Ref. CNS 3/2020

Dictamen en relación con la consulta de un centro sanitario sobre la legalidad de una Plataforma de gestión de ensayos clínicos

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito de un centro sanitario (en adelante, el Hospital) sobre la legalidad, conforme a la normativa de protección de datos, de una Plataforma de gestión de ensayos clínicos (en adelante, la Plataforma).

La consulta se acompaña de copia del documento "Acuerdo de red de organizaciones sanitarias" que, por la información aportada, firmaría el Hospital con la empresa responsable de la Plataforma, y de copia del documento "Addenda sobre el tratamiento de datos" , que complementa el documento anterior. Asimismo, la consulta se acompaña de información sobre la Plataforma (...).

Analizada la petición y documentación adjunta, vista la normativa vigente aplicable, y el informe de la Asesoría Jurídica, se dictamina lo siguiente.

(...)

II

La consulta explica que la Plataforma es una iniciativa privada que surge de un proyecto financiado por fondos públicos y privados bajo la convocatoria europea IMI (Innovative Medicines Initiative) para impulsar el diseño y ejecución de ensayos clínicos basado en la obtención de datos agregados de la historia clínica electrónica, aplicable a cualquier centro que utilice este formato electrónico, como es, según explica la consulta, el caso del Hospital. Según la consulta, la plataforma tiene por objetivo "construir una red paneuropea/global de centros que quieren maximizar su participación en la investigación clínica con la industria y el mundo académico."

Según la consulta, la Plataforma, de la empresa (...), es una herramienta que permite identificar, de forma automática y en base a los datos de la historia clínica electrónica, los pacientes que cumplen determinados criterios, coincidentes con los de un ensayo clínico determinado. La consulta explica que si los criterios coinciden o interesan a los terceros, "el Hospital recibirá una alerta y contactaría con los pacientes, ofreciendo la posibilidad de participación en el estudio o ensayo clínico."

El documento que se acompaña a la consulta explica que la Plataforma es la mayor red europea para la reutilización de datos de historias clínicas electrónicas para investigación médica. Según esta información, entre los servicios que la Plataforma ofrece a los hospitales se encuentra el reclutamiento de pacientes para poder realizar investigación cl

La consulta añade que el software estaría instalado en el servidor del Hospital, y que se firmará el preceptivo contrato de encargado del tratamiento. En relación con este contrato y con el tratamiento de datos objeto de consulta, se adjunta a la consulta copia del documento "ACUERDO DE RED DE ORGANIZACIONES SANITARIAS" (en adelante, el Acuerdo) y del documento "ADENDA SOBRE TRATAMIENTO DE DATOS" (en adelante, la Adenda), así como otra información complementaria sobre la Plataforma.

Sita la consulta en estos términos, 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 número, 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, ya sea de los pacientes o de los profesionales del Hospital que serán usuarios de la Plataforma, está sometido a los principios y garantías 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)).

III

Cabe decir que a pesar de la amplitud de la documentación aportada al realizar la consulta, los documentos resultan poco concretos, ya veces incluso contradictorios, tanto en lo que se refiere a la sistemática empleada, como en lo que respecta a la definición de los tratamientos que se pretende llevar a cabo, la definición de los papeles que van a jugar cada uno de los agentes implicados y de sus responsabilidades. En este sentido resulta especialmente confusa la utilización de dos documentos y una adenda donde se tratan de forma a menudo mezclada aspectos relativos a datos que se tratarían en régimen de corresponsabilidad, con otros aspectos relativos a datos que se tratarían en el marco de un encargo del tratamiento. Convendría diferenciarlo claramente.

En cualquier caso, esta carencia de claridad impide hacer un pronunciamiento preciso sobre estas cuestiones.

Sin embargo, visto el contenido de la documentación aportada, referida a la participación del Hospital en la Plataforma, desde la perspectiva de la protección de datos conviene analizar distintos aspectos, en concreto:

1. Descripción del tratamiento de datos personales 2. Necesidad de realizar una Evaluación de Impacto en la Protección de Datos 3. Esquema de atribución de responsabilidades 4. Legitimación del tratamiento 5. Aplicación del principio de minimización

6. Ejercicio de derechos 7. Transferencias internacionales de datos (TID) 8. Medidas de seguridad

Descripción del tratamiento de datos personales

a) Tratamiento de datos de los pacientes:

En síntesis, según el documento "Acuerdo de Red de organizaciones sanitarias", la empresa (...) es propietaria de una plataforma informática basada en la nube para facilitar la investigación, en concreto, para "permitir a los usuarios analizar poblaciones agregadas de pacientes de organizaciones sanitarias participantes y otras fuentes de datos".

Según el Acuerdo, la organización sanitaria (OS) -que sería, en caso de que nos ocupa, el Hospital que formula la consulta-, accedería a la Plataforma a través de una licencia que le proporcionaría la empresa, que incluye el acceso a la Red de Investigación Global de

la empresa. El apartado 1.16 del acuerdo define la Red como "la plataforma informática… basada en la nube para facilitar la investigación, como por ejemplo, pero no limitado, a permitir a los usuarios analizar poblaciones agregadas de pacientes de las organizaciones sanitarias. "

La utilización de expresiones como "por ejemplo, pero no limitado" impide conocer con exactitud en qué consistirá el tratamiento de los datos de los pacientes llevados a cabo por la plataforma.

Hay otros ejemplos de cuestiones que no están suficientemente bien definidas. Así, por ejemplo, según el punto 2.1 del Acuerdo, el Hospital "posee y retiene el derecho de controlar la transferencia y uso de los datos del OS en relación con la Red de Investigación Global de la empresa . Los datos personales relativos a pacientes del OS se conservan en el entorno del OS y no se transfieren fuera del entorno del OS, salvo lo dispuesto en la Sección 2.2 (del Acuerdo)."

Habría que concretar la referencia al "entorno del OS" (que tampoco aparece definido de forma clara en la definición que da el apartado 1.5 del Acuerdo), dado que no está claro a que se está refiriendo (los servidores del OS, el tratamiento bajo su responsabilidad con la colaboración del encargado del tratamiento…).

