CNS 29/2015

Dictamen en relació amb la consulta plantejada sobre la seguretat en la protecció de dades d'un projecte sobre salut mental per a l'anàlisi i explotació de les dades de la història clínica electrònica

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'un Grup format per diverses entitats de l'àmbit de la salut (en endavant, el Grup), per tal de demanar informe a l'Autoritat sobre la seguretat en la protecció de dades d'una activitat que el Grup vol desenvolupar, basada en l'anàlisi de les dades de la història clínica electrònica (en endavant, HCE).

(...).

Segons s'exposa en els antecedents del Projecte (Annex 1), el Grup és el proveïdor de l'atenció pública a la salut mental en una província, de manera que es disposa de les dades de salut mental de tota la població atesa a qualsevol punt de la xarxa pública, cosa que permet plantejar, segons la consulta, un registre de base poblacional.

El projecte sobre salut mental (en endavant, el Projecte) consisteix en crear una plataforma tecnològica, consistent en un conjunt de recursos humans, recursos informàtics, i una base de dades relacional derivada de l'activitat assistencial del Grup.

La consulta explica que l'objectiu general del Projecte és fer possible que les dades referides a la salut mental de la població del territori afectat puguin ser utilitzades per generar coneixement. S'afegeix que el Projecte està circumscrit a l'activitat i a l'entorn físic del Grup i que l'equip de professionals que hi treballarà estarà format per professionals de les àrees d'informàtica, mèdica, de recerca i d'innovació del Grup.

La consulta s'acompanya de còpia dels següents documents:

- Annex 1. Presentació del projecte
- Annex 2. Esquema de les entitats del Grup
- Annex 3. Acord per a la protecció de dades de caràcter personal en les comunicacions i accessos de dades entre les empreses del Grup
- Annex 4. Reglament de la Comissió de protecció de dades
- Annex 5. Informe d'auditoria
- Annex 6. Documents de seguretat de diversos fitxers de dades
- Annex 7. Document de seguretat del Fitxer d'Investigació
- Annex 8. Manual de bones pràctiques dels empleats respecte la protecció i seguretat de les dades de caràcter personal
- Annex 9. Formulari de cessió de dades

Analitzada la consulta, la documentació que l'acompanya i la normativa aplicable, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

Descripció del projecte

La consulta plantejada pel GRUP es refereix a una nova activitat que es vol desenvolupar, basada en l'anàlisi i la utilització de les dades de la HCE. Segons la consulta, l'objectiu del projecte de creació de la plataforma, és fer possible que les dades referides a la salut mental de la població del territori afectat puguin ser utilitzades per generar coneixement.

La base de dades que crearia el Projecte, *"tindrà les característiques de ser estructurada, en base poblacional"* (de les persones ateses a tota la província per les entitats del Grup), "*prospectiva i acumulativa partint de les dades ja existents (1994-2014) sobre les quals s'aniran acoblant periòdicament les dades noves. Aquesta base de dades general l'anomenem base de dades del Grup".* (En aquest informe ens referirem a aquesta base de dades com a "BD-G").

Segons els esquemes de l'Annex 1 (Figura 1 –pàg.5-, Figura 2 –pàg. 9-, i secció 2.2), la informació continguda en la HCE, s'anirà incorporant a la BD-G, a partir de la qual s'anirien creant diferents bases de dades per cada projecte (BD-PRO).

Com s'explica en l'Annex 1 (seccions 2.2.1 i 2.2.2), a les diferents bases de dades assistencials (fitxers d'origen de la informació, provinents dels diferents centres del Grup) se'ls aplicaria un procés de dissociació, i a la BD-G resultant se li aplicaria un procés d'anonimització o dissociació irreversible. Les BD-PRO resultants s'utilitzarien per a les finalitats previstes del Projecte (secció 2.1 de l'Annex 1):

- 1. Generar informes interns per millorar la gestió dels recursos dedicats a l'atenció a la salut mental al Grup.
- 2. Desenvolupar recerca epidemiològica i observacional en salut mental que permeti generar publicacions científiques.
- 3. Desenvolupar projectes de col·laboració amb entitats externes al Grup per generar informes específics.

L'Annex 1 (secció 2.2) exposa les *"Solucions tècniques a la privadesa de dades",* que el Projecte vol garantir en tres nivells diferents:

"I) En les pròpies dades, és a dir, eliminant les variables identificatives dels individus, i per tant treballant amb dades anònimes.
II) En la possibilitat de re-identificació dels individus, és a dir minimitzant aquest risc al màxim.
III) En el bon ús en general d'aquestes dades, és a dir vetllar per a que s'utilitzin per a millorar la salut i mai en detriment del col·lectiu que ha permès que es generin."

En la secció 2.2 del mateix Annex 1 es descriuen diverses *"solucions per a garantir els tres nivells de seguretat en la privadesa de les dades"*, entre les quals es troba el procés d'extracció i anonimització de les dades de dades (seccions 2.2.1 i 2.2.2 de l'Annex 1), la limitació i el control d'accés a les dades (secció 2.2.3 de l'Annex 1), o la valoració del risc d'identificació en el disseny i en la difusió de dades dels projectes (secció 2.2.5 de l'Annex 1), previsions a les que es farà referència, amb detall, més endavant.

Vist, en síntesi, l'esquema del Projecte presentat, cal partir de la base que la recollida i el posterior tractament de dades personals ha de donar compliment al que disposa la

Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, i el Reial Decret 1720/2007, de 21 de desembre, de desenvolupament de la Llei Orgànica (LOPD i RLOPD).

L'objecte d'aquest informe consisteix en valorar si el tractament específic de dades personals que es pot derivar de la posada en funcionament del Projecte, compleix de forma adequada amb els principis i garanties de la normativa de protecció de dades personals.

A això cal afegir que la consulta formula 6 preguntes, en relació amb aspectes concrets de l'Annex 1. Sens perjudici de donar resposta a aquestes preguntes que formula el Grup, en aquest informe es farà altres consideracions que consideri necessàries i rellevants, sempre des de la perspectiva de la protecció de dades personals (LOPD i RLOPD), en relació amb el tractament de dades que preveu el Projecte.

D'entrada, la consulta formula la següent pregunta:

Pregunta 1: *"La proposta de solucions per a la protecció de les dades personals que exposem en el projecte (secció 2.2, pàgines 6-18) s'ajusta a la legislació vigent?"*

Atesos els termes amplis d'aquesta pregunta, s'hi donarà resposta en els següents Fonaments Jurídics d'aquest informe, en els que ens referirem a l'habilitació del projecte en termes generals, des de la perspectiva de la protecció de dades, així com a diverses qüestions referides als principis i garanties de la normativa de protecció de dades.

Pel que fa a la resta de preguntes formulades, referides a qüestions més concretes, s'hi farà referència més endavant.

III

Legitimació del tractament de dades previst al Projecte

La informació que ha de servir de base per a aquest Projecte, segons la informació aportada, es refereix al contingut de la història clínica dels pacients (HC), que es concreta en la normativa específica, en concret, la Llei 41/2002, de 14 de novembre, estatal, reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica, que regula amb caràcter bàsic determinades qüestions relatives a la HC i els drets dels pacients, així com, en l'àmbit de Catalunya, 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 (article 15.2 Llei 41/2002, i article 10 Llei 21/2000).

El contingut de la HC és ampli, de manera que s'hi contenen dades sensibles, informes relatius al pacient, i d'altres que poden donar informació de terceres persones, com ara els antecedents familiars o els professionals que atenen els pacients.

En qualsevol cas, el tractament de dades per a cadascuna d'aquestes finalitats presenta diferències, tant pel que fa a la informació concreta a la que es pot accedir, com per altres qüestions, com ara qui pot accedir i tractar aquestes dades dins del propi Grup, la necessitat o no de disposar del corresponent consentiment (article 6 LOPD), o les comunicacions que el Grup podrà efectuar d'aquestes dades.

Segons aquestes previsions, la finalitat d'investigació o recerca mèdica requereix ineludiblement el consentiment dels afectats, llevat que es procedeixi a l'anonimització, en uns termes que assegurin la protecció de la privacitat dels afectats.

El Projecte planteja la comunicació d'informació anonimitzada (tot i que, com veurem, no descarta la comunicació d'informació codificada i identificable), per generar informes interns per millorar la gestió dels recursos dedicats a l'atenció a la salut mental al Grup, per fer recerca epidemiològica i observacional en salut mental per a publicacions científiques, i per desenvolupar projectes de col·laboració per generar informes específics.

Sens perjudici de les consideracions que es faran en aquest informe, es considera que el Projecte disposa de suficient habilitació legal per articular un procediment d'anonimització d'informació personal de les HC per a les finalitats de recerca o investigació científica en l'àmbit de la salut, epidemiologia o docència, en els termes de l'article 11.3 Llei 21/2000, i la resta de normativa aplicable. Això, sempre que el procediment d'anonimització impedeixi la identificació de les persones afectades sense esforços desproporcionats.

Ara bé, atesa la informació aportada, no es descarta que el Projecte prevegi realitzar altres tipus d'estudis o informes, interns o externs, a partir de la informació de les HC, relacionats amb altres finalitats.

En aquest sentit, per exemple, si el Projecte preveu la realització d'estudis o informes relacionats amb les tasques d'administració i gestió del Grup, caldria tenir en compte que la normativa limita l'accés a la informació a aquelles dades relacionades amb les dites funcions, i limita també la comunicació de les dades, ja que només hi pot accedir determinat personal del centre (article 11.4 Llei 21/2000).

La mateixa consideració es pot fer respecte les funcions d'inspecció per comprovar la qualitat de l'assistència, ja que només determinat personal al servei de l'Administració sanitària pot accedir a aquesta informació (article 11.5 Llei 21/2000). Aquest personal podrà accedir a la informació que requereixi, sense necessitat de consentiment dels afectats ni d'anonimització, en els termes que ho prevegi la normativa. Però no sembla que el Grup quedi habilitat per, a través del Projecte, anonimitzar informació completa de les HC dels pacients per a aquestes finalitats, ni donar-ne un accés intern o extern general a aquesta informació.

