Ref. CNS 3/2020

Dictamen en relació amb la consulta d'un centre sanitari sobre la legalitat d'una Plataforma de gestió d'assajos clínics

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'un centre sanitari (en endavant, l'Hospital) sobre la legalitat, conforme a la normativa de protecció de dades, d'una Plataforma de gestió d'assajos clínics (en endavant, la Plataforma).

La consulta s'acompanya de còpia del document *"Acuerdo de red de organizaciones sanitarias"* que, per la informació aportada, signaria l'Hospital amb l'empresa responsable de la Plataforma, i de còpia del document "*Addenda sobre el tratamiento de datos*", que complementa el document anterior. Així mateix, la consulta s'acompanya d'informació sobre la Plataforma (...).

Analitzada la petició i la documentació adjunta, vista la normativa vigent aplicable, i l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

La consulta explica que la Plataforma és una iniciativa privada que sorgeix d'un projecte finançat per fons públics i privats sota la convocatòria europea IMI (*Innovative Medicines Initiative*) per impulsar el disseny i execució d'assajos clínics basat en l'obtenció de dades agregades de la història clínica electrònica, aplicable a qualsevol centre que utilitzi aquest format electrònic, com és, segons explica la consulta, el cas de l'Hospital. Segons la consulta, la plataforma té per objectiu *"construir una xarxa paneuropea/global de centres que volen maximitzar la seva participació en la investigació clínica amb la indústria i el món acadèmic."*

Segons la consulta, la Plataforma, de l'empresa (...), és una eina que permet identificar, de manera automàtica i en base a les dades de la història clínica electrònica, els pacients que compleixen determinats criteris, coincidents amb els d'un assaig clínic determinat. La consulta explica que si els criteris coincideixen o interessen als tercers, "*l'Hospital rebrà una alerta i contactaria amb els pacients, oferint la possibilitat de participació en l'estudi o assaig clínic."*

El document que s'acompanya a la consulta, explica que la Plataforma és la major xarxa europea per a la reutilització de dades d'històries clíniques electròniques per a recerca mèdica. Segons aquesta informació, entre els serveis que la Plataforma ofereix als hospitals es troba el reclutament de pacients per a poder fer recerca clínica.

La consulta afegeix que el programari estaria instal·lat en el servidor de l'Hospital, i que es signarà el preceptiu contracte d'encarregat del tractament. En relació amb aquest contracte i amb el tractament de dades objecte de consulta, s'adjunta a la consulta còpia del document "ACUERDO DE RED DE ORGANIZACIONES SANITARIAS" (en endavant, l'Acord) i del document "ADENDA SOBRE TRATAMIENTO DE DATOS" (en endavant, l'Addenda), així com altra informació complementària sobre la Plataforma.

Situada la consulta en aquests termes, segons el Reglament (UE) 2016/679, del Parlament i del Consell Europeu, de 27 d'abril de 2016, General de Protecció de Dades

(en endavant, RGPD), són dades personals: *"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 tractament de dades (art. 4.2 RGPD) de les persones físiques, ja sigui dels pacients o dels professionals de l'Hospital que seran usuaris de la Plataforma, es troba sotmès als principis i garanties de la normativa de protecció de dades personals (RGPD, així com la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD)).

III

S'ha de dir que malgrat l'amplitud de la documentació aportada en fer la consulta, els documents resulten poc concrets, i a vegades fins i tot contradictoris, tant pel que fa a la sistemàtica emprada, com pel que fa a la definició dels tractaments que es pretenen dur a terme, la definició dels papers que jugaran cadascun dels agents implicats i de les seves responsabilitats. En aquest sentit resulta especialment confusa la utilització de dos documents i una addenda on es tracten de manera sovint barrejada aspectes relatius a dades que es tractarien en règim de corresponsabilitat, amb altres aspectes relatius a dades que es tractarien en el marc d'un encàrrec del tractament. Convindria diferenciar-ho clarament.

En qualsevol cas, aquesta manca de claredat impedeix fer un pronunciament precís sobre aquestes qüestions.

No obstant això, vist el contingut de la documentació aportada, referida a la participació de l'Hospital en la Plataforma, des de la perspectiva de la protecció de dades convé analitzar diferents aspectes, en concret:

1. Descripció del tractament de dades personals
2. Necessitat de realitzar una Avaluació d'Impacte en la Protecció de Dades
3. Esquema d'atribució de responsabilitats
4. Legitimació del tractament
5. Aplicació del principi de minimització
6. Exercici de drets
7. Transferències internacionals de dades (TID)
8. Mesures de seguretat

Descripció del tractament de dades personals

a) Tractament de dades dels pacients:

En síntesi, segons el document "*Acuerdo de Red de organizaciones sanitarias*", l'empresa (...) és propietària d'una plataforma informàtica basada en el núvol per facilitar la investigació, en concret, per *"permetre als usuaris analitzar poblacions agregades de pacients d'organitzacions sanitàries participants i altres fonts de dades"*.

Segons l'Acord, l'organització sanitària (OS) -que seria, en el cas que ens ocupa, l'Hospital que formula la consulta-, accediria a la Plataforma a través d'una llicència que li proporcionaria l'empresa, que inclou l'accés a la Xarxa de Recerca Global de

l'empresa. L'apartat 1.16 de l'acord defineix la Xarxa com *"la plataforma informàtica ... basada en el núvol per facilitar la recerca, com per exemple, però no limitat, a permetre als usuaris analitzar poblacions agregades de pacients de les organitzacions sanitàries."*

La utilització d'expressions com ara "*com per exemple, però no limitat*" impedeix conèixer amb exactitud en què consistirà el tractament de les dades dels pacients duts a terme per la plataforma.

Hi ha altres exemples de qüestions que no estan prou ben definides. Així, per exemple, segons el punt 2.1 de l'Acord, l'Hospital *"posseeix i reté el dret de controlar la transferència i l'ús de les dades de l'OS en relació amb la Xarxa de Recerca Global de l'empresa. Les* ***dades personals relatives a pacients de l'OS es conserven en l'entorn de l'OS*** *i no es transfereixen fora de l'entorn de l'OS, tret del que disposa la Secció 2.2* (de l'Acord)."

