añadido un nuevo artículo 105 bis a la Ley 14/1986, de 25 de abril, general de sanidad, según el cual: "El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley orgánica de protección de datos personales y garantía de los derechos digitales".

Según el artículo 58.1 de la Ley de garantías y uso racional de los medicamentos y productos sanitarios de 2015 (Real decreto legislativo 1/2015, de 24 de julio), se entiende por ensayo clínico: "toda investigación efectuada en seres humanos con el fin de determinar o confirmar los efectos clínicos, farmacológicos y/o demás efectos farmacodinámicos, y/o de detectar las reacciones adversas, y/o de estudiar la absorción, distribución, metabolismo y eliminación de uno o varios medicamentos en investigación con el fin de determinar su seguridad y/o su eficacia. (...)".

En relación con los ensayos clínicos, es preciso referirse al artículo 3 del Real decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los comités de ética de la investigación con medicamentos y el Registro español de estudios clínicos, según el cual:

"1. Solo se podrá iniciar un ensayo clínico objeto de esta regulación cuando el CEIM y la Agencia Española de Medicamentos y Productos Sanitarios hayan considerado que se cumplen la totalidad de las siguientes **condiciones**:

(...)

c) **Se obtiene y documenta el consentimiento informado** de cada uno de los sujetos del ensayo, libremente expresado, antes de su inclusión en el ensayo en los términos previstos en los artículos 4 a 8.

d) **Se respetan los derechos del sujeto a su integridad física y mental, y a su intimidad, y se protegen los datos de carácter personal que le conciernen, de acuerdo con la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y su normativa de desarrollo, así como con la normativa europea vigente en la materia.**

(...)"

En definitiva, el marco normativo estudiado permite habilitar el tratamiento de datos de salud para finalidades de investigación médica, en concreto, para la realización de ensayos clínicos, sobre la base del consentimiento informado del paciente que participa en ellos, en los términos apuntados.

IV

Es responsable del tratamiento de datos: *“la persona física o jurídica, autoridad pública, servicio u otro organismo que, **solo o junto con otros, determine los fines y medios del tratamiento**; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”* (art. 4.7 RGPD).

Es encargado del tratamiento: *“la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento”* (art. 4.8 RGPD).

Desde la perspectiva de la protección de datos, partimos de la base de que el tratamiento de datos personales debe tener un *responsable*, quien asume en consecuencia una serie de responsabilidades y obligaciones respecto del tratamiento que se realiza.

Por otra parte, el **Promotor** es: *“el individuo, empresa, institución u organización responsable de iniciar, gestionar y organizar la financiación de un ensayo clínico”* (artículo 2.1.s) RD 1090/2015).

El **Monitor** es el *“profesional capacitado con la formación y competencia clínica y/o científica necesaria, escogido por el promotor, que se encarga del **seguimiento directo del ensayo**. Sirve de vínculo entre el promotor y el investigador principal, cuando estos no concurren en la misma persona. En ningún caso el monitor debe formar parte del equipo investigador”* (art. 2.2.i) RD 1090/2015).

El nombramiento del Monitor es función y responsabilidad del Promotor (art. 39.3.h) RD 1090/2015). Según el artículo 40.1 del mismo RD 1090/2015, las funciones del monitor son, entre otras: *“a) Trabajar de acuerdo con los procedimientos normalizados de trabajo del promotor, visitar al investigador antes, durante y después del ensayo, en función del tipo de estudio, para comprobar el cumplimiento del protocolo, garantizar que los datos son registrados de forma correcta y completa, así como asegurarse de que se ha obtenido el consentimiento informado de todos los sujetos antes de su inclusión en el ensayo”*.

Según el artículo 39 del RD 1090/2015:

“4. El promotor de un ensayo clínico podrá delegar la totalidad o una parte de sus tareas en un particular, organización de investigación por contrato (CRO), institución u organismo, que deberá disponer de un sistema de garantía y control de calidad.

5. Las obligaciones del promotor establecidas en las normas de buena práctica clínica que se hayan delegado serán de aplicación al particular, CRO, empresa, institución u organismo contratado. No obstante, en estos casos, el promotor seguirá siendo el responsable de garantizar que la realización del ensayo clínico

y los datos finales generados en dicho estudio se ajustan a lo dispuesto en este real decreto. Cualquier delegación de funciones del promotor en relación con un ensayo clínico debe quedar específicamente documentada en un contrato entre ambas partes”.

Así, el Promotor puede contratar una “organización de investigación por contrato” (CRO), para realizar las funciones de monitorización previstas en la normativa estudiada (“Monitor externo”), a que se refiere la consulta.