En conclusió, pel que fa a la valoració global del Projecte, es pot concloure que el Grup estaria legitimat per articular un sistema de tractament i anonimització de dades de la HC dels pacients, principalment, per a les finalitats de recerca o investigació mèdica, l'epidemiologia i la docència, si es compta amb el consentiment de les persones afectades o s'anonimitza la informació de manera que no siguin identificables.

IV

Sobre la responsabilitat del tractament i sobre l'encàrrec del tractament

D'entrada, l'article 3.d) de l'LOPD determina que és responsable del fitxer o el tractament la persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que decideixi sobre la finalitat, el contingut i l'ús del tractament.

Cal tenir en compte que la informació que passarà a formar part del projecte forma part dels fitxers d'alguna de les entitats que hi participen. Aquestes entitats, pel que sembla, habilitarien una tercera entitat –en el projecte no queda clar quina seria- que duria a terme la consolidació de la informació i l'anonimització per tal de poder-la destinar a les finalitats previstes al projecte. Aquesta tercera entitat tindria la consideració d'encarregat del tractament (art. 3.g) LOPD).

En la secció 2.2.4 de l'Annex 1 s'al·ludeix a que serà el Grup qui durà a terme el procés d'anonimització. La secció 2.2.1 fa referència al disseny i càrrega de dades al BD-G i fa esment que és important eliminar duplicitats, i que el procés d'extracció de les dades inclou un tractament que ordena, classifica i agrupa les dades de cada pacient, i que en el fitxer consolidat (que seria el BD-G), s'identifiquen i tracten els casos duplicats. S'afegeix que tots aquests processos són realitzats pel departament d'informàtica del Grup, que és el responsable de la seguretat d'aquests fitxers creats amb finalitats assistencials (és a dir, els fitxers de pacients de cada centre).

En qualsevol cas, aquesta tercera entitat sembla que intervindria com a encarregada del tractament respecte cadascuna de la resta d'entitats implicades.

La consulta adjunta, com Annex 3, una còpia de l'Acord per a la protecció de dades de caràcter personal en les comunicacions i accessos de dades entre les empreses del Grup (Annex 3) establert l'any 2013. Aquest Acord estipula que quan una de les entitats del Grup hagi d'accedir a dades personals contingudes en fitxers de les altres entitats, s'obliga a respectar l'LOPD conforme els articles 9 i 12 de l'LOPD (Acord segon).

D'entrada, no sembla que l'Acord de l'Annex 3, citat, pugui considerar-se com un contracte d'encàrrec del tractament de dades personals -en atenció al que disposa l'article 12 LOPD i articles 20 a 22 RLOPD-. La documentació aportada no inclou, pròpiament, un contracte d'encàrrec del tractament, en els termes de l'article 12 LOPD i dels articles 20 a 22 RLOPD, sinó només una previsió de formalitzar-lo en el futur.

Més enllà d'això, les entitats que signen aquest Acord no coincideixen plenament amb les que participen en el Projecte i a més, els serveis que s'hi descriuen tampoc coincideixen amb els que són objecte del Projecte. (Els serveis previstos en l'Acord primer, es refereixen a la gestió de personal i recursos humans, al servei de prevenció de riscos i de salut laboral, als serveis de compra de medicaments als laboratoris, etc tot i que es preveu que es podran veure ampliats a altres anàlegs).

Segons disposa l'article 12.2 de la LOPD:

> *"La realització de tractaments per compte de tercers ha d'estar regulada en un contracte que ha de constar per escrit o en alguna altra forma que permeti acreditar-ne la concertació i el contingut, i s'hi ha d'establir de manera expressa que l'encarregat del tractament només ha de tractar les dades d'acord amb les instruccions del responsable del tractament, que no les pot aplicar ni utilitzar amb una finalitat diferent de la que figuri en el contracte esmentat, ni comunicar-les a altres persones, ni tan sols per conservar-les.*
>
> *El contracte també ha d'estipular les mesures de seguretat a què es refereix l'article 9 d'aquesta Llei que l'encarregat del tractament està obligat a implementar."*

D'acord amb això, aquesta entitat que actuaria per encàrrec de cadascuna de les entitats responsables de la informació, hi pot accedir per dur a terme un tractament –la consolidació i l'anonimització- per compte del responsable, però no habilita en cap cas

per a que es pugui produir un intercanvi d'informació no anonimitzada amb altres entitats, encara que formin part del mateix Grup.

En relació amb la intervenció de terceres entitats, la consulta formula la següent pregunta:

Pregunta 4: *"Està previst que les dades siguin estructurades i analitzades per professionals contractats per l'entitat* (...)*, però si en algun cas fos necessària la participació d'un tercer, aliè a la nostra empresa, els mecanismes previstos en la nostra proposta (secció 2.2.4, pàgines 14-16), són suficients per garantir la seguretat de les dades?"*

En la secció 2.2.3 de l'Annex 1, es preveu:

"En el cas excepcional d'un projecte que impliqui anàlisis sobre les dades de la BD-PRO d'una persona aliena a la nostra empresa es farà un Contracte de tractament de dades i es decidirà el procediment d'accés a les dades a emprar (especificat a l'apartat 2.2.4)."

D'entrada s'ha de fer notar que sembla que hi ha una errada en la redacció d'aquest paràgraf, atès que en lloc de "*que impliqui anàlisis sobre les dades de la BD-PRO d'una persona aliena*" sembla que es volia dir "*que impliqui l'anàlisis per una persona aliena de les dades de la BD-PRO*".

Al marge d'això, la secció 2.2.4 del mateix Annex 1, fa referència a la *"Connexió des de l'exterior (Protocol d'accés remot, amb Contracte de tractament de dades)",* i fa una previsió en el sentit que el responsable del Fitxer de Recerca on s'allotja la BD-G *"valorarà l'interès de la connexió des de l'exterior de personal aliè. Si està justificat es formalitzarà la col·laboració en un "Contracte de tractament de dades "que signaran ambdues parts."* (...). La mateixa secció, inclou alguna previsió respecte l'accés de persones alienes a la institució, com ara que hauran de sol·licitar el permís a la Comissió de gestió de dades de la plataforma.

La informació aportada no explica quin és el rol i atribucions dels *"professionals contractats per l'entitat"* que sembla que realitzarien les tasques pròpies del procés de codificació i anonimització. El Projecte no concreta si és personal propi i integrat en el Grup o personal extern contractat, el que ha de realitzar aquestes tasques.

Si el procés de codificació i anonimització de bases de dades que contenen dades personals implica l'accés per part de tercers, el responsable del fitxer o tractament hauria d'especificar, en el context del Projecte, com es durà a terme aquest procés, per part de qui (personal intern o extern, en quins casos i amb quin grau de participació en cada fase del procés) i, si escau, formalitzar prèviament a l'inici del tractament, el contracte o contractes d'encàrrec del tractament que siguin necessaris. I òbviament caldria establir el corresponent acord d'encàrrec del tractament en els termes de l'article 12 LOPD i 20-22 RLOPD, tot i que en aquest cas en realitat es tractaria d'un subencarregat del tractament, per la qual cosa caldrà tenir en compte específicament el que estableix l'article 21 del RLOPD per a la subcontratació de serveis.

En qualsevol cas hauria de tractar-se de persones concretes que tinguin atribuïdes aquestes funcions dins el Grup – ja siguin personal propi o contractat-, sense cap tipus de vinculació amb els projectes de recerca de què es tracti i sotmeses a una especial exigència pel que fa al compliment del deure de confidencialitat.

Per tant, convindria clarificar com es duu a terme l'accés i tractament de les dades de determinats fitxers que són responsabilitat de cada centre, dins el propi Grup, per a la finalitat de donar compliment al Projecte.

Fets aquests advertiments, atesa la insuficiència de la informació aportada no es pot valorar ni l'oportunitat de preveure el dit contracte ni el seu contingut. En qualsevol cas, les previsions de la secció 2.2.4 de l'Annex 1, sobre les que es formula la pregunta, no sembla que puguin considerar-se suficients en aquest sentit, tenint en compte les exigències de l'article 12 LOPD.

V

Aplicació del principi de qualitat de les dades

L'article 4.1 de l'LOPD recull el principi de qualitat de les dades, que en la seva vessant de proporcionalitat, estableix el següent:

> *"1. Les dades de caràcter personal només es poden recollir per ser tractades, així com sotmetre-les a aquest tractament, quan siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut.*

El principi de qualitat s'ha de tenir present en totes les fases del Projecte. Tant en el moment inicial de concretar quins fitxers de dades (article 3.b) LOPD) del Grup han de formar part del Projecte, com a l'hora de concretar quina informació personal, tractada en els dits fitxers, es podrà comunicar en cada cas, per a les finalitats de cada projecte d'investigació concret.

La informació que ha de servir de base per a aquest Projecte es refereix al contingut de la història clínica dels pacients (HC), que és ampli, ja que conté dades sensibles, informes relatius al pacient, i d'altres que poden donar informació de terceres persones, com ara els antecedents familiars o els professionals que atenen els pacients (Llei 41/2002, i Llei 21/2000).

L'LOPD estableix un règim de protecció reforçat per a les dades de salut, entenent com a tals les informacions que concerneixen la salut passada, present i futura, física o mental, d'un individu, així com les referides al seu percentatge de discapacitat i a la seva informació genètica (article 5.1.g) RLOPD), que es tradueix en un seguit de garanties (articles 7 i 8 de la LOPD) i l'exigència de l'aplicació de mesures de seguretat de nivell alt (art. 81 RLOPD).