También existen ciertas confusiones o contradicciones en el tratamiento que puede hacer la empresa de la información seudonimizada. Según el punto 2.4 del Acuerdo: "El OS manifiesta y garantiza que los datos del OS que se envíen a la empresa se seudonimizarán de conformidad con el RGPD y todas las leyes de privacidad antes de transferirse a (la empresa). Sin perjuicio de ello, cada una de las Partes llevará a cabo todas las actividades descritas en el Acuerdo y protegerá la privacidad y seguridad de todos los datos personales de conformidad con el RGPD."

Parecería, a partir de esto y de lo que se explica en el texto de la consulta que el OS entregará información de salud de sus pacientes, previamente pseudonimizada en la empresa.

Se valora positivamente el tratamiento seudonimizado de datos de los pacientes, de que dispone el Hospital para fines de investigación médica sin perjuicio de lo que se dirá más adelante.

Según se explica en el texto de la consulta (aunque en los documentos adjuntos no se explica con la misma claridad), parece que al menos en un primer momento, la función de la empresa consiste en identificar a los pacientes coincidentes con el perfil de paciente sobre los que se quiere llevar a cabo un determinado estudio.

En esta fase, los resultados que podrían entregarse a terceros ("terceros y promotores" en los términos que se expresa la consulta) serían resultados anónimos. En este sentido, el punto 1.9 del Acuerdo, hace referencia a los "resultados anónimos de las consultas en las redes de datos de (la empresa), como por ejemplo recuentos de los pacientes, métricas de prevalencia, tasas de incidencia y otros datos estadísticos agregados, que se proporcionan a los usuarios de la plataforma.". Parece que esta referencia debe entenderse hecha a resultados agregados de las consultas que no pueden vincularse de ninguna manera con personas concretas. Sólo en ese caso resultaría adecuado referirse a información anónima.

Cabe recordar que sólo se puede considerar como anónima la información que se desvincula de manera irreversible del paciente, lo que no sucede, precisamente, con la información seudonimizada. La distinción es relevante desde la perspectiva de la protección de datos, ya que la información seudonimizada es a todos los efectos información personal protegida por el RGPD, mientras que la información anónima pierde esta condición (considerando 26 RGPD).

En este punto, es necesario hacer un inciso, porque en algunos puntos de los documentos aportados parece no tenerse en cuenta esta distinción. Así, por ejemplo, según el punto 2.1 del Acuerdo, se afirma que los datos personales relativos a pacientes del OS se conservan en el entorno del OS y no se transfieren fuera del entorno del OS OS, salvo lo dispuesto en la Sección 2.2 (del Acuerdo).” . Cuando en realidad por lo que se expone en los mismos documentos los datos seudonimizados de los pacientes pasan a los servidores de la empresa.

A partir de esta información seudonimizada, y si los criterios coinciden con el interés del tercero o promotor, en la consulta se indica que el centro contactaría con los pacientes ofreciendo la posibilidad de participar en el estudio.

No se encuentra suficientemente concretado en la documentación disponible, qué tipología de terceros destinatarios podrían solicitar y recibir información seudonimizada de las HC del Hospital, el alcance geográfico que podrían tener estos terceros, si se limita al ámbito europeo (entidades que, en principio, podrían estar sometidas como el Hospital a las previsiones del RGPD), o si los destinatarios podrían ser hospitales o centros de investigación de otros países. En cualquier caso, en la medida en que se trate de información anonimizada no estaría sujeto a las previsiones del RGPD.

Hay que tener en cuenta que existen diferentes modalidades de investigación que prevé la Ley 14/2007, de 3 de julio, de investigación biomédica (LIB), pero también otros tipos de investigación que quedan excluidos del ámbito de aplicación de la LIB, como los estudios observacionales (art. 58.2 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)), los ensayos clínicos, a los que no se aplica la LIB, y que como recuerda el considerante 161 del RGPD, están regulados por su normativa específica (Reglamento UE 536/2014, de 16 de abril, sobre los ensayos clínicos de medicamentos de uso humano) , o los estudios epidemiológicos (previstos en la legislación de autonomía del paciente (art. 16.3 Ley 41/2002 y art. 11.3 Ley 21/2000).

Teniendo en cuenta que las tipologías de investigación médica son muy variadas, en función del tipo de estudio que se quiera llevar a cabo puede ser necesario identificar a los pacientes, o no.

Así, en el caso de los ensayos clínicos, dada la normativa reguladora, sí sería necesario que el responsable o promotor del ensayo contacte con los pacientes que se haya comprobado, a partir del cribado inicial de información sedonimizada que permite la Plataforma, que pueden ser participantes potenciales en el ensayo. En este caso, obviamente sí puede resultar necesario que el Hospital contacte con estos pacientes, a fin de ofrecerles la posibilidad de participar. Ahora bien, en otros casos, puede que un centro de investigación pueda llevar a cabo un estudio con datos seudonimizados (apartado d) de la DA 17ª de la LOPDDDD) sin que sea estrictamente necesario contactar con los pacientes. Pero no parece que sea éste el caso expuesto en la consulta, dado que se limita a indicar que “los datos accesibles por terceros serían anonimizados”.

En este sentido, se observa también una contradicción con el apartado 2.3 del Acuerdo, en el que se otorga a la empresa el derecho a “acceder a, utilizar, alojar, copiar, traducir, distribuir y formatear los datos de la OS”. La utilización del término “distribuir” parece contradictorio con el objeto definido en la consulta y con el contenido de la cláusula 2.2 del Acuerdo.

Se debe hacer notar en este punto que la exposición de la consulta incurre en una contradicción, porque mientras por un lado indica que “los datos accesibles por terceros serían anonimizados” a continuación se indica que “(los terceros no podrían saber a quien corresponden)” . Y ambas expresiones no son equivalentes. La primera expresión hace referencia a datos anónimos. La segunda podría hacer referencia también a datos seudonimizados. En cualquier caso, dado que en los textos de los documentos adjuntos no se

prevé que la empresa facilite a terceros conjuntos de datos seudonimizados, habrá que entender que se refiere sólo a datos anónimos.