Hacemos notar que, según el apartado 49 del “Documento de instrucciones de la Agencia Española de Medicamentos y Productos Sanitarios para la realización de ensayos clínicos en España” (disponible en la web: www.aemps.es):

“Los datos relacionados con la salud son considerados por la LOPD datos especialmente protegidos, que merecen un régimen de protección más estricto, (...). Por este motivo, el cuaderno de recogida de datos únicamente debe incluir un código que no permita la identificación del sujeto. Además, no podrá recoger datos identificativos de los sujetos participantes en el estudio: (...)”.

Como menciona la consulta, el documento de la AEMPS “Anexo VIII C. Instrucciones revisadas para la actualización del apartado Protección de datos personales en la hoja de información al sujeto (HIP/CI) en lo relativo al Reglamento (UE) nº 2016/679 General de Protección de Datos”, (anexo al documento de instrucciones de la AEMPS, citado), prevé lo siguiente:

“Tanto el Centro como el Promotor son responsables respectivamente del tratamiento de sus datos y se comprometen a cumplir con la normativa de protección de datos en vigor. Los datos recogidos para el estudio estarán identificados mediante un código, de manera que no se incluya información que pueda identificarle, y solo su médico del estudio/colaboradores podrá relacionar dichos datos con usted y con su historia clínica. Por lo tanto, su identidad no será revelada a ninguna otra persona salvo a las autoridades sanitarias, cuando así lo requieran o en casos de urgencia médica. Los Comités de Ética de la Investigación, los representantes de la Autoridad Sanitaria en materia de inspección y el personal autorizado por el Promotor, únicamente podrán acceder para comprobar los datos personales, los procedimientos del estudio clínico y el cumplimiento de las normas de buena práctica clínica (siempre manteniendo la confidencialidad de la información)”.

Aunque este documento hace referencia a la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos personales (LOPD), derogada por la LOPDGDD, a los efectos que interesan se desprende de este documento que, como apunta la consulta, y en línea con dicho marco normativo, el Hospital es el responsable del tratamiento de los datos de la HC de los pacientes que participan en los ensayos clínicos.

Por lo que se desprende de la consulta, **el Hospital** es, a efectos de la normativa de protección de datos y de la normativa sectorial (Ley 21/2000 y Ley 41/2002), el responsable de los datos tratados en la HC de los pacientes que atiende, incluidos aquellos que, a través de la prestación de su consentimiento, deciden participar en un ensayo clínico. Con respecto al investigador principal, sería “el investigador responsable de un equipo de investigadores que realizan un ensayo clínico en un centro de ensayos clínicos” (art. 2.1.u) RD 1090/2915).

Ahora bien, según la consulta, *“tanto el Hospital como el Promotor están legitimados como responsables respectivamente del tratamiento de los datos personales que participan en el ensayo. El Hospital es responsable del tratamiento de datos identificados y el Promotor es responsable del tratamiento de datos seudonimizados”*. La consulta añade que *“también el personal autorizado por el Promotor está legitimado para acceder a datos identificados de sujetos del ensayo para realizar tareas de monitorización o auditoría”*.

Conviene tener presente que, a los efectos de la normativa de protección de datos, los datos seudonimizados son datos de carácter personal. Así, según el considerando 26 del RGPD: *Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. (...)”*.

Según la información disponible, tanto el Hospital como el Promotor tienen responsabilidad en el tratamiento de datos personales (sean identificados o seudonimizados) relacionados con la realización de ensayos clínicos.

Partiendo de esta premisa no podemos descartar que se tenga que considerar que tanto el Hospital y el Promotor deciden qué tratamiento hay que hacer de los datos personales relacionados con el ensayo clínico.

Si es así, y son los dos (Hospital y Promotor) los que determinan qué tratamiento de datos personales se llevará a cabo para el ensayo (cohorte de pacientes afectados, objetivos y alcance del estudio, información personal que puede ser necesario tratar, etc.), parecería razonable establecer una responsabilidad compartida o corresponsabilidad sobre el tratamiento de datos personales (identificados o seudonimizados) necesarios para llevar a cabo el ensayo clínico, posibilidad prevista en el artículo 4.7 del RGPD.

Así, según el artículo 26 del RGPD:

*“1. Cuando **dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento** serán considerados corresponsables del tratamiento. Los corresponsables **determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas** en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.*

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables”.

En línea con estas previsiones, el artículo 29 de la LOPDGDD dispone que: *“La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento”*.