Com ha fet avinent aquesta Autoritat en els Dictàmens 34/2014 i 20/2015, en què s'ha analitzat la utilització de la HC per a finalitats d'investigació i reutilització d'informació en el Projecte VISC+ (que es poden consultar al web www.apd.cat, i les consideracions dels quals són en bona mesura aplicables al Projecte que ara analitzem), la protecció reforçada de les dades de salut, i la necessària aplicació del principi de qualitat, essencial en el tractament de dades personals no anonimitzades, és rellevant també per al cas de les dades anonimitzades, perquè en l'entorn del *big data* i amb les possibilitats que ofereix la mineria de dades -conceptes als quals es refereix el Projecte que analitzem (secció 1.1 de l'Annex 1)-, l'encreuament d'informació obtinguda d'orígens diversos, fins i tot si ha estat anonimitzada, pot acabar fent identificable una persona.

En l'entorn de la reutilització d'informació sensible, fins i tot quan aquesta informació es codifica i posteriorment s'anonimitza com preveu el Projecte, no és possible assegurar el risc zero respecte d'una possible re-identificació dels afectats (article 5.o) RLOPD).

En funció del volum de dades que, en el context del Projecte que analitzem, es posin a disposició del propi entorn assistencial del Grup ("informes interns") o fins i tot a disposició de qualsevol persona ("publicacions i informes externs"), i segons la forma com s'ofereixin, la possibilitat que la combinació d'aquesta informació amb informacions obtingudes d'altres fonts pugui acabar fent identificables persones concretes, no es pot descartar. Per això cal tenir especialment en compte que no es produeixi un risc per a la privacitat dels afectats, com s'ha posat de manifest, entre d'altres, en la Comunicació de la Comissió, sobre *"Dades obertes. Un motor per a la innovació, el creixement i la governança transparent"* (COM(2011)882 final).

Atesos els riscos inherents, cal ser molt restrictiu amb la informació de salut que s'ofereixi en obert -recordem que en el projecte s'inclou la possibilitat de fer "publicacions" tot i que no es concreta quin serà el seu contingut i naturalesa-, llevat que s'ofereixi amb nivells d'agregació sobradament amplis.

Respecte d'això, cal tenir en compte, encara, un altre factor. En el cas que ens ocupa, la informació de base sobre la que es sustenta el Projecte en alguns casos pot no permetre un alt nivell d'agregació de la informació, als efectes d'assegurar un risc mínim de re-identificació. L'abast de persones afectades es circumscriu a una província, la qual cosa implica, d'entrada, una limitació inicial, a nivell quantitatiu, de persones afectades. A més, per la informació de què es disposa, sembla que els informes i publicacions resultants del Projecte, es referiran no a qualsevol malaltia o trastorn de salut, algun dels quals pot afectar a una part quantitativament important de la població (com seria el cas d'una malaltia típica i recurrent en infants i adolescents, per exemple), sinó que es circumscriu a malalties mentals, l'abast i incidència de les quals, en la població general, pot ser limitat. Aquest factor pot comportar que, pel propi abast geogràfic, quantitatiu i qualitatiu del Projecte, no es pugui descartar un cert risc de re-identificació dels afectats.

En aquest sentit, la secció 2.2.3 de l'Annex 1 es refereix a què les BD-PRO tindran el nombre de casos necessari per assolir els objectius del projecte. Seria bo afegir-hi que també tindran el nombre de casos necessaris per garantir la no-identificabilitat de les persones afectades.

Per tot l'exposat, la necessària aplicació del principi de qualitat i de proporcionalitat en la seva vessant de minimització (tractar la informació personal mínima imprescindible per a cada projecte), és clau quan es tracten dades personals, però també si es fa un tractament de dades anonimitzades.

Si ens atenim a la informació aportada en la consulta (principalment, l'Annex 1, que descriu el Projecte), es fan referències generals a "les dades de salut mental" de la població afectada, que tracten els diferents centres del Grup, i a la informació continguda a la HCE dels pacients atesos pel Grup, a "dades mèdiques" (secció 2.2.5 Annex 1) i a la "extracció de dades de múltiples fonts" (Figura 2 Annex 1), entre d'altres. Les mencions genèriques a les HCE com a font d'informació del Projecte, no resulten suficients des de la perspectiva de la normativa de la protecció de dades, en concret, del principi de qualitat, als efectes de concretar la informació personal afectada pel Projecte.

Per tot això, cal que el Projecte estableixi amb claredat:

a) Quins fitxers, dels diferents centres que formen part del Grup, segons la informació del Registre de l'Agència Espanyola de Protecció de Dades (AEPD), formaran part del Projecte. Cal tenir en compte que alguns fitxers dels centres, com els referits a salut laboral, inclouen dades de salut, però no sembla que hagin de formar part del Projecte, i així s'hauria d'explicitar.

b) Quina informació concreta dels fitxers afectats s'utilitzarà en el Projecte: segons la informació relativa als fitxers de pacients o usuaris inscrits a l'AEPD, a banda de dades de salut, es tracten dades d'origen racial o ètnic, i de vida sexual, informació que també és sensible als efectes de l'article 7 LOPD. Cal aclarir si aquestes tipologies queden afectades pel Projecte. En alguns fitxers de pacients, també es tracten altres tipologies de dades que no són pròpies de la HC dels pacients, i informacions que afecten terceres persones (familiars del pacient, així com dades del metge responsable i de l'equip que atén el pacient). Resulta necessari que el Projecte concreti quines tipologies de dades, de les incloses en els fitxers que seran font d'informació del Projecte, quedaran afectades pel mateix.

c) També, i en atenció als riscos inherents al seu tractament, caldria excloure determinats tipus d'informació com ara dades genòmiques.

d) Un cop elaborada la BD-G, cal concretar quina informació anonimitzada ha de ser comunicada per a projectes concrets (BD-PRO), i que aquesta sigui la mínima indispensable per a assolir la finalitat pretesa en cada cas. Dins de les dades anonimitzades, aquesta prevenció és encara més rellevant en el cas de les publicacions i els informes externs als que es refereix el Projecte, que puguin tenir una difusió àmplia i generalitzada. En aquest sentit, seria bo que quan la secció 2.3.2.2 de l'Annex 1 es refereix al contingut de la plantilla que ha de formar part del formulari de sol·licitud, s'inclogués una referència a les dades estrictament necessàries per a dur a terme el projecte.

Concretament en relació amb els fitxers, la consulta formula la següent pregunta:

Pregunta 2: *"És correcte allotjar la base de dades primària amb la identificació de les persones dissociada* (BD-G) *al FITXER PACIENTS de l'entorn assistencial (secció 2.2.1.2, pàgina 10) i les bases de dades anonimitzades, específiques de cada projecte, llestes per fer les anàlisis i que anomenem BD-PRO al Fitxer recerca (secció 2.2.3, pàgina 12), ambdós ja donats d'alta a l'AEPD. Si no és correcte, caldria crear i donar d'alta un nou fitxer per a aquesta activitat? Si la resposta fos afirmativa, on caldria registrar-lo: a l'AEPD o a l'APDCAT?".*

Cal partir de la base que l'exigència de la normativa de protecció de dades respecte la creació de fitxers de dades, respon a la necessitat que els tractaments de dades siguin coneguts pels afectats.

Com es desprèn de la informació disponible (Registre de l'AEPD i documents de seguretat dels Annexos 6 i 7), cada centre del Grup té el seu propi fitxer de pacients o usuaris, que es refereix als pacients atesos al propi centre, i no als pacients atesos en altres centres del Grup. Hi ha dos fitxers "Investigación" (de dues de les entitats del Grup), de manera que no tots els centres del Grup tenen un fitxer de recerca propi.

Cal recordar, d'acord amb el que hem exposat, que els responsables de la informació són les entitats que en origen tenien aquesta informació en els seus fitxers, i que l'entitat que dugui a terme el procés d'anonimització només intervindrà com a encarregada del tractament.

Als efectes de transmetre informació clara als afectats, cal tenir en compte que els fitxers de "pacients", incorporen la finalitat o ús de "investigació epidemiològica", però no altres tipus d'investigació. En qualsevol cas, la finalitat principal d'aquests fitxers és la de donar prestació sanitària als afectats, i així ho poden percebre aquests. En canvi, la gestió de les dades necessàries per a finalitats d'investigació, és pròpia dels fitxers d'Investigació.

Amb tot això, vist el contingut dels fitxers de "pacients" i de "recerca" dels centres del Grup, i atès el tractament que s'ha de realitzar en base al Projecte, sembla més convenient que siguin els fitxers de "Recerca" de cadascun dels responsables de la informació els que incorporin (o "allotgin", en els termes de la consulta), la base de dades primària amb la identificació de les persones (BD-G). Ara bé, això suposaria que tots els centres que participen en el Projecte tinguin creat el seu propi fitxer de "Investigació o recerca".

Cal fer notar que la informació resultant d'un procés d'anonimització, de manera que no faci identificable les persones a les quals fa referència, no té la consideració d'informació de caràcter personal, per la qual cosa, no estaria sotmesa a l'obligació de figurar en un fitxer (article 3.b) LOPD). Qüestió diferent és que abans i durant el procés d'anonimització sí que hauria de formar part d'un fitxer que pugui englobar la informació dels diferents centres que participen en el Projecte i que prevegi expressament les finalitats que formen part del Projecte.

En qualsevol cas, tenint en comte l'àmbit d'actuació d'aquesta Autoritat (article 3.f) Llei 32/2010), que abasta les entitats proveïdores de serveis públics de salut, els fitxers que s'hagin de crear en relació amb la implementació del Projecte s'han de notificar al Registre de Protecció de Dades de Catalunya, d'aquesta Autoritat.

VI

Sobre la finalitat del tractament de dades, els destinataris de la informació i la gestió de peticions

Com ha fet avinent aquesta Autoritat en anteriors ocasions, entre d'altres en l'Informe 3/2014 relatiu al Projecte de decret de modificació del Decret 67/2010, i com ha reiterat en els Dictàmens 34/2014 i 20/2015, citats, l'exigència de legitimitat ha de ser especialment estricta quan es tracten dades sensibles.