El reclutamiento de participantes para un ensayo clínico a partir de la participación en la Plataforma podría resultar habilitado siempre que sea el Hospital, como responsable del HC, quien reidentifique al paciente.

A pesar de lo expuesto en la consulta, no es menos cierto que los apartados 2.1 y 2.2 del Acuerdo abren la puerta, dentro de lo que se llaman como funciones avanzadas de la plataforma, a las que se puedan transferir datos de pacientes a terceros. En ese caso esta comunicación de datos estaría sometida al RGPD. En cualquier caso, en este dictamen no se analizará esta cuestión, puesto que la consulta sólo hace referencia de paso a esta cuestión, sin hacer una exposición precisa y que estos apartados reservan el control y la decisión de estas transferencias a el OS y recogen expresamente que será necesario aplicar los principios de la protección de datos personales.

- Tratamiento de datos de los usuarios:

Se prevé utilizar datos identificativos de los profesionales del Hospital usuarios de la Plataforma. El tratamiento de estos datos será objeto, según la información disponible (punto 1.6 del acuerdo), de un encargo del tratamiento (art. 28 RGPD).

En principio estos datos parece que no serían seudonimizados, aunque el apartado 2 de la adenda, dedicado a las disposiciones generales (por tanto aplicable también a los datos de los usuarios) prevé entre las obligaciones del OS "proporcionar sólo datos seudonimizados en el servidor de (la empresa)" (apartado b)).

Obviamente, estos datos son datos personales sometidos a los principios y garantías de el RGPD.

Según el apartado 1.1 de la Adenda, la empresa "actúa como encargado del tratamiento bajo el control del Hospital respecto al tratamiento de datos personales de los usuarios del Hospital de los productos y servicios prestados en virtud del Acuerdo. Estos datos personales consisten en la información típica utilizada para implementar el control de acceso (...).

Según el apartado 8.2 de la Adenda, la empresa "sólo procesará los datos personales de los usuarios del hospital necesarios para prestar los servicios en virtud del Acuerdo, concretamente para proporcionar a los usuarios del Hospital el acceso a los productos de (la empresa)", en concreto: Nombre completo; información de contacto profesional, incluyendo direcciones de correo electrónico; nivel/situación profesional (cargos); información sobre el uso de la plataforma; información de registro de auditoría, incluyendo la dirección IP.

Se valora positivamente esta concreción con respecto al tratamiento de datos de los usuarios.

No puede descartarse que algunos de estos datos puedan ser tratados, no ya por el propio encargado (la empresa), sino por otros terceros. En principio, no parece que deba ser necesariamente así, aunque el apartado 4.1 de la adenda permitiría el acceso por parte del subencargado del tratamiento (Amazon web services) que albergaría la plataforma.

IV

Necesidad de realizar una Evaluación de Impacto en la Protección de Datos (AIPD)

Según dispone el artículo 35 del RGPD:

"1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o finas, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de las datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de las datos personales relativas a condenas e infracciones penales a que se refiere el artículo 10, o

c)observación sistemática a gran escala de una zona de acceso público."

Si nos atenemos a las características del tratamiento de datos seudonimizados objeto de consulta, que son datos de salud y genéticos (art. 9 RGPD), que el tratamiento se producirá previsiblemente a gran escala (no sólo por los entes que la tratarán sino porque se podría tratar de un conjunto cualitativa y cuantitativamente muy significativo de datos de las HHCC), en caso de que nos ocupa resulta imprescindible llevar a cabo una AIPD.

En este sentido el Grupo de Trabajo del Artículo 29 ("Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tracamento entraña un probablemente un alto riesgo a efectos del RGPD"), ha explicitado que es necesario llevar a cabo una AIPD cuando se dan, entre otras, estas características en el tratamiento: la elaboración de perfiles y predicciones en base a datos de salud, entre otros; tratamiento de categorías de datos sensibles; tratamiento de datos a gran escala; datos relacionados con personas vulnerables; y uso innovador de tecnologías, entre otros. No sólo eso, sino que en este caso hay que mencionar de nuevo que la posibilidad de reidentificación de datos personales siempre comporta un cierto riesgo, que hay que prever y paliar en la medida de lo posible.

Todas estas características confluyen en el tratamiento que nos ocupa y por tanto la realización de una AIPD previa al tratamiento resulta imprescindible.

Además, según el apartado 2.f) de la DA 17a de la LOPGGD:

> **"f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:**
>
> **1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá**

de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de las datos.

2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no accedan a datos de identificación de los interesados.

4.º Designar a un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con lo previsto en el artículo 27.1 del Reglamento (UE) 2016/679."

Los mecanismos concretos de seudonimización, así como aquellos que se establezcan para minimizar el riesgo de reidentificación indebida de los pacientes por parte de otros participantes en la Plataforma, son cuestiones que deben estar definidas y previstas de forma previa al inicio del tratamiento, y que deberá concretarse en la evaluación de impacto en la protección de datos (35 RGPD y art. 2.f.1 LOPDGDD).

Por todo lo expuesto es necesario llevar a cabo una evaluación de impacto en los términos previstos en el artículo 35 del RGPD, antes del inicio del tratamiento.

Nos remitimos, al respecto, a la Guía práctica "Evaluación de impacto relativa a la protección de datos", disponible en la web www.apd.cat.

V

Esquema de atribución de responsabilidades

Hay que partir de la base de que el Hospital es responsable de la información personal de los pacientes contenida en la historia clínica de éstos (HC), en los términos de la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica, y de 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 .

En la documentación aportada (Acuerdo y Adenda) se prevé establecer dos relaciones diferenciadas entre la empresa propietaria de la Plataforma (en adelante, la empresa), y el Hospital que formula la consulta (OS), en función de la información personal objeto de tratamiento. Según el apartado 1.1 de la Adenda, ésta tiene por objeto "diferenciar las responsabilidades de las partes como responsables del tratamiento conjuntos, y como encargado del tratamiento". Este mismo apartado concreta lo siguiente:

La empresa "actúa como encargado del tratamiento bajo el control del OS en lo que respecta al tratamiento de datos personales de los usuarios del Hospital de los productos y servicios prestados en virtud del Acuerdo. (...).
La empresa "y el Hospital son responsables del tratamiento conjuntos en lo que respecta al tratamiento de los datos clínicos de pacientes (...)."