Caldria concretar la referència a "*l'entorn de l'OS*" (que tampoc apareix definit de manera clara en la definició que en dona l'apartat 1.5 de l'Acord), atès que no està clar a que s'està referint (els servidors de l'OS, el tractament sota la seva responsabilitat amb la col·laboració de l'encarregat del tractament ...).

També hi ha certes confusions o contradiccions en el tractament que pot fer l'empresa de la informació seudonimitzada. Segons el punt 2.4 de l'Acord: *"L'OS manifesta i garanteix que* ***les dades de l'OS que s'enviïn a l'empresa es seudonimitzaran*** *de conformitat amb l'RGPD i totes les lleis de privacitat* ***abans de transferir-se a*** **(l'empresa)**. *Sens perjudici d'això, cadascuna de les Parts durà a terme totes les activitats descrites en l'Acord i protegirà la privacitat i la seguretat de totes les dades personals de conformitat amb l'RGPD."*

Semblaria, a partir d'això i del que s'explica en el text de la consulta que l'OS lliurarà informació de salut dels seus pacients, prèviament pseudonimitzada a l'empresa.

Es valora positivament el tractament seudonimitzat de dades dels pacients, de què disposa l'Hospital per a finalitats de recerca mèdica sens perjudici del que es dirà més endavant.

Segons s'explica en el text de la consulta (tot i que en els documents adjunts no s'explica amb la mateixa claredat), sembla que si més no en un primer moment, la funció de l'empresa consisteix en identificar els pacients coincidents amb el perfil de pacient sobre els quals es vol dur a terme un estudi determinat.

En aquesta fase, els resultats que es podrien lliurar a tercers ("tercers i promotors" en els termes que s'expressa la consulta) serien resultats anònims. En aquest sentit, el punt 1.9 de l'Acord, fa referència als *"resultats anònims de les consultes en les xarxes de dades de* (l'empresa), *com per exemple recomptes dels pacients, mètriques de prevalença, taxes d'incidència i altres dades estadístiques agregades, que es proporcionen als usuaris de la plataforma.".* Sembla que aquesta referència s'ha d'entendre feta a resultats agregats de les consultes que no es poden vincular de cap manera amb persones concretes. Només en aquest cas resultaria adequat referir-se a informació anònima.

Cal recordar que només és pot considerar com anònima la informació que es desvincula de manera irreversible del pacient, cosa que no succeeix, precisament, amb la informació seudonimitzada. La distinció és rellevant des de la perspectiva de la protecció de dades, ja que la informació seudonimitzada és a tots els efectes informació personal protegida per l'RGPD, mentre que la informació anònima perd aquesta condició (considerant 26 RGPD).

En aquest punt, cal fer un incís, perquè en alguns punts dels documents aportats sembla que no es té en compte aquesta distinció. Així, per exemple, segons el punt 2.1 de l'Acord, s'afirma que *les **dades personals relatives a pacients de l'OS es conserven en l'entorn de l'OS** i no es transfereixen fora de l'entorn de l'OS, tret del que disposa la Secció 2.2* (de l'Acord)." . Quan en realitat pel que s'exposa en els mateixos documents les dades seudonimitzades dels pacients passen als servidors de l'empresa.

A partir d'aquesta informació seudonimitzada, i si els criteris coincideixen amb l'interès del tercer o promotor, a la consulta s'indica que el centre contactaria amb els pacients oferint la possibilitat de participar en l'estudi.

No es troba suficientment concretat en la documentació disponible, quina tipologia de tercers destinataris podrien sol·licitar i rebre informació seudonimitzada de les HC de l'Hospital, l'abast geogràfic que podrien tenir aquests tercers, si es limita a l'àmbit europeu (entitats que, en principi, podrien estar sotmeses com l'Hospital a les previsions de l'RGPD), o si els destinataris podrien ser hospitals o centres de recerca d'altres països. En qualsevol cas, en la mesura que es tracti d'informació anonimitzada no estaria subjecte a les previsions de l'RGPD.

Cal tenir en compte que hi ha diferents modalitats d'investigació que preveu la Llei 14/2007, de 3 de juliol, d'investigació biomèdica (LIB), però també altres tipus d'investigació que queden exclosos de l'àmbit d'aplicació de la LIB, com ara els estudis observacionals (art. 58.2 de la Llei de garanties i ús racional dels medicaments i productes sanitaris de 2015 (Reial decret legislatiu 1/2015, de 24 de juliol)), els assajos clínics, als quals no s'aplica la LIB, i que com fa avinent el considerant 161 de l'RGPD, estan regulats per la seva normativa específica (Reglament UE 536/2014, de 16 d'abril, sobre els assajos clínics de medicaments d'ús humà), o els estudis epidemiològics (previstos a la legislació d'autonomia del pacient (art. 16.3 Llei 41/2002 i art. 11.3 Llei 21/2000).

Tenint en compte que les tipologies de recerca mèdica són molt variades, en funció del tipus d'estudi que es vulgui dur a terme pot ser necessari identificar els pacients, o no.

Així, en el cas dels assajos clínics, atesa la normativa reguladora, sí seria necessari que el responsable o promotor de l'assaig contacti amb els pacients que s'hagi comprovat, a partir del cribatge inicial d'informació seudonimitzada que permet la Plataforma, que poden ser participants potencials en l'assaig. En aquest cas, òbviament sí pot resultar necessari que l'Hospital contacti amb aquests pacients, per tal d'oferir-los la possibilitat de participar. Ara bé, en altres casos, pot ser que un centre de recerca pugui dur a terme un estudi amb dades seudonimitzades (apartat d) de la DA 17ª de l'LOPDGDD) sense que sigui estrictament necessari contactar amb els pacients. Però no sembla que sigui aquest el cas exposat en la consulta, atès que es limita a indicar que "*les dades accessibles per tercers serien anonimitzades*".

En aquest sentit, s'observa també una contradicció amb l'apartat 2.3 de l'Acord, en el qual s'atorga a l'empresa el dret "a "*acceder a, utilitzar, alojar, copiar, traduir, distribuir y formatear los datos de la OS*". La utilització del terme "distribuir", sembla contradictori amb l'objecte definit a la consulta i amb el contingut de la clàusula 2.2 de l'Acord.