Tal com hem vist, l'article 4.1 de l'LOPD preveu que la informació només pot tractar-se en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut. La secció 2 del mateix article 4 afegeix que les dades de caràcter personal objecte de tractament no es poden utilitzar per a finalitats incompatibles amb aquelles per a les quals les dades hagin estat recollides. No es considera incompatible el tractament posterior d'aquestes dades amb finalitats històriques, estadístiques o científiques.

Aquestes previsions conformen el que s'anomena principi de finalitat en la normativa de protecció de dades de caràcter personal.

Tal com hem vist, si ens atenim a les previsions de la normativa sectorial, la finalitat d'investigació o recerca mèdica requereix ineludiblement el consentiment dels afectats, llevat que es procedeixi a l'anonimització, en uns termes que assegurin la protecció de la privacitat dels afectats. Per al compliment d'altres finalitats, pot no ser requerit el dit consentiment (Lleis 21/2000 i 41/2002).

La documentació tramesa sobre el Projecte, no conté una descripció detallada sobre les finalitats per a les quals s'utilitzaria la informació inclosa en el Projecte. La secció 2.2.2 de l'Annex 1 del Projecte fa referència per una banda a projectes interns de gestió clínica i per una altra banda a projectes de recerca i col·laboratius.

Pel que fa a l'elaboració d'informes interns de gestió clínica, sembla que els circumscriu a la millora de la gestió dels recursos relacionats amb la salut mental. D'entrada, cal fer notar que, encara que formin part d'un mateix Grup, la informació de cadascuna de les entitats només pot ser tractada en el marc de l'activitat de cadascuna de les institucions que en formen part. Per això, no es pot considerar un "*ús intern*" cap tractament que comporti una comunicació de dades entre aquestes entitats. Això sens perjudici del que ja s'ha exposat respecte dels casos en què una entitat intervingui per compte d'una altra en el marc d'un encàrrec del tractament.

En aquest sentit, a la secció 2.3.2.1 de l'Annex 1 convindria aclarir que quan aquests projectes interns requereixin tractar dades personals de pacients d'altres institucions del Grup cal comptar amb el seu consentiment o amb una habilitació legal suficient.

En qualsevol cas, les previsions genèriques contingudes a la documentació aportada no permeten determinar si els dits informes (peticions internes que no sortirien de l'àmbit hospitalari, segons la secció 2.3.2.1 de l'Annex 1), es refereixen, per exemple, a funcions d'inspecció (art. 11.5 Llei 21/2000), de planificació o si també es refereixen a la finalitat d'investigació. Cal, doncs, aclarir el concepte de "gestió clínica" de la secció 2.3.2.1, citat, i vincular-lo amb els usos de la HC previstos a la normativa. Resulta necessari aclarir aquesta qüestió, atès que això condiciona la necessitat de requerir o no el consentiment dels afectats, o si aquest consentiment es pot obviar a través d'un procés d'anonimització de la informació suficient i adequat. En definitiva, això condiciona la informació personal que es podrà utilitzar, i en quins termes es podrà utilitzar.

Pel que fa a la finalitat de desenvolupar projectes de recerca i col.laboratius, aquesta finalitat s'emmarcaria en la previsió de l'article 11.3 Llei 21/2000, i és clar que una adequada anonimització exclouria la necessitat de consentiment. Es dedueix (secció 2.3.2.2 de l'Annex 1) que la utilització de la informació de les HC, en el context del Projecte, per a finalitats d'investigació, podria dur-se a terme dins l'àmbit hospitalari, però també es podria dur a terme per "entitats externes" que la documentació aportada no concreta, i que també serà necessari concretar. En aquest sentit, de la documentació aportada no es pot inferir quin és "l'entorn no assistencial" (Figura 1 Annex 1) que podria ser receptor de la informació del Projecte, si es circumscriu a l'àmbit de la xarxa sanitària pública, si podria tractar-se d'investigadors de l'àmbit públic o privat, d'empreses privades, vinculades o no a l'àmbit sanitari, etc.

D'entrada, la utilització del terme "col.laboratius" com quelcom diferenciat dels projectes de recerca, pot fer pensar que en aquest segon cas no es tractaria d'una finalitat de recerca científica. Però a més, caldria concretar que es tracta en tots els casos de projectes de recerca en l'àmbit de les ciències de la salut, i que en canvi s'exclouen altres àmbits de recerca com per exemple en l'àmbit de les assegurances o de la prospecció comercial.

Més encara, el fet que el Projecte es refereixi, sense més concreció, a "informes externs" o a "publicacions", permet interpretar que les dades tractades en el context del Projecte podrien ser difoses en obert (com es desprèn de diversos apartats de la documentació aportada, entre d'altres, la secció 2.3.2.2 de l'Annex 1), o que podrien ser comunicades a qualsevol interessat, públic o privat, o posades a disposició de la ciutadania en general.

La poca concreció respecte les finalitats o usos de la HC a les que es pot donar compliment en cada cas, respecte els destinataris finals de la informació, i respecte el tipus de difusió que podria tenir la informació tractada, no permet considerar que el Projecte s'ajusta, en els seus termes actuals, a les exigències de la normativa de protecció de dades (principi de finalitat). En aquest sentit, la informació aportada no permet realitzar una anàlisi imprescindible des de la perspectiva de la protecció de dades –i necessàriament prèvia a la comunicació d'informació-, que ha de tenir en compte els següents aspectes:

- Quin és l'ús concret, habilitat en la normativa, al que es vol donar compliment amb cada projecte o petició d'informació.
- Si el consentiment és o no necessari en cada cas.
- Quines dades són necessàries per a cada projecte, tenint en compte el principi de minimització.
-Quina entitat, i de quina naturalesa (pública, privada, associacions), sol·licita les dades, i per a quina finalitat concreta.
- Quina difusió es farà de la informació tractada (difusió en obert per al públic en general, a determinades institucions, o limitada al Grup).

L'anàlisi d'aquests factors ha de ser, necessàriament, previ a la comunicació de qualsevol conjunt d'informació (BD-PRO), fins i tot si es tracta d'informació anonimitzada, i s'ha de referir a cada projecte en concret. En qualsevol cas, cal apuntar que la realització d'un procés d'anonimització, atès el risc de re-identificació, no és motiu suficient per obviar aquesta anàlisi prèvia dels factors esmentats, des de la perspectiva de la protecció de dades.

Pel que fa als possibles destinataris de la informació, caldria que el Projecte els concretés, si més no les categories de subjectes destinataris, atès que aquest és un element essencial a l'hora d'analitzar l'adequació a la finalitat prevista i les garanties que cal adoptar.

El Projecte tampoc estableix la manera com es realitzarà la gestió de les sol·licituds de BD-PRO per a un projecte determinat. Manca, en la documentació aportada, un esquema clar respecte el procediment d'anàlisi de les demandes de conjunts d'informació.

Caldria establir de manera clara el procés d'anàlisi de les demandes, que manera que es pugui analitzar amb les garanties escaients l'adequació de les finalitats de cada projecte concret, els destinataris de la informació, el contingut que ha de tenir cada BD-PRO concreta, i les mesures a adoptar en funció de la resta de circumstàncies concurrents.

La inconcreció respecte els destinataris tampoc no permet avaluar si es pot produir en algun cas una transferència internacional de dades (TID), necessàriament sotmesa a les exigències del règim previst (article 33 i 34 LOPD).

En definitiva, el Projecte hauria d'establir un quadre en el que es concretessin les finalitats que es poden dur a terme amb la informació tractada segons la normativa

específica (Llei 41/2002 i Llei 21/000), quins poden ser els destinataris (o tipologies de destinataris) de la informació en cada cas, en funció de les finalitats preteses, quin és el procediment d'aprovació de les demandes concretes i quin grau de difusió podrà tenir l'informe o estudi resultant en cada cas.

Dit d'una altra manera, cal que el Projecte estableixi i expliqui una connexió clara entre el destinatari de la informació (d'una BD-PRO), la finalitat a complir, la concreció de la informació a què podria tenir accés, i si aquesta informació ha de ser anonimitzada o en quins casos es pot comunicar dades no anonimitzades en base al consentiment.

VII

Sobre el règim de comunicació i el consentiment dels afectats

Pel que fa a la possibilitat de comunicar dades a tercers (els destinataris de les BD-PRO), cal atendre al règim de comunicació de dades personals (article 11 LOPD, citat).

L'article 11.6 LOPD, per la seva banda, estableix que si la comunicació es produeix previ procediment de dissociació, no és aplicable el que s'estableix en els apartats anteriors.

Per tant, la comunicació de la informació a terceres persones o entitats per part del Grup només es pot dur a terme si la informació està anonimitzada o si es compta amb el consentiment dels pacients.

Sobre això, cal fer menció que en la documentació tramesa s'hi inclou un formulari que s'identifica com a formulari de *"Cessió de dades".*

El formulari de l'Annex 9, citat, es refereix a la recollida de dades en relació amb el *"Fitxer de pacients"* d'una de les entitats, amb la finalitat de prestar l'assistència mèdic-sanitària al pacient. En aquest formulari es preveu que el pacient autoritza el tractament de les seves dades "per finalitats d'investigació/recerca i docència". En concret, l'afectat autoritza l'entitat *"per a què utilitzi les meves dades també per finalitats d'investigació/recerca i docència, garantint-ne la confidencialitat de la informació facilitada i en cap cas seran cedides a tercers".* En realitat però aquest formulari no seria un instrument vàlid per a legitimar la comunicació. I això no només perquè seria desitjable una major concreció a l'hora de definir la finalitat (més enllà de la menció genèrica a investigació/recerca i docència) sinó, especialment perquè tal com s'acaba de recollir, el formulari preveu expressament que l'entitat no cedirà dades a tercers. Per tant no pot habilitar cap cessió de dades.