En este sentido, la Adenda prevé unas "disposiciones generales sobre el tratamiento de datos personales" (punto 2), y unas previsiones referidas, por un lado, a las responsabilidades de las partes en relación con el tratamiento de datos en el que la empresa es encargada del tratamiento ("PARTE I" de la Adenda (punto 8)) y, por otra, a las responsabilidades de

la empresa y el Hospital en el tratamiento de datos seudonimizados de los pacientes, del que ambos son corresponsables ("PARTE II" de la Adenda (punto 9)).

- Sobre el régimen de corresponsabilidad

De acuerdo con el artículo 4.7 RGPD el responsable del tratamiento es "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento;"

La normativa también prevé la posibilidad de establecer una corresponsabilidad sobre el tratamiento, es decir, que dos o más responsables determinen conjuntamente los objetivos y medios del tratamiento (art. 4.7 y art. 26 RGPD y art. 29 LOPDGDD).

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 ya sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus respectivas responsabilidades 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."**

Cuando se establece un modelo de corresponsabilidad, el RGPD exige la firma de un acuerdo que determine claramente las funciones y relaciones respectivas de los corresponsables en relación con los interesados, quienes deben conocer los aspectos esenciales del acuerdo (art. 26 RGPD). En el caso que nos ocupa, la documentación disponible prevé que el Hospital y la empresa serán corresponsables respecto al tratamiento de datos seudonimizados de los pacientes del Hospital. De ser así, sería necesario que los corresponsables establecieran un acuerdo específico (en los términos del art. 26 RGPD) e informen a las personas afectadas.

Ahora bien, aunque la posibilidad de responsabilidad conjunta está prevista por el propio RGPD, la descripción de las responsabilidades que se realiza en la documentación aportada no parece obedecer precisamente a este esquema.

"

Así, en el punto 2.1 del Acuerdo se indica que La OS posee y retiene el derecho a controlar la transferencia y el uso de las datos de la OS en relación con la Red de Investigación Global (de la empresa). Las datos personales relativas a pacientes de la OS se conservan en el entorno de la OS, salvo por lo dispuesto en la Sección 2.2 siguiente."

Por su parte, la Sección 2.2 prevé "Si la OS decide a su entera discreción, activar ciertas funciones avanzadas de la Red de investigación global, es posible que fuera necesario transferir ciertas datos personales...."

El apartado 3.6 del Acuerdo ("Red de colaboración"), explica que el Hospital puede solicitar a la empresa la habilitación para que se le muestren los resultados de consultas realizadas a otros colaboradores de la red. Este mismo apartado contempla que el Hospital puede cerrar el acceso a los datos a otros colaboradores.

Es decir, según la información disponible, es el Hospital quien puede decidir utilizar la Plataforma para investigar y gestionar la información seudonimizada de las HC del Hospital, o puede decidir compartir la información con otros "colaboradores " de la "red de colaboración privada", que forman voluntariamente el Hospital y otras organizaciones sanitarias que participan en la Plataforma, según el apartado 1.4 del Acuerdo.

Esto respondería más a un esquema de encargo del tratamiento, del Hospital como responsable a la empresa como encargada, no sólo por tratar los datos de los trabajadores, usuarios de la plataforma, sino como encargada de llevar a cabo el proceso detección de los pacientes susceptibles de participar en un estudio).

Los responsables del tratamiento parecen más bien las diferentes entidades que participan en la red aportando información, así como las entidades que lleven a cabo los proyectos de investigación.

Es necesario, por tanto, aclarar cuál es el modelo elegido y la capacidad de decisión de cada uno de los responsables respecto a la información personal tratada.

- **Determinación del rol como responsable y encargado del tratamiento de los diferentes intervinientes**

En cuanto al tratamiento que lleve a cabo la empresa como encargada del tratamiento (en principio los datos de los usuarios, pero como acabamos de apuntar podría afectar también a los datos seudonimizados de los pacientes), es necesario velar por que la plataforma ofrezca garantías suficientes , en los términos del artículo 28.1 del RGPD, según el cual "1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, éste elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de forma que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado."

Si bien existen diferentes previsiones del artículo 28.3 del RGPD que se encuentran recogidas a lo largo de la Adenda, existen otras previsiones que no se explicitan en la documentación aportada.

La PARTE I de la Adenda (referida específicamente al tratamiento de los datos de los usuarios) sólo constata que "la empresa actúa como encargada del tratamiento y siguiendo las instrucciones del Hospital", concreta los datos personales de los usuarios que serán objeto de tratamiento, y prevé que, una vez expirado o rescindido el Acuerdo, el Hospital indicará si los datos deben ser devueltos o destruidos (en correspondencia con la previsión del art. 28.3.g) RGPD).

Ahora bien, la documentación resulta confusa ya que existen otras previsiones del artículo 28.3 del RGPD que están recogidas en diferentes apartados de la Adenda (concretamente, en el apartado 2 de la Adenda, en el que se incluyen "Disposiciones generales sobre el tratamiento de datos personales" tales como la obligación de abstenerse de tratar los datos personales para otros fines, o el compromiso general de cumplir sus obligaciones "de acuerdo con las instrucciones documentadas de el Hospital", que puede deducirse que se refieren al encargo del tratamiento, pero que también podrían referirse al modelo de corresponsabilidad para el tratamiento de las HHCC. En cualquier caso, vista la previsión del artículo 28.3. a) RGPD convendría referirse también a que la empresa debe seguir estas

instrucciones respecto a las transferencias internacionales de datos, lo que no se explicita en este punto. La obligación de confidencialidad (art. 28.3.b) se recoge en el apartado 1.3 de la Adenda. También la previsión del artículo 28.3.h) podemos considerar que queda recogida en el apartado 3.6 de la Adenda.