En definitiva, en relación con ensayos clínicos en que tanto el Hospital como el Promotor *“determinan las finalidades y medios del tratamiento”* (art. 4.7 RGPD), se podría articular un modelo de corresponsabilidad de ambos respecto al tratamiento de datos personales relacionados con los ensayos. En este caso, el tratamiento deberá quedar reflejado y concretado en el correspondiente acuerdo, en los términos previstos en los artículos 26 y 28 del RGPD.

Partiendo de la base de que se establezca un esquema de corresponsabilidad en el tratamiento de datos, hay que apuntar lo siguiente en relación con el rol del Monitor.

El Monitor deberá acceder a determinada información, no solo información pseudonimizada de la que es responsable el Promotor que encarga el ensayo, sino específicamente a información personal (HC) de los pacientes del Hospital, para el cumplimiento de las funciones que tiene atribuidas (RD 1090/2015). Esto, con independencia de que este Monitor sea interno o externo, ya que en ambos casos sus funciones son las mismas.

El Monitor del ensayo actuaría en el supuesto planteado por cuenta no de uno, sino de dos responsables del tratamiento (Hospital y Promotor), ya que serán responsables los dos que le indicarán al Monitor el alcance y las condiciones del tratamiento de información de los pacientes que está autorizado a hacer, y con qué finalidad. Hay que entender, pues, que las condiciones del tratamiento de datos que hará el Monitor las deberán establecer conjuntamente y de forma coordinada ambos responsables, ya que el Monitor trata información personal por cuenta de los dos responsables.

Por lo tanto, deberán ser los dos responsables (Hospital y Promotor) los que establezcan un acuerdo o contrato de encargo con el Monitor. De hecho, parece que se podría establecer en un único acuerdo o contrato, en el que participen los tres intervinientes (Hospital, Promotor y Monitor), las condiciones del tratamiento que llevará a cabo el Monitor, como encargado del tratamiento, por cuenta de los dos responsables.

Por todo lo expuesto, la utilización de este esquema de corresponsabilidad en el contexto de los ensayos clínicos (y la articulación de un único contrato de encargo del tratamiento con el Monitor, por parte de ambos responsables) parece bastante razonable, desde la perspectiva de la normativa de protección de datos personales.

Ahora bien, en caso de que no se establezca un modelo de corresponsabilidad en los términos apuntados y se deba entender que el Hospital es el único responsable, a efectos de la normativa de protección de datos, respecto a la información personal a la que debe tener acceso el Monitor, será preciso que el Hospital establezca un encargo del tratamiento con el Monitor, como se concretará más adelante.

V

Hechas estas consideraciones, nos referimos a la **primera pregunta** formulada: *“¿Podría el Hospital entender que el acceso del Monitor externo a los datos personales identificados de los sujetos del ensayo bajo control del Hospital está legitimado*

indirectamente en virtud de la HIP/CI que legitima el acceso directo del Promotor a estos datos?”.

Según la consulta, cuando el Promotor designa a una empresa como Monitor externo, aunque el Promotor y este Monitor externo hayan firmado un contrato de tratamiento de datos, el Hospital entiende que el Monitor externo no está legitimado para acceder a los datos personales identificados de los sujetos del ensayo en virtud de la HIP/CI y, por lo tanto, *“el Hospital exige la firma de un contrato de tratamiento de datos entre el Hospital y el Monitor externo en los términos del artículo 28 del RGPD”.*

En este punto, conviene tener presente que el artículo 28.1 del RGPD dispone lo siguiente:

*“1. Cuando se vaya a realizar un **tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado** que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado”.*

Por la información de la que se dispone, el Monitor externo del ensayo deberá acceder a datos de la HC de los pacientes, para realizar tareas de comprobación y monitorización del ensayo clínico que se lleva a cabo en el propio Hospital. Por lo tanto, por la información disponible, es el Hospital en el que se realiza el ensayo, como responsable de la HC de los pacientes, al que correspondería determinar las condiciones de este acceso del Monitor, en la medida que puede resultar pertinente para dichas tareas de monitorización, previstas en la normativa (RD 1090/2015).

El encargo del tratamiento que haya podido establecer el Promotor con el Monitor externo no sería suficiente para que el Monitor pueda acceder a datos no seudonimizados que se tratan bajo la responsabilidad del Hospital, pues debería corresponder al Hospital —y no al Promotor— la concreción de las condiciones del acceso y tratamiento que puede hacer el Monitor de datos de la HC, para el cumplimiento de sus funciones.

Así, un contrato de encargo establecido únicamente entre el Promotor y el Monitor externo, en el que no participe el Hospital, resultaría insuficiente a los efectos que interesan, ya que el Hospital no habría participado en la designación ni en el establecimiento de sus obligaciones, en los términos exigidos en la normativa (art. 28 RGPD).