S'ha de fer notar en aquest punt que l'exposició de la consulta incorre en una contradicció, perquè mentre per una banda indica que "*les dades accessibles per tercers serien anonimitzades"* a continuació s'indica que "(els tercers no podrien saber a qui corresponen)" . I ambdues expressions no són equivalents. La primera expressió fa referència a dades anònimes. La segona podria fer referència també a dades seudonimitzades. En qualsevol cas, atès que en el texts dels documents adjunts no es

preveu que l'empresa faciliti a tercers conjunts de dades seudonimitzades, caldrà entendre que es refereix només a dades anònimes.

El reclutament de participants per a un assaig clínic a partir de la participació en la Plataforma podria resultar habilitat sempre que sigui l'Hospital, com a responsable de l'HC, qui reidentifiqui al pacient.

Malgrat el que s'exposa a la consulta, no és menys cert que els apartats 2.1 i 2.2 de l'Acord obren la porta, dins el que s'anomenen com funcions avançades de la plataforma, a què es puguin transferir dades de pacients a tercers. En aquest cas aquesta comunicació de dades estaria sotmesa a l'RGPD. En qualsevol cas, en aquest dictamen no s'analitzarà aquesta qüestió, tota vegada que la consulta només fa referència de passada a aquesta qüestió, sense fer-ne una exposició precisa i que aquests apartats reserven el control i la decisió d'aquestes transferències a l'OS i recullen expressament que caldrà aplicar els principis de la protecció de dades personals.

- **Tractament de dades dels usuaris:**

Es preveu utilitzar dades identificatives dels professionals de l'Hospital usuaris de la Plataforma. El tractament d'aquestes dades serà objecte, segons la informació disponible (punt 1.6 de l'acord), d'un encàrrec del tractament (art. 28 RGPD).

En principi aquestes dades sembla que no serien seudonimitzades, tot i que l'apartat 2 de l'addenda, dedicat a les disposicions generals (per tant aplicable també a les dades dels usuaris) preveu entre les obligacions de l'OS "*proporcionar solo datos seudonimizados al servidor de* (l'empresa)" (apartat b)).

Òbviament, aquestes dades són dades personals sotmeses als principis i garanties de l'RGPD.

Segons l'apartat 1.1 de l'Addenda, l'empresa *"actua com a encarregat del tractament sota el control de l'Hospital respecte el tractament de dades personals dels usuaris de l'Hospital dels productes i dels serveis prestats en virtut de l'Acord. Aquestes dades personals consisteixen en la* ***informació típica*** *utilitzada per a implementar el control d'accés (...).*

Segons l'apartat 8.2 de l'Addenda, l'empresa *"****només processarà les dades personals dels usuaris de l'hospital necessaris per a prestar els serveis*** *en virtut de l'Acord, concretament per a proporcionar als usuaris de l'Hospital l'accés als productes de* (l'empresa)", en concret: Nom complet; informació de contacte professional, incloent adreces de correu electrònic; nivell/situació professional (càrrecs); informació sobre l'ús de la plataforma; informació de registre d'auditoria, incloent l'adreça IP.

Es valora positivament aquesta concreció respecte el tractament de dades dels usuaris.

No es pot descartar que algunes d'aquestes dades puguin ser tractades, no ja pel propi encarregat (l'empresa), sinó per altres tercers. En principi, no sembla que hagi de ser necessàriament així, tot i que l'apartat 4.1 de l'addenda permetria l'accés per part del subencarregat del tractament (Amazon web services) que allotjaria la plataforma.

IV

Necessitat de realitzar una Avaluació d'Impacte en la Protecció de Dades (AIPD)

Segons disposa l'article 35 de l'RGPD:

"1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, 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 los 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 los datos personales relativos 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 ens atenim a les característiques del tractament de dades seudonimitzades objecte de consulta, que són dades de salut i genètiques (art. 9 RGPD), que el tractament es produirà previsiblement a gran escala (no només pels ens que la tractaran sinó perquè es podria tractar d'un conjunt qualitativa i quantitativament molt significatiu de dades de les HHCC), en el cas que ens ocupa resulta imprescindible dur a terme una AIPD.

En aquest sentit el Grup de Treball de l'Article 29 *("Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tracatmiento entraña un probablemente un alto riesgo a efectos del RGPD"),* ha explicitat que cal dur a terme una AIPD quan es donen, entre d'altres, aquestes característiques en el tractament: l'elaboració de perfils i prediccions en base a dades de salut, entre d'altres; tractament de categories de dades sensibles; tractament de dades a gran escala; dades relacionades amb persones vulnerables; i ús innovador de tecnologies, entre d'altres. No només això, sinó que en aquest cas cal fer novament menció que la possibilitat de reidentificació de dades personals sempre comporta un cert risc, que cal preveure i pal.liar en la mesura del possible.

Totes aquestes característiques conflueixen en el tractament que ens ocupa i per tant la realització d'una AIPD prèvia al tractament resulta imprescindible.

A més, segons l'apartat 2.f) de la DA 17a de l'LOPDGGD:

> *"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 los 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 acceden a datos de identificación de los interesados.

4.º Designar 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 el previsto en el artículo 27.1 del Reglamento (UE) 2016/679."

Els mecanismes concrets de seudonimització, així com aquells que s'estableixin per a minimitzar el risc de reidentificació indeguda dels pacients par part d'altres participants en la Plataforma, són qüestions que han d'estar definides i previstes de forma prèvia a l'inici del tractament, i que caldrà concretar a l'avaluació d'impacte en la protecció de dades (35 RGPD i art. 2.f.1 LOPDGDD).

Per tot l'exposat cal dur a terme una avaluació d'impacte en els termes previstos a l'article 35 de l'RGPD, abans de l'inici del tractament.

Ens remetem, sobre això, a la Guia *pràctica "Avaluació d'impacte relativa a la protecció de dades",* disponible al web www.apd.cat.

V

Esquema d'atribució de responsabilitats

Cal partir de la base que l'Hospital és responsable de la informació personal dels pacients continguda a la història clínica d'aquests (HC), en els termes de la Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica, i de la Llei 41/2002, de 14 de novembre, bàsica, reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica.