Respecto a otros apartados del artículo 28.3 que habría que explicitar en el contrato de encargo, vista la información disponible en varios apartados de la Adenda, destacamos lo siguiente:

En cuanto al apartado 28.3.c) RGPD (obligación del encargado de tomar las medidas de seguridad necesarias ej. art. 32 RGPD), el apartado 2 de la Adenda recoge diversas medidas en relación con los datos que le sean reveladas por el Hospital, por lo que podría entenderse que son medidas que se aplicarán en el contrato de encargo. De todos modos, convendría preverlo explícitamente en el contrato de encargo. Las medidas de seguridad de la empresa concretadas en los apartados 3.1 y 3.2 de la Adenda, también se incluirán, en su caso, en el contrato de encargo.

En cuanto al artículo 28.3.d), el punto 4.1 de la Adenda explicita que el Hospital "reconoce y acepta" al subencargado (Amazon Web Services), así como al nombramiento de filiales de la empresa como subencargados . Al respecto, el encargo del tratamiento deberá explicitar que la empresa queda obligada a informar al Hospital de cualquier cambio en los subencargados (ej. art. 28.3.2 RGPD) y que los subencargados quedan obligados en los términos de artículo 28.3.4 RGPD. En cualquier caso, el hecho de que en la Adenda se explicite la utilización de este subencargado no exime al responsable del tratamiento de velar para que éste reúna las garantías necesarias de acuerdo con el RGPD para llevar a cabo el tratamiento (apartados 1 , 2 y 4 del artículo 28 RGPD).

En cuanto a la previsión del artículo 28.3.e) RGPD -ayudar al responsable en la atención de solicitudes de derechos-, como se concreta en el FJ VIII de este dictamen, es necesario que el contrato de encargo del tratamiento concrete cómo se vehicularán las solicitudes de ejercicio de derechos que puedan plantearse al encargado.

Por tanto, hay que distinguir claramente en la Adenda las obligaciones exigidas por el artículo 28.3 RGPD al encargado (la empresa), en relación con el tratamiento que se hace como parte del encargo del tratamiento, y que habrán de ser suscritas en el correspondiente contrato o acuerdo, de todas aquellas previsiones que se refieren al tratamiento de datos seudonimizados que, por la información aportada, se traten bajo un régimen de corresponsabilidad. Es necesario sistematizar el contenido del contrato de encargo, de forma que se agrupen de forma más clara las diferentes obligaciones que, siguiendo las instrucciones del Hospital responsable, debe cumplir la empresa como encargada.

En relación con los contratos de encargo suscritos puede ser de interés consultar la Guía sobre el encargado del tratamiento en el RGPD, disponible en la web de la Autoridad http://apdcat.gencat.cat/ca/inici/.

VI

Legitimación del tratamiento

Según el punto 2.3 del Acuerdo, el Hospital otorga a la empresa el derecho a "acceder, utilizar, alojar, copiar, traducir, distribuir y reformatear los datos del OS, así como para crear y publicar trabajos derivados de éstas, exclusivamente con el fin de proporcionarlos para su uso en la Plataforma. (...). La licencia de datos concedida sólo es para fines de búsqueda."

Los tratamientos de datos personales deben tener, para ser lícitos, una base jurídica adecuada (art. 6.1 RGPD). Entre otros, el tratamiento de datos con fines de investigación puede resultar lícito si se dispone del consentimiento de los afectados (art. 6.1.a) RGPD), o bien si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos del responsable del tratamiento (artículo 6.1.e) RGPD), o también si es necesario para la satisfacción de intereses legítimos del responsable o de un tercero (artículo 6.1.f) RGPD).

Por otra parte, el artículo 5.1.b) RGPD establece que "el tratamiento ulterior de las datos personales con fines de archivo en interés público, fines de investigación científica e histórico o fines estadísticos no se considerará incompatible con los fines iniciales".

Hay que valorar positivamente que, por la información disponible, el tratamiento de datos que se producirá con la utilización de la Plataforma por parte del Hospital, se enmarca claramente en fines de investigación médica (puntos 2.3; 2.5; 6.3 del Acuerdo (puntos 9.1, 9.2 y especialmente, 9.5 de la Adenda, entre otros). El apartado 1.12 del Acuerdo concreta qué se entiende por "búsqueda", a efectos del contrato o acuerdo suscrito entre el Hospital y la empresa. Esta definición se refiere, específicamente, a la investigación en el ámbito sanitario y al tratamiento de datos de salud (art. 4.15 RGPD) y genéticas de los pacientes (4.13 RGPD), con fines de investigación médica.

En cuanto al tratamiento de categorías de datos objeto de especial protección, el artículo 9 del RGPD regula la prohibición general del tratamiento de datos personales de diversas categorías, entre otros, los datos relativos a la salud y los datos genéticas (apartado 1). El apartado 2 del mismo artículo 9 dispone que esta prohibición general no será de aplicación cuando concurra alguna de las circunstancias previstas en este artículo, entre otras:

> **"(...)**
>
> **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, en base al Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetarlo 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 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, conforme al presente Reglamento, para los derechos y 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 las datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichas finas. Siempre que estos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, estos fines se alcanzarán de ese mo**
>
> **(...)."**

Como recuerda estas Autoridad en ocasiones anteriores (Dictámenes 15/2019, 18/2019, o 59/2018, entre otras), el RGPD admite el tratamiento de datos de categorías especiales para fines de investigación, en particular en el ámbito sanitario, con cierta flexibilidad, como se desprende, entre otros, del considerante 52 del RGPD.

La disposición final quinta de la LOPDDDD ha añadido un nuevo artículo 105 bis) a la Ley 14/1986, de 25 de abril, General de Sanidad (LGS), 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."

La Ley 41/2002, modificada por la LOPDGDD, prevé el tratamiento de datos de salud para fines de investigación y parte de la regla general (como ya establecía la legislación de autonomía del paciente, anteriormente a la entrada en vigor de el RGPD y el LOPDGDD), que deben tratarse separadamente los datos clínico-asistenciales y los datos identificativos del paciente, salvo que se disponga del consentimiento de éste.

Partiendo de esta regla general, el propio artículo 16.3 de la Ley 41/2002 remite a la disposición adicional 17ª, apartado 2, del LOPDDDD (DA 17ª), en lo que se refiere a los criterios aplicables al tratamiento de datos de salud para fines de investigación.

