CNS 34/2014

Dictamen en relació amb la consulta plantejada per una entitat de dret públic en relació amb el model de gestió i de serveis per donar valor a la informació del sistema sanitari català en el marc de les polítiques públiques (en endavant VISC+)

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'una entitat de dret públic (en endavant, l'entitat), en el qual es demana que l'Autoritat valori l'adequació de les mesures de seguretat que s'aplicaran sobre les dades incloses en l'abast del contracte VISC+ a la legislació en matèria de protecció de dades, que es descriuen en els documents que s'adjunten a la consulta.

En concret, s'adjunta còpia del Document Administratiu de solució final VISC+ (en endavant, DA), del Document Tècnic de solució final VISC+ (en endavant, DT), i del Document de procediment per a la cessió de dades personals anonimitzades de salut a l'Adjudicatari de VISC+ per recerca mèdica i avaluació, que inclou, com a annexos, els Estatuts de l'entitat (annex 1), el document d'encàrrec de gestió (annex 2), i el document sobre el procediment d'anonimització (annex 3).

Analitzada la consulta i la documentació que l'acompanya, vistos els informes del Coordinador d'Auditoria i Seguretat de la Informació de l'Autoritat, i de l'Assessoria Jurídica emeto el següent dictamen

I

(...)

II

Objecte de la consulta

A través de la consulta formulada, l'entitat exposa que està licitant un contracte de col·laboració publico privada per a la implantació i l'operació d'un model de gestió de serveis per donar valor a la informació del sistema sanitari català en el marc de les polítiques públiques (VISC+). S'afegeix que en aquest marc contractual es regulen els mecanismes i processos de seguretat que seran aplicables sobre les dades incloses en l'abast del contracte, i que han d'assegurar el compliment de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD).

En relació amb el projecte VISC+, l'entitat sol·licita informe sobre l'adequació de les mesures de seguretat que s'aplicaran sobre les dades incloses en l'objecte del contracte VISC+ a la legislació en matèria de protecció de dades.

Pel que fa l'abast d'aquest dictamen, tal i com es planteja a la consulta, es centrarà en aspectes relatius a les mesures de seguretat, però les consideracions sobre aquests aspectes no es pot desvincular dels principis i obligacions derivats de la normativa de protecció de dades. Per això, i a partir de la documentació aportada, també s'analitzaran, amb caràcter previ algunes qüestions generals sobre l'abast les característiques del projecte i les garanties necessàries per al compliment de la normativa de protecció de dades.

Per altra banda, aquest dictamen té per objecte l'anàlisi del model de seguretat i anonimització de les dades que es descriu bàsicament a l'Annex 1 del DT, relatiu al

"Model de seguretat, disponibilitat i ús de les dades", per comprovar si s'adequa a la normativa de protecció de dades i fer aquelles consideracions que, des de la perspectiva de la protecció de dades, es considerin pertinents per millorar-lo. Cal deixar clar però que l'objecte d'aquest dictamen no consisteix en validar un determinat model de seguretat, qüestió que per altra banda no seria possible atesa la manca de concreció de diferents aspectes relacionats amb la seguretat. La validació del sistema de seguretat és quelcom que només es pot dur a terme després d'un acurat procediment d'auditoria que s'ha de dur a la pràctica un cop estigui implementat. Per això, en el punt 3.1 del DT, caldria referir-se a que el model de l'Annex 1 del DT ha estat objecte de Dictamen de l'Autoritat, i no de validació. En qualsevol cas, es valora positivament la previsió que les futures modificacions del Model de seguretat, disponibilitat i ús de les dades, del dit Annex 1, també es sotmetran al parer de l'Autoritat.

III

Descripció del projecte

La consulta plantejada per l'entitat, porta causa del contracte de col·laboració publico privada pel disseny, implantació i operació d'un model de gestió i serveis per a donar valor a la informació del sistema sanitari català.