En qualsevol cas, des de la perspectiva del principi de qualitat, quan s'articuli el corresponent consentiment informat, caldrà limitar el tractament i la cessió de dades només a les que siguin rellevants als efectes de l'estudi o investigació que es vulgui dur a terme per part del destinatari final.

VIII

Gestió de drets ARCO i possibilitat d'exercir l'opt-out

L'LOPD reconeix als afectats la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició (drets ARCO), en relació amb el tractament de les seves dades personals (Títol III LOPD i Títol III RLOPD).

En la secció 2.3.3 de l'Annex 1, es preveu que:

"Tal com estableix la nostra normativa interna els nostres usuaris (pacients) en ser atesos per primera vegada reben un full informatiu en el que s'explica que les seves dades personals i les derivades de la seva atenció passen a formar part d'un base de dades assistencial (la HCE). També se'ls informa dels drets ARCO i del procediment per exercir-los. (...).

De la mateixa manera s'establirà un procediment fàcil i àgil per a que els nostres usuaris puguin en qualsevol moment manifestar el seu interès en que les seves dades total o parcialment siguin retirades (opt-out) –en referència a la BD-G- *(abans o després del procés d'anonimització) i per tant que no desitgen que les seves dades s'incloguin en els estudis de la Plataforma* (...)*".*

En aquests moments els drets ARCO s'exerceixen a través de la oficina d'atenció a l'usuari."

En relació amb això, la consulta adjunta un *"document de cessió de dades"* (Annex 9), al qual ja ens hem referit en el fonament jurídic anterior. Aquest document, que malgrat la seva denominació no té per objecte la cessió de dades, tal com hem exposat, informa sobre la possibilitat d'exercir els drets ARCO i sobre altres extrems previstos a l'article 5 de l'LOPD, però alhora també inclou un formulari d'autorització per a la utilització de les dades amb finalitats d'investigació/recerca i docència.

Caldria distingir la informació que s'ha de donar als afectats en els termes de l'article 5 LOPD, per tal de ser atesos a l'entitat i, per extensió, a la resta de centres del Grup, de la informació i recollida del consentiment, si escau, que pot comportar el tractament de dades derivat del Projecte.

Recordem que l'article 5.1 LOPD exigeix al responsable informar de manera expressa, precisa i inequívoca als afectats, prèviament al tractament:

> *"1. Els interessats als quals se sol·licitin dades personals han de ser prèviament informats de manera expressa, precisa i inequívoca:*
> *a) De l'existència d'un fitxer o un tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.*
> *b) Del caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades.*
> *c) De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.*
> *d) De la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.*
> *e) De la identitat i la direcció del responsable del tractament o, si s'escau, del seu representant.*
> *(...)*
> *2. Quan s'utilitzin qüestionaris o altres impresos per a la recollida, han de figurar-hi, de manera clarament llegible, les advertències a què es refereix l'apartat anterior.*
> *(...)"*

Vistes les consideracions fetes en aquest informe, i tenint en compte les característiques del Projecte (tractament de dades de tots els pacients del Grup i no només dels pacients de una de les entitats que en formen part), el formulari de l'Annex 9 no es pot considerar suficient als efectes de donar una informació adequada als

afectats, sobre el tractament derivat del dit Projecte, en relació amb el deure d'informació i l'exercici dels drets ARCO.

Per tant, caldria, d'entrada, que el Projecte incorporés un formulari específic en què s'expliqui adequadament als afectats, en els termes de l'article 5 LOPD, les característiques del tractament que es preveu fer en el marc del Projecte analitzat. Cal tenir en compte que els drets ARCO són d'aplicació respecte les dades dels pacients tractades en el marc de la HCE, fins que es produeixi l'anonimització en els termes apuntats (BD-PRO), i així s'hauria d'explicar als afectats.

Sens perjudici d'això, cal valorar positivament que el Projecte prevegi la possibilitat que els afectats exercitin l'opt-out, per tal que la seva informació personal no entri a formar part del Projecte, i puguin, així, mantenir-se'n al marge.

En qualsevol cas, convindria explicitar i plasmar en un formulari específic, abans de posar en marxa el Projecte, com es podrà exercir aquest dret -que hem de distingir del dret d'oposició (article 6.4 LOPD), en el sentit que l'opt-out no requereix una motivació ni justificació per part de l'afectat-, el mecanisme per exercir-lo, i les seves conseqüències, per tal que els afectats puguin decidir de forma lliure i informada si volen excloure les seves dades del Projecte.

En relació amb la conveniència de diferenciar l'exercici dels drets ARCO de l'exercici de l'opt-out, convé apuntar que en el punt 7 de la secció 2.2.1.2 de l'Annex 1, referit al procés de codificació i d'anonimització de la informació, es fa esment que a la BD-G se li aplicaran els drets ARCO dels usuaris que els han exercit, en el sentit d'eliminar els registres dels usuaris que han manifestat que no volen que les seves dades siguin emprades per aquestes anàlisis.

Sembla que el Projecte s'estaria referint a eliminar els registres de pacients que han exercit l'opt-out, i no pas als que han exercit un dret ARCO, i així s'hauria de recollir en la secció 2.2.1.2.

IX

Sobre la utilització de dades anominitzades o codificades

La consulta formula la següent pregunta:

Pregunta 3: *"La plataforma que proposem treballarà amb dades anonimitzades però en casos excepcionals de projectes que ho requerissin i sempre sense sortir dels nostres servidors, seria correcte treballar amb dades dissociades (codificades reversiblement i identificables?) (secció 2.2.3, pàgina 13).*

La secció 2.2.3 de l'Annex 1 (pàg.13), citada, preveu el següent:

"Si en algun cas excepcional fos necessari dissenyar un projecte en el que es justifiqui treballar amb dades dissociades per a poder re-identificar els subjectes de l'estudi, caldrà especificar-ho en el disseny del projecte i concretament especificar en la metodologia de l'estudi com es crearà el sistema de dissociació/codificació (...)".

El Projecte fa esment per una banda a dades anonimitzades i per una altra banda a dades dissociades, com equivalents, en aquest segon cas, a dades "*codificades reversiblement i identificables*". Vistes aquestes mencions, d'entrada, convé fer un aclariment des del punt de vista terminològic.

Segons l'article 3.a) de l'LOPD, és dada personal qualsevol informació referida a persones identificades o identificables. Segons l'article 5.1.e) del RLOPD, la dada dissociada és la que no permet la identificació d'un afectat o interessat. Segons l'article 3.f) de la LOPD, el procediment de dissociació és *"qualsevol tractament de dades personals de manera que la informació que s'obtingui no es pugui associar a una persona identificada o identificable."* Segons l'article 5.1.p) del RLOPD, aquest procediment de dissociació és el que permet l'obtenció de dades dissociades.

D'acord amb això, tant les dades que en el projecte s'anomenen anonimitzades, com les dissociades, no han de permetre identificar les persones afectades. No hi hauria problema que en el Projecte s'empri aquesta denominació per referir-se a aquelles dades a les quals s'ha incorporat un sistema de codificació, però hauria de quedar clar que tant en un cas com en l'altre, no han de poder ser identificables les persones afectades. El sistema de codificació no hauria de permetre que les persones, grups o entitats que duguin a terme les activitats de recerca, o terceres persones puguin reidentificar les persones afectades.

Per tant, d'entrada, convindria aclarir la terminologia emprada, ja que de la pregunta 3, citada, sembla que s'equipara la dada dissociada amb dada codificada i identificable.

Per altra banda, cal fer notar també que el Projecte incorre en alguna contradicció atès que, per exemple, a la secció 2.2.1.1 de l'Annex 1 s'indica primer que *"les dades amb informació de caràcter personal del pacient no formen part del procés de càrrega"* de la BD-G, però acte seguit s'afirma que les dades carregades a la BD-G inclouen el sexe, data de naixement, ABS del pacient, país del pacient i estat civil, que el poden fer fàcilment identificable.

Més enllà d'això, es valora positivament que el Projecte parteixi de l'excepcionalitat a l'hora de preveure la possibilitat de treballar amb dades codificades. Segons aquest esquema, s'haurien de distingir tres nivells: en el primer nivell i com a sistema preferent s'utilitzarien dades anonimitzades sense cap tipus de codificació; en un segon nivell i per a projectes que no es puguin dur a terme amb dades sense codificar s'empraria dades codificades de manera excepcional.

La re-identificació, en cas que resulti estrictament necessària, només hauria de ser possible, en els casos justificats previstos al Projecte, mitjançant un procediment que ofereixi les degudes garanties, per part de les persones vinculades al Grup –identificades de forma restrictiva- habilitades específicament per a dur a terme el procés d'anonimització o de re-identificació. En cap cas ho hauria de poder fer el destinatari.

Finalment, en un tercer grup o nivell d'anàlisi de les peticions d'informació, caldria agrupar, de forma excepcional i especialment motivada, les possibles comunicacions de dades "identificables". En qualsevol cas, s'entén que, pels motius exposats al llarg d'aquest informe, aquesta darrera possibilitat hauria de ser residual, i hauria de comptar amb el consentiment dels afectats.

L'articulació del flux informatiu que generarà el Projecte a partir dels tres nivells exposats, prioritzant el primer per sobre del segon i del tercer, i deixant aquest últim com a residual, facilitaria l'anàlisi per part del Grup de qualsevol petició de BD-PRO, en base a tots els elements que cal tenir en compte i vetllar, així, perquè el dit flux informatiu no posi en risc la privacitat dels afectats.