En la documentació aportada (Acord i Addenda) es preveu establir dues relacions diferenciades entre l'empresa propietària de la Plataforma (en endavant, l'empresa), i l'Hospital que formula la consulta (OS), en funció de la informació personal objecte de tractament. Segons l'apartat 1.1 de l'Addenda, aquesta té per objecte *"diferenciar les responsabilitats de les parts com a responsables del tractament conjunts, i com encarregat del tractament".* Aquest mateix apartat concreta el següent*:*

L'empresa *"actua com a **encarregat del tractament** sota el control de l'OS pel que fa al tractament **de dades personals dels usuaris** de l'Hospital dels productes i dels serveis prestats en virtut de l'Acord. (...).*
L'empresa *"i l'Hospital són **responsables del tractament conjunts** pel que fa al tractament de les **dades clíniques de pacients** (...)."*

En aquest sentit, l'Addenda preveu unes *"disposicions generals sobre el tractament de dades personals"* (punt 2), i unes previsions referides, d'una banda, a les responsabilitats de les parts en relació amb el tractament de dades en el que l'empresa és encarregada del tractament ("PART I" de l'Addenda (punt 8)) i, de l'altra, a les responsabilitats de

l'empresa i l'Hospital en el tractament de dades seudonimitzades dels pacients, del que ambdós són corresponsables ("PART II" de l'Addenda (punt 9)).

- **Sobre el règim de corresponsabilitat**

D'acord amb l'article 4.7 RGPD el responsable del tractament és "*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 també preveu la possibilitat d'establir una corresponsabilitat sobre el tractament, és a dir, que dos o més responsables determinin conjuntament els objectius i els mitjans del tractament (art. 4.7 i art. 26 RGPD i art. 29 LOPDGDD).

Així, segons l'article 26 de l'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."*

Quan s'estableix un model de corresponsabilitat, l'RGPD exigeix la signatura d'un acord que determini clarament les funcions i relacions respectives dels corresponsables en relació amb els interessats, els quals han de conèixer els aspectes essencials de l'acord (art. 26 RGPD). En el cas que ens ocupa, la documentació disponible preveu que l'Hospital i l'empresa seran corresponsables respecte el tractament de dades seudonimitzades dels pacients de l'Hospital. De ser així, caldria que els corresponsables establissin un acord específic (en els termes de l'art. 26 RGPD) i n'informin les persones afectades.

Ara bé, tot i que la possibilitat de responsabilitat conjunta està prevista pel mateix RGPD, **la descripció de les responsabilitats que es fa en la documentació aportada no sembla obeir precisament a aquest esquema.**

Així, en el punt 2.1 de l'Acord s'indica que " *La OS posee y retiene el derecho a controlar la transferència y el uso de los datos de la OS en relación con la Red de Investigación Global* (de l'empresa). *Los datos personales relatives a pacientes de la OS se conservan en el entorno de la OS, salvo por lo dispuesto en la Sección 2.2 siguiente*."

Per la seva banda, la Secció 2.2 preveu "*Si la OS decide a su entera discreción, activar ciertas funciones avanzadas de la Red de investigación global, es possible que fuera necesario transferir ciertos datos personales ...."*

L'apartat 3.6 de l'Acord (*"Xarxa de col·laboració"),* explica que l'Hospital pot sol·licitar a l'empresa l'habilitació perquè se li mostrin els resultats de consultes realitzades a d'altres col·laboradors de la xarxa. Aquest mateix apartat preveu que l'Hospital pot tancar l'accés a les dades a d'altres col·laboradors.

És a dir, segons la informació disponible, és l'Hospital qui pot decidir utilitzar la Plataforma per a fer recerca i gestionar la informació seudonimitzada de les HC de l'Hospital, o pot decidir compartir la informació amb d'altres *"col·laboradors"* de la *"xarxa de col·laboració privada",* que formen voluntàriament l'Hospital i altres organitzacions sanitàries que participen en la Plataforma, segons l'apartat 1.4 de l'Acord.

Això respondria més a un esquema d'encàrrec del tractament, de l'Hospital com a responsable a l'empresa com a encarregada, no només per tractar les dades dels treballadors, usuaris de la plataforma, sinó com encarregada de dur a terme el procés de detecció dels pacients susceptibles de participar en un estudi).

Els responsables del tractament més aviat sembla que serien les diferents entitats que participen a la xarxa aportant informació, com també les entitats que duguin a terme els projectes de recerca.

Cal, per tant, aclarir quin és el model triat i la capacitat de decisió de cadascun dels responsables respecte la informació personal tractada.

- **Determinació del rol com a responsable i encarregat del tractament dels diferents intervinents**

Pel que fa al tractament que dugui a terme l'empresa com a encarregada del tractament (en principi les dades dels usuaris, però com acabem d'apuntar podria afectar també a les dades seudonimitzades dels pacients), cal vetllar perquè la plataforma ofereixi garanties suficients, en els termes de l'article 28.1 de l'RGPD, segons el qual *"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 apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado."*

Si bé hi ha diferents previsions de l'article 28.3 de l'RGPD que es troben recollides al llarg de l'Addenda, hi ha altres previsions que no s'expliciten en la documentació aportada.

La PART I de l'Addenda (referida específicament al tractament de les dades dels usuaris) només constata que *"l'empresa actua com a encarregada del tractament i seguint les instruccions de l'Hospital",* concreta les dades personals dels usuaris que seran objecte de tractament, i preveu que, un cop expirat o rescindit l'Acord, l'Hospital indicarà si les dades han de ser retornades o destruïdes (en correspondència amb la previsió de l'art. 28.3.g) RGPD).

Ara bé, la documentació resulta confusa ja que hi ha d'altres previsions de l'article 28.3 de l'RGPD que estan recollides en diferents apartats de l'Addenda (concretament, en l'apartat 2 de l'Addenda, en el qual s'inclouen *"Disposicions generals sobre el tractament de dades personals"* com ara l'obligació d'abstenir-se de tractar les dades personals per altres finalitats, o el compromís general de complir les seves obligacions *"d'acord amb les instruccions documentades de l'Hospital",* que es pot deduir que es refereixen a l'encàrrec del tractament, però que també podrien referir-se al model de corresponsabilitat per al tractament de les HHCC. En qualsevol cas, vista la previsió de l'article 28.3.a) RGPD convindria referir-se també a que l'empresa ha de seguir aquestes

instruccions pel que fa a les transferències internacionals de dades, cosa que no s'explicita en aquest punt. L'obligació de confidencialitat (art. 28.3.b)) es recull a l'apartat 1.3 de l'Addenda. També la previsió de l'article 28.3.h) podem considerar que queda recollida en l'apartat 3.6 de l'Addenda.