El artículo 28.1 del RGPD exige al responsable designar únicamente encargados que ofrezcan suficientes garantías de que los datos se tratarán conforme a la normativa.

Esto supondría que, en caso de que únicamente se dispusiera de un contrato de encargo entre el Promotor y el Monitor, el Hospital estaría autorizando el tratamiento de datos de salud de los pacientes por un encargado (el Monitor externo) en cuya designación no habría participado, para velar por si ofrece suficientes garantías. Este es otro elemento que podría hacer aconsejable valorar el establecimiento de un modelo de corresponsabilidad respecto al tratamiento de datos (*ex art. 26 RGPD*), al que ya nos hemos referido.

En cualquier caso, teniendo en cuenta que el Monitor externo del ensayo llevaría a cabo un acceso a datos de la HC por cuenta del Hospital en el que se realiza el ensayo, el Hospital debe articular necesariamente el acceso y el tratamiento de datos

de la HC por parte del Monitor, para el cumplimiento de sus funciones, a través de un encargo del tratamiento, por exigencia de la previsión del artículo 28.1 del RGPD. Esto, sin perjuicio del encargo que haya establecido el Promotor con el Monitor o de supuestos en los que se establezca una corresponsabilidad del Hospital y el Promotor, en los términos apuntados en el fundamento jurídico anterior.

En cualquier caso, dicho contrato se debe ajustar a las previsiones del artículo 28.3 del RGPD.

Dicho esto, hay que tener en cuenta la previsión de la disposición transitoria quinta de la LOPDGDD, en relación con los contratos de encargo del tratamiento que, si procede, haya suscrito el Hospital con anterioridad al 25 de mayo de 2018. Al respecto, el RGPD ha introducido modificaciones en el contenido mínimo del contrato que regula el encargo del tratamiento, que afectan tanto a las obligaciones del responsable como a las del encargado (el Hospital y el Monitor externo, respectivamente), que se deberán tener en cuenta en el caso que nos ocupa.

En relación con dichos contratos suscritos puede ser de interés consultar la Guía sobre el encargado del tratamiento en el RGPD, elaborada por las autoridades de protección de datos para ayudar a los responsables y los encargados en la adaptación a las exigencias del RGPD, disponible en la web de la Autoridad <http://apdcat.gencat.cat/ca/inici/>.

En cualquier caso, esta conclusión no queda desvirtuada por el hecho de que el acceso del Monitor externo del ensayo a datos de la HC tenga suficiente base jurídica en base al consentimiento informado que firma el paciente que participa en el ensayo a través de la cláusula a la que se refiere la consulta (HIP/CI), y en base a las previsiones normativas estudiadas, que habilitan el acceso a datos de la HC por parte del Monitor del ensayo, para el cumplimiento de sus funciones (RD 1090/2015).

Como ha quedado dicho, el marco normativo estudiado habilita el tratamiento de datos de salud para la realización de ensayos clínicos, sobre la base del consentimiento informado del paciente que participa en ellos (art. 6 y 9 RGPD y disposición adicional 17.^a LOPDGDD, normativa de autonomía del paciente y RD 1090/2015). Ahora bien, esto no desvirtúa la necesidad de que este acceso se articule a través del correspondiente encargo del tratamiento (*ex art. 28.1 RGPD*), dado que el tratamiento se lleva a cabo por cuenta del responsable de las HHCC de los pacientes, esto es, por cuenta del Hospital, en los términos apuntados.

VI

Teniendo en cuenta las consideraciones expuestas, nos referimos a la **segunda pregunta** formulada: *“Si la respuesta a la pregunta anterior es afirmativa, ¿podría el Hospital dejar de exigir la firma de un contrato de tratamiento entre el Hospital y el Monitor externo?”*.

Como ha quedado expuesto, el Hospital, como responsable de la HC, es el que determina las finalidades y medios del tratamiento de los datos de la HC (art. 4.7 RGPD), a la que se refiere la consulta, sin perjuicio de que, vista la participación que debe tener el promotor en el ensayo clínico, se articulen modelos de corresponsabilidad del tratamiento. Cuando se produce un tratamiento por cuenta del responsable (como el que llevaría a cabo, en el caso que nos ocupa, el Monitor externo respecto al ensayo que se lleva a cabo en el Hospital), este tratamiento se debe

articular necesariamente a través del correspondiente contrato de encargo del tratamiento (art. 28.1 RGPD).

VII

A continuación, hacemos referencia a la **tercera Pregunta**: “*Si la respuesta a la pregunta anterior es afirmativa, ¿debería establecer el Hospital algún tipo de salvaguardia adicional antes de permitir el acceso del Monitor externo a datos personales bajo el control del Hospital?*”.