En qualsevol cas, i enllaçant amb el que ja s'ha apuntat en els fonaments jurídics anteriors, la manca de concreció del Projecte pel que fa a les finalitats, els destinataris i la informació comunicada en els termes apuntats, podria portar, en els termes actuals del Projecte, a una comunicació d'informació codificada –i reversible per terceres persones- que podria arribar a ser difosa a través d'un informe extern posat a disposició del públic en general, en termes *d'open data* o sota altres modalitats. Aquesta possibilitat, que forçaria els principis i garanties de la protecció de dades, hauria de quedar expressament exclosa de les possibilitats del Projecte.

El fet que, com s'apunta en la pregunta formulada, les dades codificades *"no surtin dels servidors"* del Grup, no legitima en sí mateix el tractament, en concret, la cessió de dades sensibles codificades a un destinatari que no es concreta, atès que, d'acord amb l'article 11.3 esmentat, el rellevant no és només la ubicació física de la informació sinó la finalitat per a la qual s'utilitza.

Per tot això, en relació amb la pregunta formulada, la legitimitat d'un tractament d'informació sensible a través d'una BD-PRO amb dades no anonimitzades, sinó codificades, només resultaria admissible si permet preservar la no-identificabilitat dels pacients.

X

Procediment tècnic d'anonimització

L'Annex 1 (secció 2.2) exposa les "Solucions tècniques a la privadesa de dades", que el Projecte vol garantir en tres nivells diferents:

"I) En les pròpies dades, és a dir, eliminant les variables identificatives dels individus, i per tant treballant amb dades anònimes.
II) En la possibilitat de re-identificació dels individus, és a dir minimitzant aquest risc al màxim.
III) En el bon ús en general d'aquestes dades, és a dir vetllar per a que s'utilitzin per a millorar la salut i mai en detriment del col·lectiu que ha permès que es generin."

A partir d'aquests 3 nivells de protecció que identifica el Projecte, en la secció 2.2 del mateix Annex 1 es descriuen diverses solucions per a garantir aquests nivells de seguretat en la privadesa de les dades.

En aquest context, la secció 2.2.1.1 de l'Annex 1 defineix el *"Procés informàtic per a la dissociació reversible de les dades".* Aquest primer procés de dissociació, que pretén, com exposa el Projecte, emmascarar la identitat d'un usuari per evitar la seva identificació, implica incorporar determinades dades en la BD-G (clau identificadora del pacient dins del BD-G, sexe, data de naixement, ABS del pacient, país de naixement i estat civil).

Per bé que el Projecte parteix de l'anonimització d'informació personal, en bona part, sensible, als efectes de crear les BD-PRO, cal tenir en compte cal tenir en compte les possibilitats que aquesta informació pugui permetre la identificació del seu titular. Així ho ha posat de manifest el Grup de Treball de l'Article 29 (en endavant, GTA29), en el seu Dictamen 5/2014, sobre tècniques d'anonimització, en el que es fa avinent el següent:

"(...) los responsables del tratamiento deben ser conscientes de que un conjunto de datos anonimizado puede entrañar todavía riesgos residuales para los interesados. Efectivamente, por una parte, la anonimización y la reidentificación son campos de

investigación activos en los que se publican con regularidad nuevos descubrimientos y, por otra, incluso los datos anonimizados, como las estadísticas, pueden usarse para enriquecer los perfiles existentes de personas, con la consiguiente creación de nuevos problemas de protección de datos. En suma, la anonimización no debe contemplarse como un procedimiento esporádico, y los responsables del tratamiento de datos han de evaluar regularmente los riesgos existentes."

Així, segons el GTA29, el risc de re-identificació és inherent a qualsevol tècnica d'anonimització, per la qual cosa la intimitat i el dret a la protecció de dades del titular, podria veure's compromesa. Això fa necessària la realització d'una anàlisi de possibles riscos per als drets dels afectats, i l'articulació de mesures per mitigar o evitar aquests riscos.

En els documents aportats existeixen algunes contradiccions sobre aquest punt. Així, tal com ja hem exposat, en la secció 2.2.1.1 de l'Annex 1, mentre per una banda s'indica que la informació de caràcter personal mai surt del Sistema d'informació productiu assistencial de l'organització, després s'afirma que les dades relatives al sexe, data de naixement ABS del pacient, país del pacient i estat civil sí que s'incorporen a la BD-Grup. La combinació d'aquestes dades pot permetre identificar una persona concreta amb una certa facilitat.

Cal tenir en compte que, especialment en l'entorn del *big data*, les possibilitats de re-identificació no passen exclusivament per l'eliminació de dades identificatives, sinó que la re-identificació es pot produir a partir de dades de característiques personals (nacionalitat, raça, marques físiques etc.), de dades de salut (malalties amb una baixa incidència), o de dades administratives o de l'atenció sanitària prestada (CAP on s'ha atès, ABS, metge que l'ha atès), per exemple.

En el projecte en la secció 2.2.2 de l'Annex 1 es manifesta que a partir de la BD-G es produiria el *"Procés d'anonimització de les bases de dades"* (secció 2.2.2 de l'Annex 1), segons el qual:

"Per tal de poder donar un ús legítim a la plataforma, cal trencar totalment l'enllaç que ens permetria identificar qualsevol pacient de les nostres fonts de dades principals, i que per tant, veuria compromesa i vulneraria la privacitat de la persona.

El procés d'anonimització, també conegut com a dissociació irreversible ja que un cop aplicat tota la informació del pacient queda deslligada de les dades que el permeten identificar i a més el nexe no es pot tornar a establir."

Però malgrat això no es descriu el procés d'eliminació de totes aquestes variables. Simplement es descriu la forma com s'atribueix a cada pacient un identificador únic aleatori, el UUID (*universally unique identifier*). Aquest identificador, que es generaria aleatòriament, de manera que, *"quan ja tenim tota la base de dades preparada, aquest procés genera els UUID de cada pacient, que és únic i aleatori".* Aquesta mateixa secció afegeix que, si es volgués repetir el procés, el UUID obtingut, donat un mateix pacient, ja no seria el mateix, de manera que es garanteix la destrucció de l'enllaç del qual s'ha extret la informació, i es garanteix la irreversibilitat de l'anonimització.

A la secció 2.2.5 de l'Annex 1 s'ofereixen alguns elements més, però no es concreten de manera que es pugui saber quines són les variables mínimes que s'exclouran, emmascararan o, si més no, s'analitzaran per evitar la identificabilitat (p. ex. totes les dades identificatives del pacient o de persones que hagin intervingut al procés assistencial, dades del centre, data concreta de naixement, dades de característiques personals no rellevants etc.)

Cal partir de la base que el procediment de dissociació de la informació de salut dels pacients atesos pel Grup que pugui ser objecte de tractament, amb destinació a les BD-PRO de determinats peticionaris interns o externs al Grup, entès com *"qualsevol tractament de dades personals de manera que la informació que s'obtingui no es pugui associar a una persona identificada o identificable"* (article 3.f) LOPD), haurà de ser adequat, per tal d'assegurar que es cedeixen *"dades dissociades"* (article 5.1.e) RLOPD), això és, dades que no permeten la identificació de l'afectat.

Des de la perspectiva de la protecció de dades, i de les exigències referides al procés d'anonimització de dades que s'ha de dur a terme en el context del Projecte cal valorar positivament la previsió d'atribuir un UUID a cada individu, de forma aleatòria, amb l'objectiu que la informació que rebi un destinatari (intern o extern al Grup) a través d'una BD-PRO, per a la realització d'un estudi o informe concret, no permeti la identificació d'aquest individu.

Per la informació aportada, el procés d'anonimització previst genera un UUID per a cada pacient obtingut de manera aleatòria. Des de la perspectiva de la protecció de dades, és recomanable preveure que per a cada petició d'una DB-PRO per a un determinat estudi o informe, també en el cas de dues o més peticions provinents d'un mateix destinatari, s'asseguri que el UUID generat sempre serà diferent.

Per la informació aportada, també sembla que el UUID seria únic per a cada projecte, ja que es fa referència que si es vol repetir el procés d'anonimització, el UUID obtingut per a un mateix pacient, ja no seria el mateix.

Amb aquests aclariments, en principi, l'anonimització feta a través de l'atribució de codis (UUID) aleatoris, es pot considerar adequada.

No obstant això, per aplicació del principi de minimització, el Projecte no hauria de renunciar a la possibilitat que determinats estudis o projectes no requereixin ni tan sols l'atribució de cap codi.

En qualsevol cas, en relació amb els procediments de dissociació o anonimització que s'hagin de dur a terme en el context del Projecte, resulten d'especial interès el Dictamen del GTA29, 6/2013, sobre dades obertes i reutilització de la informació del sector públic (ISP), de 5 de juny de 2013, així com el Dictamen 5/2014, del GTA29, sobre tècniques d'anonimització, de 10 d'abril de 2014, als que ens remetem.

Convindria doncs, que el projecte concretés la forma com es durà a terme el procés d'anonimització, més enllà de les previsions que ja es contenen sobre el procés d'atribució del UUID.

En relació amb aquesta qüestió, la consulta formula la següent pregunta:

Pregunta 5: *"La avaluació del risc de pèrdua de la privadesa de dades personals (secció 2.2.5 pàgina 17-19) consistent en l'aplicació d'un protocol basat en l'execució d'eines específiques en dos punts: en el procés de disseny del projecte i abans del lliurament o publicació dels resultats, és adequada?"*

La secció 2.2.5 estableix que *"es farà una anàlisi de riscos per projecte i s'aplicaran les mesures necessàries per tal de mantenir fins al final la privacitat de les dades i per tal d'assegurar que no es pot identificar cap persona amb els informes alliberats siguin lliurats a persones o entitats concretes o siguin alliberats a Internet (per exemple gràfic de paràmetres epidemiològics)".*

El Projecte afegeix altres consideracions respecte la previsió futura d'avaluar els riscos per a la privacitat, com ara que es farà un informe de risc per a cada projecte. A nivell temporal, es preveu que la valoració del risc d'identificació de persones es farà en dos moments: en la fase de disseny o preparació del projecte, i en la fase de desenvolupament, amb posterioritat a l'avaluació per part del CEIC i del Comitè de gestió de dades personals (Figura 3, pàgina 17, Annex 1), just abans d'alliberar els resultats de les anàlisis de dades. Finalment, s'afegeix que *"aquesta valoració no es farà en el cas de projectes o anàlisis interns de gestió hospitalària, ja que en aquest cas els informes són per a la pròpia institució".*

D'entrada, cal valorar positivament les previsions citades, segons les quals el Projecte preveu la necessitat de detectar possibles riscos per a la privacitat dels afectats, i d'implementar mesures de protecció de la privadesa, en atenció a la informació personal que serà tractada en el Projecte.