Respecte altres apartats de l'article 28.3 que caldria explicitar en el contracte d'encàrrec, vista la informació disponible en diversos apartats de l'Addenda, destaquem el següent:

Pel que fa a l'apartat 28.3.c) RGPD (obligació de l'encarregat de prendre les mesures de seguretat necessàries ex. art. 32 RGPD), l'apartat 2 de l'Addenda recull diverses mesures en relació amb les dades que li siguin revelades per l'Hospital, de manera que es podria entendre que són mesures que s'aplicaran en el contracte d'encàrrec. De tota manera, convindria preveure-ho explícitament en el contracte d'encàrrec. Les mesures de seguretat de l'empresa concretades als apartats 3.1 i 3.2 de l'Addenda, també s'hauran d'incloure, si escau, en el contracte d'encàrrec.

Pel que fa a l'article 28.3.d), el punt 4.1 de l'Addenda explicita que l'Hospital *"reconeix i accepta"* el subencarregat (Amazon Web Services), així com el nomenament de filials de l'empresa com a subencarregats. Sobre això, l'encàrrec del tractament haurà d'explicitar que l'empresa queda obligada a informar l'Hospital de qualsevol canvi en els subencarregats (ex. art. 28.3.2 RGPD) i que els subencarregats queden obligats en els termes de l'article 28.3.4 RGPD. En qualsevol cas, el fet que en l'Addenda s'expliciti la utilització d'aquest subencarregat no eximeix el responsable del tractament de vetllar perquè aquest reuneixi les garanties necessàries d'acord amb l'RGPD per dur a terme el tractament (apartats 1, 2 i 4 de l'article 28 RGPD).

Pel que fa a la previsió de l'article 28.3.e) RGPD -ajudar al responsable en l'atenció de sol·licituds de drets-, com es concreta en el FJ VIII d'aquest dictamen, cal que el contracte d'encàrrec del tractament concreti com es vehicularan les sol·licituds d'exercici de drets que puguin plantejar-se a l'encarregat.

Per tant, **cal distingir clarament a l'Addenda les obligacions** exigides per l'article 28.3 RGPD a l'encarregat (l'empresa), en relació amb el tractament que es fa com a part de l'encàrrec del tractament, i que hauran de ser subscrites en el corresponent contracte o acord, de totes aquelles previsions que es refereixen al tractament de dades seudonimitzades que, per la informació aportada, es tracten sota un règim de corresponsabilitat. **Cal sistematitzar el contingut del contracte d'encàrrec, de manera que s'agrupin de forma més clara les diferents obligacions que, seguint les instruccions de l'Hospital responsable, ha de complir l'empresa com a encarregada**.

En relació amb els contractes d'encàrrec subscrits pot ser d'interès consultar la Guia sobre l'encarregat del tractament a l'RGPD, disponible al web de l'Autoritat http://apdcat.gencat.cat/ca/inici/.

VI

Legitimació del tractament

Segons el punt 2.3 de l'Acord, l'Hospital atorga a l'empresa el dret a *"accedir, utilitzar, allotjar, copiar, traduir, distribuir i reformatejar les dades de l'OS, així com per a crear i publicar treballs derivats d'aquestes, exclusivament amb la finalitat de proporcionar-los per al seu ús a la Plataforma. (...).* ***La llicència de dades concedida només és per a finalitats de recerca****."*

Els tractaments de dades personals han de tenir, per ser lícits, una base jurídica adequada (art. 6.1 RGPD). Entre d'altres, el tractament de dades amb finalitats de recerca pot resultar lícit si es disposa del consentiment dels afectats (art. 6.1.a) RGPD), o bé si és necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics del responsable del tractament (article 6.1.e) RGPD), o també si és necessari per a la satisfacció d'interessos legítims del responsable o d'un tercer (article 6.1.f) RGPD).

Per altra banda, l'article 5.1.b) RGPD estableix que *"el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales".*

Cal valorar positivament que, per la informació disponible, el tractament de dades que es produirà amb la utilització de la Plataforma per part de l'Hospital, **s'emmarca clarament en finalitats de recerca mèdica** (punts 2.3; 2.5; 6.3 de l'Acord; punts 9.1, 9.2 i especialment, 9.5 de l'Addenda, entre d'altres). L'apartat 1.12 de l'Acord concreta què s'entén per "recerca", als efectes del contracte o acord subscrit entre l'Hospital i l'empresa. Aquesta definició es refereix, específicament, a la recerca en l'àmbit sanitari i al tractament de dades de salut (art. 4.15 RGPD) i genètiques dels pacients (4.13 RGPD), amb finalitats de recerca mèdica.

Pel que fa al tractament de categories de dades objecte d'especial protecció, l'article 9 de l'RGPD regula la prohibició general del tractament de dades personals de diverses categories, entre d'altres, les dades relatives a la salut i les dades genètiques (apartat 1). L'apartat 2 del mateix article 9 disposa que aquesta prohibició general no serà d'aplicació quan concorri alguna de les circumstàncies que preveu aquest article, entre d'altres:

> *"(...)*
>
> *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.".*

Segons disposa l'article 89 de l'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.*
>
> *(...)."*

Com ha fet avinent aquestes Autoritat en ocasions anteriors (Dictàmens 15/2019, 18/2019, o 59/2018, entre d'altres), l'RGPD admet el tractament de dades de categories especials per a finalitats de recerca, en particular en l'àmbit sanitari, amb certa flexibilitat, com es desprèn, entre d'altres, del considerant 52 de l'RGPD.

La disposició final cinquena de l'LOPDGDD ha afegit un nou article 105 bis) a la Llei 14/1986, de 25 d'abril, general de sanitat (LGS), segons el qual: *"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 Llei 41/2002, modificada per l'LOPDGDD, preveu el tractament de dades de salut per a finalitats de recerca i parteix de la regla general (com ja establia la legislació d'autonomia del pacient, anteriorment a l'entrada en vigor de l'RGPD i l'LOPDGDD), que cal tractar separadament les dades clínicoassistencials i les dades identificatives del pacient, llevat que es disposi del consentiment d'aquest.

Partint d'aquesta regla general, el propi article 16.3 de la Llei 41/2002 remet a la disposició addicional 17a, apartat 2, de l'LOPDGDD (DA 17a), pel que fa als criteris aplicables al tractament de dades de salut per a finalitats de recerca.