Como ha quedado expuesto, vista la información disponible, partimos de la base de que correspondería suscribir el correspondiente acuerdo o contrato de encargo del tratamiento entre los corresponsables del tratamiento —el Hospital y el Promotor— y el Monitor externo como encargado (art. 26 RGPD), en los términos del artículo 28 del RGPD.

Por lo tanto, de entrada, en respuesta a la consulta formulada, el establecimiento de “*salvaguardias adicionales*” no sustituiría a la necesidad de articular el encargo del tratamiento a través del correspondiente contrato.

Aparte de que el contrato entre el Hospital y el Monitor externo deba recoger las previsiones del artículo 28.3 del RGPD, será preciso que el tratamiento de los datos personales de la HC dé cumplimiento al resto de principios y obligaciones de la normativa de protección de datos personales.

Entre otras, en relación con el tratamiento de información personal de los participantes en el ensayo clínico, conviene hacer especial mención de las siguientes cuestiones:

El tratamiento de información para finalidades de investigación debe adecuarse a los principios establecidos en el RGPD.

De entrada, hay que reiterar la necesidad de aplicar al tratamiento de datos las exigencias derivadas del principio de minimización (art. 5.1.c) y art. 89 RGPD). En este sentido, en el contexto de la investigación médica y de la realización de ensayos clínicos, desde la perspectiva de la protección de datos resulta de especial interés la utilización de mecanismos de seudonimización de la información (art. 89 RGPD), como mecanismo para reforzar el cumplimiento de dicho principio.

Puesto que en el ámbito de los ensayos clínicos se tratará información codificada o seudonimizada que, como ha quedado dicho, sigue siendo información personal a efectos de la normativa de protección de datos, habrá que prestar especial atención a las previsiones sobre los procedimientos de seudonimización y las medidas para evitar la reidentificación.

En este sentido conviene tener en cuenta también las exigencias específicas establecidas por el apartado segundo de la disposición adicional decima séptima de la LOPDGDD para el tratamiento de datos en la investigación en salud, en especial en relación con la evaluación del impacto relativa a la protección de datos.

También hay que referirse al principio de integridad y confidencialidad (art. 5.1.f) RGPD). La información de los afectados deberá ser tratada por todos los intervinientes (el propio Hospital, los investigadores, el Promotor y el Monitor), ya sea en su condición de responsables o de encargados del tratamiento, de acuerdo con este principio.

Según el artículo 24 del RGPD: *“1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario. (...)”*.

El RGPD impone la obligación al responsable del tratamiento de adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales que serán tratados, obligación que también hace extensible al encargado del tratamiento (art. 28.3.c) RGPD).

El RGPD configura un sistema de seguridad que ya no se basa en los niveles de seguridad básico, medio y alto previstos en el Reglamento de desarrollo de la LOPD, aprobado por el Real decreto 1720/2007, de 21 de diciembre (RLOPD), sino en determinar, a partir de las características del tratamiento y de una previa valoración de los riesgos, qué medidas de seguridad son necesarias en cada caso (considerando 83 y artículo 32 RGPD).

Por lo tanto, por aplicación de las previsiones de la normativa de protección de datos personales (artículos 24 y 32 RGPD), resultaría exigible la elaboración de un análisis y valoración de los riesgos que supone el tratamiento de datos, que tiene como objetivo determinar las medidas técnicas y organizativas que deberán aplicar responsables y encargados del tratamiento (ex art. 28.3.c) RGPD).

Habrá que tener en cuenta, si procede, la previsión de la disposición adicional primera de la LOPDGDD, relativa a las medidas de seguridad en el ámbito del sector público, según la cual:

“1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

(...)”.

De acuerdo con las consideraciones hechas hasta ahora en relación con la consulta planteada, se extraen las siguientes

Conclusiones

Puesto que el Monitor externo del ensayo debe acceder a datos de la HC por cuenta del responsable (el Hospital), este debe articular el acceso y tratamiento de datos por

parte de dicho Monitor, para el cumplimiento de sus funciones, necesariamente a través de un encargo del tratamiento.

Esta conclusión no queda desvirtuada por el hecho de que el acceso del Monitor externo del ensayo a datos de la HC de los participantes en el ensayo tenga suficiente base jurídica, en base al consentimiento informado de las personas afectadas.

No se puede sustituir el contrato de encargo entre el Hospital y el Monitor externo del ensayo por otros tipos de “*salvaguardias adicionales*”, sin perjuicio del cumplimiento de los principios y obligaciones de la normativa de protección de datos.

Barcelona, 11 de enero de 2019