Los tratamientos de datos de salud para fines de investigación, previstos en el marco normativo del Estado, pueden encontrar cobertura en diferentes excepciones (art. 9.2.g), h), i) yj) RGPD), que levantan la prohibición de tratar datos de categorías especiales, como los datos de salud, y habilitan su tratamiento (art. 9.1 RGPD).

Más en concreto, ya los efectos que interesan, según el apartado 2 de la DA 17a de la LOPDDDD:

> **"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 las datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.**
>
> **En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales ya la libre circulación de estas datos, en un sitio fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.**
>
> **Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.**

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 conservan la información que posibilite la reidentificación. 2.º Que las datos seudonimizadas 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.

Podrá procederse a la reidentificación de las datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria. (…)

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de las datos. 2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica. 3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no accedan a datos de identificación de los interesados. 4.º Designar a un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con lo previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679. (…)"

El Acuerdo prevé que el Hospital, responsable de las HHCC de los pacientes, debe sedenimizar la información de los pacientes que deba tratarse a través de la Plataforma.

Así, el apartado 2.4 del Acuerdo prevé que "La OS manifiesta y garantiza que las datos de la OS que se envíen a (la empresa) se pseudonomizarán de conformidad con el RGPD antes de transferirse (...)."

Los principios y garantías de la protección de datos son plenamente aplicables a los datos seudonimizados que son, a todos los efectos, datos personales (considerando 26 RGPD).

Según el artículo 4.5 del RGPD, hay que entender por seudonimización: "el tratamiento de datos personales de tal forma que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que las datos personales no se atribuyan a una persona física identificada o identificable;"

El RGPD configura su donimización como una garantía adecuada para la protección de datos (art. 6.4.e), 25.1, y 32.1.a) RGPD, entre otros), sin excluir del alcance de la normativa de protección de datos la información personal sedenimizada.

Esta previsión normativa que examinamos considera lícito el tratamiento de datos seudonimizados para fines de investigación en salud, siempre que se apliquen garantías adecuadas, sin que se explicite la exigencia de la prestación de consentimiento por parte de los afectados (art. 6.1. a) y 9.2.a) RGPD).

En definitiva, a los efectos que interesan, está claro que el tratamiento de datos seudonimizados para fines de investigación biomédica, puede encontrar suficiente habilitación en base a las previsiones del apartado 2.d) de la DA 17 del LOPDDDD, en relación con los artículos 9.2, apartado j) y 89.1, del RGPD.

Cuando concurran las circunstancias previstas en el apartado 2.d) de la DA 17a) de la LOPDGDD, no será imprescindible el consentimiento de los afectados para llevar a cabo el tratamiento de datos de salud seudonimizados de los pacientes del Hospital.

VII

Aplicación del principio de minimización

Según el artículo 5.1.c) del RGPD, los datos deben ser los adecuados, pertinentes y limitados a lo necesario en relación con las finalidades para las que se tratan.

El apartado 9.2 del Acuerdo, prevé tratar "toda la información relativa al estado de salud de las personas físicas (incluyendo información demográfica, de diagnosis, sobre procedimientos, de laboratorio, genética, relativa a medicaciones...)" .

Según Adenda, también se puede tratar la "información sobre los profesionales sanitarios relativos a la asistencia o el tratamiento proporcionados o en relación con los pacientes (por ejemplo, intervenciones médicas efectuadas, relación del médico con un paciente...)' Se debería aclarar si esta información se trata igualmente sudonimizada. Pero incluso si así fuera, no está claro que pueda ser información relevante o pertinente a efectos de investigación médica, incluir información sobre la relación del médico con el paciente o, sencillamente, información personal de los profesionales que tratan al paciente. Convendría revisar esta previsión.

En cualquier caso, parece deducirse que toda la información de salud y genética de los pacientes, es decir, el contenido íntegro de los datos de salud y genéticos de las HHCC podrían quedar afectados por el Acuerdo.

El principio de minimización debe estar presente en la valoración previa del Hospital a la hora de concretar qué categorías de datos de salud y genéticas se considera necesario seudonimizar y compartir. Valoración que debe responder a un análisis previo desde la perspectiva del principio de minimización, y que no parece que deba incluir

necesariamente la totalidad de las HHCC, para cualquier estudio de investigación que se quiera realizar. Antes de llevar a cabo cualquier tratamiento, es necesario determinar la información relevante a los efectos de la investigación.

En cualquier caso, es necesario valorar positivamente a previsión expresa del apartado 9.4 del Acuerdo, en el sentido de que el Hospital determina qué datos de pacientes seudonimizados se proporcionan a la empresa y los métodos con los que se efectúa al tratamiento previo (entemos que se refiere a la sudonimización) a la comunicación de los datos.

Esta previsión general es adecuada si se interpreta en el sentido apuntado, de valorar previamente qué datos de salud y genéticos puede ser oportuno pseudonimizar de cara a los estudios concretos de investigación que se podrían llevar a cabo.

VIII

Ejercicio de derechos

En cuanto al ejercicio de derechos por parte de los interesados respecto al tratamiento de los datos seudonimizados (arts. 15 y ss. RGPD), el apartado 9.6.1 de la Adenda prevé que, la empresa debe remitir todas las solicitudes que se puedan plantear en el Hospital, para que éste pueda responderlas.

El apartado 9.6.2 de la Adenda prevé que el Hospital "mantiene la responsabilidad de responder a las solicitudes de los interesados, ya que los datos se le proporcionan a (la empresa) en forma sededonimizada y (la empresa) por tanto no puede responder a estas solicitudes.", y el apartado 3.4 de la Adenda prevé que la empresa notificará inmediatamente al Hospital y cooperará si se presenta una queja o solicitud respecto al ejercicio de derechos del interesado en virtud del RGPD. El apartado 6.1.3 de la Adenda concreta los derechos de los afectados, en consonancia con las previsiones del RGPD.

Se valora positivamente la concreción, tanto de los derechos previstos en el RGPD para los afectados, como la previsión según la cual la empresa comunicará estas solicitudes al Hospital, respecto a la información sededonimizada.