Els tractaments de dades de salut per a finalitats de recerca, previstos al marc normatiu de l'Estat, poden trobar cobertura en diferents excepcions (art. 9.2.g), h), i) i j) RGPD), que aixequen la prohibició de tractar dades de categories especials, com ara les dades de salut, i n'habiliten el tractament (art. 9.1 RGPD).

Més en concret, i als efectes que interessen, segons l'apartat 2 de la DA 17a de l'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.*
>
> *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 y a la libre circulación de estos datos, en un lugar 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 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.
Podrá procederse a la reidentificación de los 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 los 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 acceden a datos de identificación de los interesados.
4.º Designar 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 el 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.
(…)"

L'Acord preveu que l'Hospital, responsable de les HHCC dels pacients, ha de seudonimitzar la informació dels pacients que s'hagi de tractar a través de la Plataforma.

Així, l'apartat 2.4 de l'Acord preveu que *"La OS manifiesta y garantiza que los datos de la OS que se envien a* (l'empresa) *se pseudonomizarán de conformidad con el RGPD antes de transferirse (...)."*

Els principis i garanties de la protecció de dades són plenament aplicables a les dades seudonimitzades que són, a tots els efectes, dades personals (considerant 26 RGPD).

Segons l'article 4.5 de l'RGPD, cal entendre per seudonimització: *"el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilitzar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;"*

L'RGPD configura la seudonimització com una garantia adequada per a la protecció de dades (art. 6.4.e), 25.1, i 32.1.a) RGPD, entre d'altres), sense excloure de l'abast de la normativa de protecció de dades la informació personal seudonimitzada.

Aquesta previsió normativa que examinem considera lícit el tractament de dades seudonimitzades per a finalitats de recerca en salut, sempre que s'apliquin garanties adequades, sense que s'expliciti l'exigència de la prestació de consentiment per part dels afectats (art. 6.1.a) i 9.2.a) RGPD).

En definitiva, als efectes que interessen, és clar que **el tractament de dades seudonimitzades per a finalitats de recerca biomèdica, pot trobar suficient habilitació en base a les previsions de l'apartat 2.d) de la DA 17 de l'LOPDGDD, en relació amb els articles 9.2, apartat j) i 89.1, de l'RGPD.**

Quan concorrin les circumstàncies previstes a l'apartat 2.d) de la DA 17a) de l'LOPDGDD, no serà imprescindible el consentiment dels afectats per a dur a terme el tractament de dades de salut seudonimitzades dels pacients de l'Hospital.

VII

Aplicació del principi de minimització

Segons l'article 5.1.c) de l'RGPD, les dades han de ser les adequades, pertinents i limitades a allò necessari en relació amb les finalitats per a les que es tracten.

L'apartat 9.2 de l'Acord, preveu tractar *"**tota la informació** relativa a l'estat de salut de les persones físiques (incloent informació demogràfica, de diagnosi, sobre procediments, de laboratori, genètica, relativa a medicacions...)".*

Segons l'Addenda, també es pot tractar la *"informació sobre els professionals sanitaris relatius a l'assistència o el tractament proporcionats o en relació amb els pacients (per exemple, intervencions mèdiques efectuades, relació del metge amb un pacient...)".* S'hauria d'aclarir si aquesta informació es tracta igualment seudonimitzada. Però fins i tot si fos així, no és clar que pugui ser informació rellevant o pertinent a efectes de recerca mèdica, incloure informació sobre la relació del metge amb el pacient o, senzillament, informació personal dels professionals que tracten el pacient. Convindria revisar aquesta previsió.

En qualsevol cas, sembla deduir-se que tota la informació de salut i genètica dels pacients, és a dir, el contingut íntegre de les dades de salut i genètiques de les HHCC, podrien quedar afectades per l'Acord.

El principi de minimització ha d'estar present en la valoració prèvia de l'Hospital a l'hora de concretar quines categories de dades de salut i genètiques es considera necessari seudonimitzar i compartir. Valoració que ha de respondre a una anàlisi prèvia des de la perspectiva del principi de minimització, i que no sembla que hagi d'incloure

necessàriament la totalitat de les HHCC, per a qualsevol estudi de recerca que es vulgui fer. Abans de dur a terme qualsevol tractament, cal determinar la informació rellevant als efectes de la recerca.

En qualsevol cas, cal valorar positivament a previsió expressa de l'apartat 9.4 de l'Acord, en el sentit que l'Hospital determina quines dades de pacients seudonimitzades es proporcionen a l'empresa i els mètodes amb els que s'efectua al tractament previ (entem que es refereix a la seudonimització) a la comunicació de les dades.

Aquesta previsió general és adequada si s'interpreta en el sentit apuntat, de valorar prèviament quines dades de salut i genètiques pot ser oportú seudonimitzar de cara als estudis concrets de recerca que es podrien dur a terme.

VIII

Exercici de drets

Pel que fa a l'exercici de drets per part dels interessats respecte el tractament de les dades seudonimitzades (arts. 15 i ss. RGPD), l'apartat 9.6.1 de l'Addenda preveu que, l'empresa ha de remetre totes les sol.licituds que es puguin plantejar a l'Hospital, per tal que aquest les pugui respondre.

L'apartat 9.6.2 de l'Addenda preveu que l'Hospital *"manté la responsabilitat de respondre les sol·licituds dels interessats, ja que les dades se li proporcionen a* (l'empresa) *en forma seudonimitzada i* (l'empresa) *per tant no pot respondre aquestes sol·licituds.",* I l'apartat 3.4 de l'Addenda preveu que l'empresa notificarà immediatament a l'Hospital i hi cooperarà si es presenta una queixa o sol·licitud respecte l'exercici de drets de l'interessat en virtut de l'RGPD. L'apartat 6.1.3 de l'Addenda concreta els drets dels afectats, en consonància amb les previsions de l'RGPD.

Es valora positivament la concreció, tant dels drets que preveu l'RGPD per als afectats, com la previsió segons la qual l'empresa comunicarà aquestes sol·licituds a l'Hospital, respecte la informació seudonimitzada.

Ara bé, convindria incloure una previsió respecte la possibilitat que els usuaris de l'Hospital (les dades dels quals no es seudonimitzen), que utilitzen la plataforma, exerceixin els drets que preveu l'RGPD, no només davant del propi Hospital (que pot atendre-les i resoldre com a responsable del tractament de dades dels seus treballadors), sinó també per al cas que la sol·licitud es plantegi davant de l'empresa, possibilitat que no podem descartar.