La previsió d'introduir una primera valoració en la fase de disseny o preparació del projecte (entenent que es refereix a cada BD-PRO), s'alinea amb el concepte de "privacitat en el disseny" (PbD), segons el qual la perspectiva de la protecció de dades s'hauria d'incorporar des de les fases inicials del disseny de projectes que impliquen tractament de dades –i, amb més motiu, si es tracta de dades sensibles-, concepte que també està present en el projecte de Reglament de Protecció de Dades de la UE. Aquesta voluntat del Projecte, d'incorporar la perspectiva de la protecció de dades des de l'inici, s'ha de valorar positivament.

Ara bé, cal fer avinent que aquestes previsions d'anàlisi de riscos s'haurien d'aplicar en el mateix disseny de la plataforma, abans d'iniciar el tractament de les dades.

Ateses les fortes implicacions per a la privacitat de les persones, que es podrien derivar d'un tractament inadequat d'informació de salut dels afectats, seria recomanable disposar d'una avaluació de l'impacte sobre la privacitat (PIA) sobre la plataforma. L'elaboració d'aquest estudi, que actualment no és preceptiu d'acord amb la normativa vigent en matèria de protecció de dades, s'alinearia amb les previsions del projecte de Reglament de Protecció de Dades de la UE, que actualment s'està tramitant, el qual preveu, entre d'altres, l'elaboració, per part del responsable del tractament, d'una avaluació de l'impacte sobre la privacitat quan es duguin a terme tractaments a gran escala de dades de salut.

Aquesta avaluació hauria d'incloure una descripció general de les operacions de tractament previstes, una avaluació dels riscos per als drets i llibertats dels interessats, les mesures previstes per fer front als riscos identificats, i les garanties, mesures de seguretat i mecanismes destinats a garantir la conformitat amb la normativa de protecció de dades.

En aquest sentit, fem notar que l'AEPD ha publicat una "*Guía para una evaluación de impacto en la protección de datos*", disponible a http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php.

Finalment, s'ha de qüestionar la previsió del Projecte que la valoració de riscos no es farà en el cas de projectes o anàlisis interns de gestió hospitalària, ja que en aquest cas els informes són, segons argumenta el Projecte, per a la pròpia institució.

El fet que la finalitat de generar una BD-PRO sigui l'elaboració d'un informe intern de l'àmbit hospitalari del Grup, si bé pot comportar una reducció de determinats riscos per

a la privacitat de les persones (per la menor difusió que pot tenir, o el flux informatiu més reduït que comporta, en comparació amb altres projectes que tenen per destinataris tercers aliens al Grup), no elimina en absolut els dits riscos.

Per això, no es considera adequat, des de la perspectiva de la protecció de dades que el Projecte descarti realitzar una anàlisi de riscos, quan la finalitat d'una BD-PRO sigui l'elaboració d'informes interns del Grup.

XI

Mesures de seguretat

L'LOPD estableix un règim de protecció reforçat en relació amb determinades tipologies de dades personals, entre d'altres, les dades de salut, que es tradueix, entre d'altres, en l'exigència de l'aplicació de mesures de seguretat de nivell alt (article 9 LOPD i Títol VIII RLOPD).

El Projecte analitzat parteix de la base de l'anonimització de la informació, per bé que, com s'ha assenyalat, no descarta comunicar BD-PRO amb informació codificada i identificable.

Val a dir que la documentació aportada fa esment, en diversos apartats, a mesures de seguretat concretes que corresponen al nivell alt de seguretat, exigible en el cas que ens ocupa.

Ara bé, algunes d'aquestes referències a mesures de seguretat concretes, incloses en la documentació aportada, es fan, en termes generals, en relació amb el tractament de dades que fa el Grup per al compliment de les seves funcions (prestar servei als ciutadans en el context de la salut mental), però no es refereixen, estrictament, al tractament de dades propi i derivat del Projecte analitzat.

Així, en la secció 2.2.1 de l'Annex 1, s'explica que les aplicacions o eines incloses en l'ecosistema informàtic del Projecte (aplicació Ekon Salus, aplicació Aegerus i aplicació d'hospitalització en caché), contenen sistemes de control d'usuaris, basats en la definició de perfils que garanteixen la limitació d'accés a la informació en funció del tipus de professional, la validació d'usuaris o els registres de traçabilitat amb identificació de l'usuari i l'acció realitzada, entre d'altres.

En la documentació aportada s'inclouen altres previsions respecte mesures de seguretat encaminades a garantir la confidencialitat de les dades, com ara les contingudes en el Manual de bones pràctiques (Annex 8), o en la secció 2.2.4 de l'Annex 1. Aquest manual de bones pràctiques està destinat als treballadors del Grup en relació amb el tractament de dades en general, però no, en concret, amb el Projecte.

A això cal afegir l'especial naturalesa i sensibilitat de la informació que serà font d'origen del Projecte, i les característiques dels tractaments i les activitats que implica el Projecte (procediments d'anonimització i codificació d'informació, anàlisi de les finalitats, de la destinació i la difusió que tindrà la informació, anàlisi de riscos, especialment de re-identificació, etc).

Per tot això, cal fer avinent la necessitat de concretar, específicament pel que fa al tractament de dades derivat del Projecte (gestió de la BD-Grup i les BD-PRO), un model integral de mesures de seguretat, acord amb les exigències del Títol VIII del RLOPD. Això, sens perjudici de les previsions que es puguin contenir en els

documents de seguretat dels fitxers implicats en el Projecte (Annexos 6 i 7 en relació amb els fitxers de pacients i de investigació).

Però a més de concretar i implementar les mesures de nivell alt que exigeix el Títol VIII del RLOPD, les característiques del tractament derivat del Projecte aconsellen anar més enllà de l'estricta implementació d'aquestes mesures.

I això, amb independència que a partir d'un determinat moment les dades es puguin trobar codificades o anonimitzades. Tractant-se d'una informació tan sensible com aquesta, els riscos inherents a un eventual risc de re-identificació aconsellen mantenir aquestes mesures al llarg de tota la vida de la informació.

En aquest sentit, amb caràcter general, en relació amb el disseny del Projecte convindria que, com a punt de partida, la seguretat de la informació que el Grup tractarà en el Projecte estigui alineada amb algun dels conjunts de bones pràctiques existents (Tipus ISO27001). Com a mínim, convindria estudiar quines mesures, a nivell de bones pràctiques, implantarà el Grup, i que aquestes s'hauran de basar en la gestió de riscos, que hauran de poder ser certificades per un tercer independent, i que poden ser revisables mitjançant procediments estàndards d'auditoria de seguretat o de sistemes d'informació. A partir d'aquesta base, es podria verificar com s'implanten els requisits en relació amb la protecció de dades de caràcter personal.

Dit això, en particular, cal assenyalar que l'article 96 del RLOPD imposa l'obligació de realitzar auditories en els fitxers i tractaments de dades a partir del nivell mitjà de seguretat.

L'Annex 5 de la documentació aportada inclou còpia d'un escrit referit a un informe d'auditoria que una empresa privada ha realitzat respecte el tractament de dades en els centres del Grup. Ara bé, el Projecte no detalla cap qüestió referida a les auditories enfocades a valorar les particularitats del Projecte que analitzem. En aquest sentit, la implementació del Projecte hauria de comptar amb un model d'auditoria que verifiqui els processos de codificació i d'anonimització, l'eficàcia de les mesures de control del risc de re-identificació dels afectats, etc, en definitiva, que amb el contingut mínim exigit per la normativa (article 96.2 RLOPD), es refereixi, específicament, al tractament i flux informatiu derivat del Projecte. Auditoria que s'hauria de dur a terme no només amb el caràcter biennal previst pel RLOPD, sinó que caldria dur a terme d'una manera continuada. Així, per exemple, es podria establir un sistema d'auditories biennals a càrrec d'entitats externes, complementat amb altres auditories, si escau fetes internament, en lapses de temps inferiors que permetin fer un seguiment continuat del projecte i de l'evolució dels riscos.

Per altra banda, a la secció 2.2.3 de l'Annex 1 es fa referència a que les dades es destruiran un cop el projecte hagi finalitzat i els resultats hagin estat publicats en el mitjà que s'hagués previst. Cal fer notar que la destrucció de la informació no pot quedar condicionada a la publicació. Un cop es pugui donar per acabat el projecte s'haurien de destruir totes les dades.

Finalment, cal fer notar que la previsió continguda en la secció 2.2.4 de l'Annex 1, sobre el control d'accés a les dades, preveu que *"els tercers que tinguin o no tinguin accés a les dades estan obligats a sotmetre's a les mesures de seguretat que el responsable del fitxer consideri necessàries."*

Respecte d'aquesta previsió en particular, convé recordar que l'article 82 RLOPD determina que l'encarregat del tractament ha d'aplicar les mesures de seguretat que correspongui i això amb independència que el responsable ho consideri convenient o

no. La menció a les mesures que el responsable consideri convenients cal entendre-la referida a les mesures addicionals que estableixi el responsable. Convindria aclarir aquest extrem.