Ahora bien, convendría incluir una previsión respecto a la posibilidad de que los usuarios del Hospital (cuyos datos no se pseudonimizan), que utilizan la plataforma, ejerzan los derechos previstos en el RGPD, no sólo ante el propio Hospital (que puede atenderlas y resolver como responsable del tratamiento de datos de sus trabajadores), sino también para el caso de que la solicitud se plantee ante la empresa, posibilidad que no podemos descartar.

Conviene pues prever cómo se vehicularán estas solicitudes de derechos de los usuarios de la plataforma.

IX

Transferencias internacionales de datos (TID)

Según la cláusula 6 de la Adenda, las partes (Hospital y Empresa) se someten a las "Cláusulas Contractuales Tipo", aprobadas por la Comisión Europea para la transferencia de datos personales entre los responsables y encargados del tratamiento y entre responsables del tratamiento que se recogen en los anexos I y II de la Adenda.

En cuanto a las previsiones sobre transferencias internacionales de datos (TID), del artículo 44 del RGPD, el RGPD establece, de entrada, que "podrá realizarse una transferencia de

datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado", supuestos en que la TID "no requerirá ninguna autorización específica" (artículo 45.1).

Según la información disponible, la empresa encargada del tratamiento, la empresa, con sede en Estados Unidos, está incluida como entidad adherida al Privacy Shield. En el enlace https://www.privacyshield.gov/list se puede consultar un listado con las entidades adheridas a Privacy shield. Según el apartado 1.5 del Acuerdo, la empresa filial actúa como representante en la Unión Europea de la empresa.

Por aplicación del artículo 46.2 del RGPD, vista la información disponible, se puede considerar que la adopción de las cláusulas contractuales tipo de la Comisión Europea en relación con el contrato de encargo que nos ocupa, permite ofrecer garantías adecuadas para tratamiento de los datos.

El Anexo 1 de la Adenda recoge, entre otros aspectos, las definiciones que se encuentran en el artículo 3 de la Decisión de la Comisión (cláusula 1 del Anexo 1), así como las obligaciones del exportador , es decir, el responsable (cláusula 4 del Anexo 1) y del importador, es decir, el encargado (cláusula 5 del Anexo 1), tal y como prevé la Decisión de la Comisión.

Convendría, en cualquier caso, aclarar las siguientes cuestiones:

Notemos que, según la cláusula 5.c) del Anexo 1 (obligaciones del encargado), se prevé que el encargado garantiza que ha implementado las medidas técnicas y organizativas "especificadas en el Apéndice 2 antes de tratar las datos personales transferidos". Ahora bien, el Apéndice 2, hace una mención de nuevo general y poco precisa a las medidas de seguridad tomadas, en los siguientes términos: "El importador de los datos mantendrá las salvaguardias administrativas, físicas, y técnicas para proteger la seguridad, confidencialidad e integridad de los datos personales, como se describe en el "Healthcare Organization Network Agreement." Dado que se desconoce el contenido de este Agreement no puede contrastarse si su contenido se ajusta a lo que exigen las cláusulas contractuales tipo. Convendría, pues, revisar esta cuestión.

Según el Apéndice 1 de la Adenda (correspondiente a dichas cláusulas contractuales tipo a las que las partes someten el encargo del tratamiento), en el apartado "fecha subjects", se indican las siguientes categorías de afectados, las datos de los que podrían ser objeto de comunicación al encargado: "prospects, customers, sufrientes, website visitores, bussiness partners and vendors of data exportar. Empleees or contact persons of data exporters (...)."

Teniendo en cuenta que el Apéndice 1 se refiere al contrato de encargo del tratamiento que firmaría el Hospital con la empresa para realizar el tratamiento de datos de los usuarios del Hospital que utilizarían la Plataforma, la descripción de las categorías de afectados resulta excesiva.

Sobre todo, por la referencia que se hace a los datos de pacientes, que no deben ser objeto, por la información consultada, de dicho encargo del tratamiento (que sólo afecta a datos de los usuarios que utilizan la Plataforma desde el Hospital). Conviene revisar este apartado que, en principio, dada la información disponible, sólo debe referirse a los trabajadores del Hospital que deban ser usuarios de la Plataforma.

X

Medidas de seguridad de la información

El tratamiento de los riesgos asociados a la seguridad de los datos debe basarse en un análisis del riesgo asociado a la pérdida de la confidencialidad, la integridad y la disponibilidad de los datos. Las metodologías de análisis de riesgos estándar (por ejemplo, ISO) pueden resultar convenientes a efectos del tratamiento previsto.

Más allá de ello, el responsable del tratamiento (o los corresponsables, en este caso, ej. art. 26 RGPD), debe articular las medidas técnicas y organizativas que resulten necesarias para asegurar la licitud del tratamiento de las datos de salud, en los términos que exige el artículo 9.2.j) y 89.1 del RGPD, teniendo en cuenta el considerante 53 del RGPD, según el cual: "(...). El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y las datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la s Sin embargo, esto no debe suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de estas datos."

Así, incluso en caso de que el tratamiento se enmarque en el supuesto del artículo 2.d) de la DA 17a) del LOPDDDD, la compatibilidad prevista en el artículo 89 del RGPD no actúa de forma automática sino que está sometida a la adopción por parte de los responsables del tratamiento de las garantías adecuadas para garantizar la protección de los datos pe

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

La Adenda incluye referencias genéricas a la adopción de medidas de seguridad, como en el apartado 2.e) de las disposiciones generales ("adoptar medidas técnicas y organizativas adecuadas contra todo tratamiento no autorizado o ilícito y evaluar periódicamente la idoneidad de dichas medidas de seguridad, modificándolas cuando sea necesario (.