Convé doncs preveure com es vehicularan aquestes sol·licituds de drets dels usuaris de la plataforma.

IX

Transferències internacionals de dades (TID)

Segons la clàusula 6 de l'Addenda, les parts (Hospital i Empresa) es sotmeten a les "**Clàusules Contractuals Tipus"**, aprovades per la Comissió Europea per a la transferència de dades personals entre els responsables i encarregats del tractament i entre responsables del tractament que es recullen als annexes I i II de l'Addenda.

Pel que fa a les previsions sobre transferències internacionals de dades (TID), de l'article 44 de l'RGPD, l'RGPD estableix, d'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", supòsits en què la TID *"no requerirá ninguna autorización específica"* (article 45.1).

Segons la informació disponible, l'empresa encarregada del tractament, l'empresa, amb seu als Estats Units, està inclosa com a entitat adherida al Privacy shield. A l'enllaç https://www.privacyshield.gov/list es pot consultar un llistat amb les entitats adherides al Privacy shield. Segons l'apartat 1.5 de l'Acord, l'empresa filial, actua com a representant a la Unió Europea de l'empresa.

Per aplicació de l'article 46.2 de l'RGPD, vista la informació disponible, es pot considerar que **l'adopció de les clàusules contractuals tipus de la Comissió Europea en relació amb el contracte d'encàrrec que ens ocupa, permet oferir garanties adequades** per al tractament de les dades.

L'Annex 1 de l'Addenda recull, entre d'altres aspectes, les definicions que es troben en l'article 3 de la Decisió de la Comissió (clàusula 1 de l'Annex 1), així com les obligacions de l'exportador, és a dir, el responsable (clàusula 4 de l'Annex 1) i de l'importador , és a dir, l'encarregat (clàusula 5 de l'Annex 1), tal i com preveu la Decisió de la Comissió.

Convindria, en qualsevol cas, aclarir les següents qüestions:

Fem notar que, segons la clàusula 5.c) de l'Annex 1 (obligacions de l'encarregat), es preveu que l'encarregat garanteix que ha implementat les mesures tècniques i organitzatives *"especificades en l'Apèndix 2 abans de tractar les dades personals transferides".* Ara bé, l'Apèndix 2, fa una menció novament general i poc precisa a les mesures de seguretat preses, en els següents termes: *"L'importador de les dades mantindrà les salvaguardes administratives, físiques, i tècniques per protegir la seguretat, confidencialitat i integritat de les dades personals, com es descriu en el "Healthcare Organization Network Agreement."* Atès que es desconeix el contingut d'aquest *Agreement* no es pot contrastar si el seu contingut s'ajusta al que exigeixen les clàusules contractuals tipus. Convindria, doncs, revisar aquesta qüestió.

Segons l'Apèndix 1 de l'Addenda (corresponent a les dites clàusules contractuals tipus a les que les parts sotmeten l'encàrrec del tractament), en l'apartat "*data subjects*", s'indiquen les següents categories d'afectats, les dades dels quals podrien ser objecte de comunicació a l'encarregat: *"prospects, customers, patients, website visitors, bussiness partners and vendors of data exportar. Empleyees or contact persons of data exporters (...)."*

Tenint en compte que l'Apèndix 1 es refereix al contracte d'encàrrec del tractament que signaria l'Hospital amb l'empresa per a fer el tractament de dades dels usuaris de l'Hospital que utilitzarien la Plataforma, la descripció de les categories d'afectats resulta excessiva.

Sobretot, per la referència que es fa a les dades de pacients, que no han de ser objecte, per la informació consultada, del dit encàrrec del tractament (que només afecta a dades dels usuaris que utilitzen la Plataforma des de l'Hospital). **Convé revisar aquest apartat** que, en principi, atesa la informació disponible, només s'ha de referir als treballadors de l'Hospital que hagin de ser usuaris de la Plataforma.

X

Mesures de seguretat de la informació

El tractament dels riscos associats a la seguretat de les dades s'ha de basar en una anàlisi del risc associat a la pèrdua de la confidencialitat, la integritat i la disponibilitat de les dades. Les metodologies d'anàlisi de riscos estàndard (per exemple, ISO), poden resultar convenients als efectes del tractament previst.

Més enllà d'això, el responsable del tractament (o els corresponsables, en aquest cas, *ex. art.* 26 RGPD), ha d'articular les mesures tècniques i organitzatives que resultin necessàries per tal d'assegurar la licitud del tractament de les dades de salut, en els termes que exigeix l'article 9.2.j) i 89.1 de l'RGPD, tenint en compte el considerant 53 de l'RGPD, segons el qual: *"(...). El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los 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 salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos."*

Així, fins i tot en el cas que el tractament s'emmarqui en el supòsit de l'article 2.d) de la DA 17a) de l'LOPDGDD, la compatibilitat prevista a l'article 89 de l'RGPD no actua de manera automàtica sinó que està sotmesa a l'adopció per part dels responsables del tractament de les garanties adequades per garantir la protecció de les dades personals.

L'RGPD configura un sistema de seguretat que ja no es basa en els nivells de seguretat bàsic, mitjà i alt que es preveien al Reglament de desplegament de l'LOPD, aprovat pel Reial decret 1720/2007, de 21 de desembre (RLOPD), sinó en determinar, a partir de les característiques del tractament i d'una prèvia anàlisi dels riscos, quines mesures de seguretat són necessàries en cada cas (considerant 83 i article 32 RGPD).

L'Addenda inclou referències genèriques a l'adopció de mesures de seguretat, com en l'apartat 2.e) de les disposicions generals *("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 (...)").*

Aquesta previsió, juntament amb d'altres del mateix apartat 2 de l'Acord, poden ser pertinents des de la perspectiva de la protecció de dades. Més en concret, l'apartat 3 de l'Addenda referit a les *"Mesures de seguretat",* preveu que: L'empresa *"compta amb la certificació ISO 2700:2013 i la mantindrà durant el termini de vigència de l'Acord i l'Addenda sobre el tractament (...)".* Aquest mateix apartat preveu, entre d'altres, que l'empresa garanteix el control de l'accés únicament de personal autoritzat a la informació, l'ús de controls d'entrada físics i lògics adequats, mesures que poden ser adequades en el cas que ens ocupa. També cal destacar la previsió de mesures tècniques específiques durant la instal·lació i el manteniment del servidor de l'empresa en les dependències de l'Hospital, on s'ubicaran físicament (apartat 9.6.4 Addenda).