Per altra banda, seria bo que també es preveiés en el Projecte la necessitat que les persones o entitats a qui es lliuri una BD-PRO subscriguin un document on es recullin, entre d'altres, els aspectes següents:

a) Deure de confidencialitat
b) No fer accions per re-identificar,
c) Vinculació de la informació lliurada al projecte sol·licitat
d) Obligació de comunicar immediatament al Grup els supòsits en què s'hagi detectat un risc de re-identificació
e) Destrucció de la informació un cop ja no sigui necessària pel projecte i acreditació d'aquest fet davant del Grup. Seria bo en aquest sentit que en la sol·licitud s'indiqués el termini en què l'entitat es compromet a fer-ho.
f) Mesures sancionadores aplicables en cas d'incompliment d'aquestes obligacions

XII

Avaluació per òrgans col·legiats dels aspectes ètics i de privadesa de dades dels projectes

En la consulta es formula la següent pregunta:

Pregunta 6: *"És adequada la proposta de crear un Comitè de Gestió de Dades Personals (secció 2.2.6.2, pàgina 19), que vetlli per l'activitat de la Plataforma* (...)*?"*

La secció 2.2.6 (Annex 1) es refereix a l'Avaluació per òrgans col·legiats dels aspectes ètics i de privadesa de dades dels projectes. Aquesta avaluació, segons s'exposa en el dit Annex 1, es fonamenta i pren com a model el funcionament dels comitès externs dels biobancs (Llei 14/2007, de 3 de juliol, d'Investigació biomèdica, i Reial decret 1716/2011, de 18 de novembre, que estableix els requisits bàsics d'autorització i funcionament dels biobancs).

En concret, el Projecte proposa que els projectes a desenvolupar en la Plataforma siguin avaluats per dos comitès, això és, un Comitè Ètic d'Investigació Clínica (CEIC) i el Comitè de Gestió de Dades Personals (CGDP).

Respecte la intervenció del CEIC, en la secció 2.2.6.1 de l'Annex 1 es preveu que *"els projectes de recerca desenvolupats en el marc de la Plataforma* (...) *hauran de ser avaluats pel CEIC corresponent* (...)". És a dir, sembla que es preveu que tots els projectes han de ser avaluats pel CEIC. Ara bé, en la secció 2.2.3 de l'Annex 1, es preveu que:

"Quan les característiques del projecte de recerca amb persones ho requereixen (Ley 14/2007, de 3 de julio, de Investigación biomédica), el projecte ha de ser aprovat per la Comissió Clínica d'Investigació del Grup i pel Comitè ètic d'investigació clínica (CEIC) local."

Cal aclarir si són tots els projectes, o no, els que han de passar pel CEIC, així com la participació, si escau, en l'avaluació de les peticions d'informació de la Comissió

Clínica d'Investigació del Grup, a la que no es fa referència, al menys de forma clara, en la secció 2.2.6 de l'Annex 1.

A banda de la intervenció del CEIC, la secció 2.2.6.2, proposa crear un comitè interdisciplinari amb diversos especialistes, que vetlli pel bon ús de les dades personals obtingudes en el marc de l'activitat assistencial i supervisi els aspectes ètics vinculats a la recerca amb aquests tipus de dades. S'afegeix que aquest comitè s'ocuparà d'avaluar el risc d'identificació de les persones i el bon ús de les dades en general en cada projecte desenvolupat a la Plataforma.

S'ha de valorar molt positivament tant la previsió de la intervenció d'un CEIC com la creació d'aquest CGDP. Però més enllà de constatar que aquest CGDP s'ocuparà d'avaluar el risc d'identificació i el bon ús de les dades en general, no queda clar com es concreta aquesta avaluació. Com ha quedat dit, el Projecte no concreta, en els seus termes actuals, quin serà el contingut de l'avaluació de la demanda en relació amb cada projecte o BD-PRO. Per tant, més enllà de preveure la intervenció d'un CEIC (la qual també s'hauria d'aclarir), i d'un CGDP, mesures que s'han de valorar positivament, cal dotar de contingut aquestes intervencions.

En aquest sentit, també es fa avinent que no és clara la relació entre els CEIC, el CGDP, la *"unitat administrativa"* i la *"unitat tècnica"* que, segons s'explica en la secció 2.3 i Figura 5 de l'Annex 1, participen també en l'avaluació de les sol·licituds, ni el rol que han de tenir cadascun d'aquests ens en l'avaluació de cada sol·licitud d'informació.

D'acord amb les consideracions fetes en aquests fonaments jurídics en relació amb la consulta plantejada, es fan les següents,

Conclusions

En relació amb les preguntes formulades pel Grup en l'escrit de consulta s'ha de dir el següent:

Pregunta 1: *"La proposta de solucions per a la protecció de les dades personals que exposem en el projecte (secció 2.2, pàgines 6-18) s'ajusta a la legislació vigent?"*

Des de la perspectiva de la protecció de dades, i vista la documentació aportada, resultaria necessari que el Projecte aclareixi o concreti les següents qüestions, en els termes apuntats en aquest informe:

- Els fitxers relacionats amb el Projecte i quines dades contingudes en els fitxers es veuran afectades pel Projecte, tenint en compte el principi de minimització.
- Quines són les finalitats, habilitades en la normativa, que poden fonamentar els projectes o peticions d'informació.
- Si la informació es tractarà de manera anonimitzada de manera que no permeti identificar les persones afectades o en base al consentiment dels pacients afectats.
-Quins poden ser els destinataris de la informació, i per a quina finalitat concreta.
- Quina difusió es pot fer de la informació tractada, en cada cas (difusió a tercers determinats, en obert, o limitada al Grup).
- Que es clarifiqui l'exercici dels drets ARCO i de l'opt-out, en relació amb el Projecte.
- Que es concretin les qüestions relatives al procediment tècnic d'anonimització a què es refereixen els Fonaments Jurídics IX i X d'aquest informe.
- Que s'estableixi un model integral de mesures de seguretat de nivell alt i, si escau, un model de bones pràctiques, en relació, específicament, amb el tractament de dades derivat del Projecte.

Pregunta 2: *"És correcte allotjar la base de dades primària amb la identificació de les persones dissociada* (BD-G) *al FITXER PACIENTS de l'entorn assistencial (secció 2.2.1.2, pàgina 10) i les bases de dades anonimitzades, específiques de cada projecte, llestes per fer les anàlisis i que anomenem BD-PRO al Fitxer recerca (secció 2.2.3, pàgina 12), ambdós ja donats d'alta a l'AEPD. Si no és correcte, caldria crear i donar d'alta un nou fitxer per a aquesta activitat? Si la resposta fos afirmativa, on caldria registrar-lo: a l'AEPD o a l'APDCAT?".*

Vist el contingut dels fitxers de "pacients" i de "recerca" dels centres del Grup, i atès el tractament que s'ha de realitzar en base al Projecte, es recomana que siguin els fitxers de "Recerca" de cadascuna de les entitats responsables de les dades els que incorporin (o "allotgin", en els termes de la consulta), la base de dades primària amb la identificació de les persones (BD-Grup). La informació resultant d'un procés d'anonimització que no faci identificables les persones a les quals fa referència no està sotmesa a l'obligació de figurar un fitxer.

Pregunta 3: *"La plataforma que proposem treballarà amb dades anonimitzades però en casos excepcionals de projectes que ho requerissin i sempre sense sortir dels nostres servidors, seria correcte treballar amb dades dissociades (codificades reversiblement i identificables?) (secció 2.2.3, pàgina 13).*

El Projecte hauria d'articular un procediment adequat d'anàlisi de les peticions de BD-PRO per part de tercers destinataris, ja siguin del propi Grup o externs. Aquest procediment d'anàlisi hauria de preveure un decalatge de peticions en tres nivells diferenciats, prioritzant les peticions d'informació anonimitzada o dissociada que no ha de permetre, en cap cas, la re-identificació del subjecte, en els termes exposats al Fonament Jurídic IX d'aquest informe.

Pregunta 4: *"Està previst que les dades siguin estructurades i analitzades per professionals contractats per l'entitat* (...), *però si en algun cas fos necessària la participació d'un tercer, aliè a la nostra empresa, els mecanismes previstos en la nostra proposta (secció 2.2.4, pàgines 14-16), són suficients per garantir la seguretat de les dades?"*

El responsable del fitxer o tractament hauria d'especificar, en el context del Projecte, com es durà a terme el tractament de dades relacionat amb el procés de codificació i anonimització, per part de qui (personal intern o extern, en quins casos i amb quin grau de participació en cada fase del procés) i, si escau, formalitzar prèviament a l'inici del tractament, el contracte o contractes d'encàrrec del tractament que siguin necessaris.

Pregunta 5: *"La avaluació del risc de pèrdua de la privadesa de dades personals (secció 2.2.5 pàgina 17-19) consistent en l'aplicació d'un protocol basat en l'execució d'eines específiques en dos punts: en el procés de disseny del projecte i abans del lliurament o publicació dels resultats, és adequada?"*

Sens perjudici de valorar positivament les previsions que conté el Projecte, que s'haurien d'aplicar a tots els projectes, seria recomanable incorporar una avaluació d'impacte sobre la privacitat (PIA) de la Plataforma, que hauria d'incloure una descripció general de les operacions de tractament previstes, una avaluació dels riscos per als drets i llibertats dels interessats, les mesures previstes per fer front als

riscos identificats, i les garanties, mesures de seguretat i mecanismes destinats a garantir la conformitat amb la normativa de protecció de dades.

Pregunta 6: *"És adequada la proposta de crear un Comitè de Gestió de Dades Personals (secció 2.2.6.2, pàgina 19), que vetlli per l'activitat de la Plataforma* (...) *?"*

Sens perjudici que la proposta de crear un Comitè de Gestió de Dades personal és adequada, convindria concretar els termes de l'avaluació que realitzarà aquest Comitè, i la participació del CEIC.

Barcelona, 23 de juliol de 2015