Esta previsión, junto con otras del mismo apartado 2 del Acuerdo, pueden ser pertinentes desde la perspectiva de la protección de datos. Más en concreto, el apartado 3 de la Adenda referido a las "Medidas de seguridad", prevé que: La empresa "cuenta con la certificación ISO 2700:2013 y la mantendrá durante el plazo de vigencia del Acuerdo y 'Addenda sobre el tratamiento (...)". Este mismo apartado contempla, entre otros, que la empresa garantiza el control del acceso únicamente de personal autorizado a la información, el uso de controles de entrada físicos y lógicos adecuados, medidas que pueden ser adecuadas en el caso que nos ocupa. También cabe destacar la previsión de medidas técnicas específicas durante la instalación y mantenimiento del servidor de la empresa en las dependencias del Hospital, donde se ubicarán físicamente (apartado

En el apartado 3.2 de la Adenda, explicita que la empresa tiene la certificación ISO 2700:2013, y que "mantendrá esta certificación durante la totalidad del plazo de vigencia del Acuerdo". Se añade que, en caso de petición, la empresa facilitará al Hospital la documentación que demuestre esta certificación. Al respecto, dado que corresponde al responsable velar por el cumplimiento de la normativa de protección de datos en materia de seguridad, por parte del encargado del tratamiento, el Hospital debería llevar a cabo las verificaciones necesarias no sólo sobre la disponibilidad y vigencia de esta certificación, sino para velar la adecuación y suficiencia de la misma dados los riesgos inherentes tanto a la naturaleza de los datos tratados, el volumen de información tratada, las consecue

a las personas afectadas un tratamiento inadecuado o las demás circunstancias del tratamiento.

Añadimos que, aparte del tratamiento de datos seudonimizados de las HHCC, el uso de la Plataforma también comporta el tratamiento de datos identificativos de los usuarios de la Plataforma (en el marco del encargo del tratamiento entre el Hospital y la empresa). También convendría explicitar con más claridad las medidas técnicas y organizativas tendentes a proteger esta información.

- Hay que evitar el riesgo de reidentificación

La licitud para la utilización de datos seudonimizados con fines de investigación pasa necesariamente por el cumplimiento de las medidas establecidas por el RGPD (artículo 9.2.j), en conexión con el artículo 89.1 del RGPD).

Si bien el RGPD considera la utilización de su donimización como una medida de seguridad que puede suponer una garantía adecuada para el tratamiento de la información personal (entre otros, considerantes 28 y 156, y arts. 6.4.e) y 25.1 RGPD), es necesario poner de manifiesto, en línea con lo que expone el Grupo de Trabajo del Artículo 29 (GT 29) en el Dictamen 5/2014, sobre técnicas de anonimización, que el riesgo de reidentificación es inherente a cualquier técnica de anonimización, por lo que la intimidad y la protección de los datos del titular (en este caso, especialmente, de los pacientes del Hospital), podría verse comprometida, en caso de que se produzca una reversión no autorizada de su donimización (considerantes 75 y 85 RGPD).

Ante cada petición que pueda producirse de datos seudonimizados, corresponderá al responsable del tratamiento analizar previamente a la comunicación qué medidas conviene articular para minimizar el riesgo de reidentificación de la información personal. Así, en caso de que exista un riesgo de reidentificación habrá que denegar la solicitud o de otro modo introducir las garantías suficientes para hacer desaparecer este riesgo.

La especial naturaleza de la información tratada exige un análisis previo y una concreción por parte del Hospital en la elección de los mecanismos de seudonimización, como recuerda el dictamen del GT 29, citado, y esta Autoridad en diferentes ocasiones (Dictámenes CNS 34/2014 y CNS 20/2015). Dado que la finalidad de la utilización por parte del Hospital de la Plataforma consiste en el tratamiento de datos seudonimizados para fines de investigación (DA 17a, apartado 2.d) LOPDGDD), el responsable del tratamiento (en este caso, los corresponsables), deben articular las medidas técnicas y organizativas necesarias para garantizar, entre otros, el respeto al principio de minimización de los datos personales y para evitar el riesgo de reidentificación de la información en los términos previstos en el RGPD, dada la remisión al derecho de los Estados, a la DA 17a, apartado 2 d) f) yg) de la LOPDDDD, cuestiones que no quedan suficientemente concretadas en la documentación disponible.

De acuerdo con las consideraciones hechas en este dictamen se hacen las siguientes,

Conclusiones

El tratamiento de datos de salud de los pacientes del Hospital para fines de investigación médica por parte del Hospital, a través de la utilización de la Plataforma, puede encontrar suficiente habilitación en el artículo 5.1.b) RGPD y la Disposición adicional 17ª LOPDGDD, en conexión con los artículos 9.2, apartado j) y 89.1 RGPD, siempre que se apliquen las garantías adecuadas que exige la normativa.

Resulta confusa la utilización de dos documentos y una adenda en la que se tratan de forma a menudo mezclada aspectos relativos a datos que se tratarían en régimen de corresponsabilidad, con otros aspectos relativos a datos que se tratarían en el marco de un encargo del tratamiento. Convendría diferenciarlo claramente.

En concreto, habría que revisar las siguientes cuestiones, en los términos concretados en éste Dictamen:

- Convendría concretar mejor los flujos de información previstos, en especial en lo que se refiere a las "funciones avanzadas" a que se refiere el punto 2.2 del Acuerdo.

- Convendría definir mejor las responsabilidades de las partes intervinientes y, en su caso, revisar la utilización del régimen de corresponsabilidad.

En cuanto al encargo del tratamiento entre el Hospital y la empresa, y, en su caso, el acuerdo de corresponsabilidad (ej. art. 26 RGPD), convendría sistematizar su contenido, de forma que se agrupen de forma más clara las distintas obligaciones del Hospital y la empresa, en uno y otro caso. Es necesario que el encargo del tratamiento incorpore todos los apartados del artículo 28.3 del RGPD, de forma clara y precisa.

- Es necesario realizar una evaluación de impacto en los términos previstos en el artículo 35 del RGPD, antes del inicio del tratamiento.

- Los responsables o responsables deben establecer qué medidas técnicas concretas se utilizarán para evitar o, al menos, minimizar el riesgo de reidentificación de los pacientes por la empresa o por parte de terceros (hospitales, centros de investigación, etc), participantes en la Red, tanto en los casos en que se facilite información agregada, como en el caso de que, eventualmente, en uso de las "funciones avanzadas" se entregara información seudonimizada.

- Conviene prever el mecanismo para atender los derechos (arts. 15 y ss. RGPD) que puedan ejercer los usuarios de la Plataforma, si éstos se dirigen a la empresa.

Barcelona, 31 de marzo de 2020