L'apartat 3.2 de l'Addenda, explicita que l'empresa té la certificació ISO 2700:2013, i que *"mantindrà aquesta certificació durant la totalitat del termini de vigència de l'Acord"*. S'afegeix que, en cas de petició, l'empresa facilitarà a l'Hospital la documentació que demostri aquesta certificació. Sobre això, atès que correspon al responsable vetllar pel compliment de la normativa de protecció de dades en matèria de seguretat, per part de l'encarregat del tractament, l'Hospital hauria de dur a terme les verificacions necessàries no només sobre la disponibilitat i vigència d'aquesta certificació, sinó per vetllar l'adequació i suficiència de la mateixa atesos els riscos inherents tant a la naturalesa de les dades tractades, el volum d'informació tractada, les conseqüències que pot tenir per

a les persones afectades un tractament inadequat o les altres circumstàncies del tractament.

Afegim que, a banda del tractament de dades seudonimitzades de les HHCC, l'ús de la Plataforma també comporta el tractament de dades identificatives dels usuaris de la Plataforma (en el marc de l'encàrrec del tractament entre l'Hospital i l'empresa). També convindria explicitar més clarament les mesures tècniques i organitzatives tendents a protegir aquesta informació.

- **Cal evitar el risc de reidentificació**

La licitud per a la utilització de dades seudonimitzades amb finalitats de recerca passa necessàriament pel compliment de les mesures que estableix l'RGPD (article 9.2.j), en connexió amb l'article 89.1 de l'RGPD).

Si bé l'RGPD considera la utilització de la seudonimització com una mesura de seguretat que pot suposar una garantia adequada per al tractament de la informació personal (entre d'altres, considerants 28 i 156, i arts. 6.4.e) i 25.1 RGPD), cal posar de manifest, en línia amb el que exposa el Grup de Treball de l'Article 29 (GT 29) en el Dictamen 5/2014, sobre tècniques d'anonimització, que **el risc de reidentificació és inherent a qualsevol tècnica d'anonimització,** per la qual cosa la intimitat i la protecció de les dades del titular (en aquest cas, especialment, dels pacients de l'Hospital), podria veure's compromesa, en el cas que es produeixi una reversió no autoritzada de la seudonimització (considerants 75 i 85 RGPD).

Davant de cada petició que es pugui produir de dades seudonimitzades, correspondrà al responsable del tractament analitzar prèviament a la comunicació quines mesures convé articular per minimitzar el risc de reidentificació de la informació personal. Així, en cas que existeixi un risc de reidentificació caldrà denegar la sol·licitud o altrament introduir les garanties suficients per fer desaparèixer aquest risc.

L'especial naturalesa de la informació tractada exigeix una anàlisi prèvia i una concreció per part de l'Hospital en la tria dels mecanismes de seudonimització, com ha fet avinent el dictamen del GT 29, citat, i aquesta Autoritat en diferents ocasions (Dictàmens CNS 34/2014 i CNS 20/2015). Atès que la finalitat de la utilització per part de l'Hospital de la Plataforma consisteix en el tractament de dades seudonimitzades per a finalitats de recerca (DA 17a, apartat 2.d) LOPDGDD), el responsable del tractament (en aquest cas, els corresponsables), han d'articular les mesures tècniques i organitzatives necessàries per garantir, entre d'altres, el respecte al principi de minimització de les dades personals i per evitar el risc de reidentificació de la informació en els termes previstos a l'RGPD, atesa la remissió al dret dels Estats, a la DA 17a, apartat 2 d) f) i g) de l'LOPDGDD, qüestions que no queden suficientment concretades en la documentació disponible.

D'acord amb les consideracions fetes en aquest dictamen es fan les següents,

Conclusions

El tractament de dades de salut dels pacients de l'Hospital per a finalitats de recerca mèdica per part de l'Hospital, a través de la utilització de la Plataforma, pot trobar suficient habilitació en l'article 5.1.b) RGPD i la Disposició addicional 17ª LOPDGDD, en connexió amb els articles 9.2, apartat j) i 89.1 RGPD, sempre que s'apliquin les garanties adequades que exigeix la normativa.

Resulta confusa la utilització de dos documents i una addenda on es tracten de manera sovint barrejada aspectes relatius a dades que es tractarien en règim de corresponsabilitat, amb altres aspectes relatius a dades que es tractarien en el marc d'un encàrrec del tractament. Convindria diferenciar-ho clarament.

En concret, caldria revisar les següents qüestions, en els termes concretats en aquest Dictamen:

- Convindria concretar millor els fluxos d'informació previstos, en especial pel que fa a les "funcions avançades" a que es refereix el punt 2.2 de l'Acord.

- Convindria definir millor les responsabilitats de les parts intervinents i, si escau, revisar la utilització del règim de corresponsabilitat.

Pel que fa a l'encàrrec del tractament entre l'Hospital i l'empresa, i, si escau, l'acord de corresponsabilitat (ex. art. 26 RGPD), convindria sistematitzar el seu contingut, de manera que s'agrupin de forma més clara les diferents obligacions de l'Hospital i l'empresa, en un i altre cas. Cal que l'encàrrec del tractament incorpori tots els apartats de l'article 28.3 de l'RGPD, de manera clara i precisa.

- Cal fer una avaluació d'impacte en els termes previstos a l'article 35 de l'RGPD, abans de l'inici del tractament.

- Els responsable o responsables han d'establir quines mesures tècniques concretes s'utilitzaran per evitar o, al menys, minimitzar el risc de reidentificació dels pacients per l'empresa o per part de tercers (hospitals, centres de recerca, etc), participants en la Xarxa, tant ens els casos que es faciliti informació agregada, com en el cas que, eventualment, en ús de les "funcions avançades" es lliurés informació seudonimitzada.

- Convé preveure el mecanisme per atendre els drets (arts. 15 i ss. RGPD) que puguin exercir els usuaris de la Plataforma, si aquests s'adrecen a l'empresa.

Barcelona, 31 de març de 2020