L'entitat que formula la consulta és una entitat de dret públic de la Generalitat sotmesa a l'ordenament jurídic privat, adscrita al departament competent en matèria de salut de la Generalitat de Catalunya, amb personalitat jurídica pròpia, autonomia administrativa i financera i plena capacitat d'obrar per al compliment dels seus objectius i les seves funcions, i actua, en el marc de les funcions que li atribueixen els seus Estatuts, sota les directrius del dit departament, el qual exerceix el control d'eficàcia i eficiència sobre la seva activitat. Són objectius de l'entitat generar el coneixement rellevant per contribuir a la millora de la qualitat, seguretat i sostenibilitat del sistema de salut de Catalunya que facilitin la presa de decisions a la ciutadania, als professionals i als gestors de l'àmbit de la salut, i als òrgans responsables de la planificació en salut, així com facilitar la implicació dels professionals sanitaris en el sistema i la seva coresponsabilitat en la consecució de les finalitats comunes i la qualitat de l'atenció. Entre d'altres funcions, correspon a l'entitat definir, impulsar i desplegar l'estratègia del sistema d'informació i les tecnologies de la informació i comunicació del sistema de salut de responsabilitat pública, així com dur a terme la gestió i el manteniment dels elements comuns i/o unificats del sistema d'informació del sistema sanitari integral d'utilització pública de Catalunya (SISCAT) i la seva explotació i rendibilització garantint, d'acord amb les directrius del departament competent en matèria de salut, la disponibilitat de la informació del sistema sanitari de Catalunya, fent-la accessible i interoperable al servei d'una assistència sanitària de qualitat, d'acord amb la política corporativa de la Generalitat de Catalunya en matèria de telecomunicacions i tecnologies de la informació, segons els Estatuts de l'entitat.

El Pla de Govern 2013-2016, va incloure el "Projecte VISC+ (Valorització d'Informació del Sistema Sanitari Català), entre els projectes d'interès per a l'Eix de Cohesió social i serveis d'interès públic, inclòs en el dit Pla de Govern.

S'ha de dir que en elaborar aquest dictamen no s'ha disposat d'una memòria global que descrigui d'una manera detallada les necessitats, les alternatives disponibles i les característiques (fluxes d'informació, característiques del sistema d'anonimització dades, col·lectius concrets afectats, etc.) i els beneficis de l'opció escollida. Només es disposa de diversos documents -descrits a l'apartat d'antecedents d'aquest dictamen- que, des de perspectives diferents, descriuen diferents aspectes del projecte. Així,

alguns dels documents aportats sembla que formen part de la documentació contractual de la relació entre entitat i l'Adjudicatari (DA i DT), altres es refereixen a la relació entre els responsables del fitxer i l'entitat (Encàrrec de serveis) i altres no resulta clara quina naturalesa tenen (Document sobre procediment per a la cessió).

S'ha de dir també que, ateses les fortes implicacions per a la privacitat de les persones i per als altres drets que es podrien veure afectats en cas d'un tractament inadequat d'una informació tan sensible com la que s'inclou en el projecte, **seria recomanable disposar d'una avaluació de l'impacte sobre la privacitat** que pot tenir aquesta iniciativa. 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 europeu de protecció de dades 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, i les garanties, mesures de seguretat i mecanismes destinats a garantir la conformitat amb la normativa de protecció de dades. En aquest sentit, l'Agència Espanyola de Protecció de Dades ha publicat recentment una "*Guia para una evaluación de impacto en la protección de datos*", disponible a http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php .

En síntesi, pel que es desprèn dels diferents documents aportats, l'esquema del Projecte VISC+ és el següent:

La constitució d'un encàrrec del tractament (article 12 LOPD) entre el Departament de Salut, el Servei Català de la SALUT (CATSALUT) i l'Institut Català de la Salut (ICS), com a responsables dels fitxers de dades implicats en el Projecte, i l'entitat, com a prestador de serveis i encarregat del tractament, que ha de permetre que l'entitat procedeixi a anonimitzar la informació per tal que l'Adjudicatari, a qui se li comunicaria la informació, la faciliti a tercers (clients o usuaris finals).

També es preveu que l'entitat pugui cedir directament a tercers dades personals no anonimitzades, prèvia comprovació, per part de l'entitat, que el cessionari disposa dels consentiments corresponents dels afectats i d'una auditoria de compliment de l'LOPD.

L'Adjudicatari s'haurà d'encarregar de definir, construir i posar en marxa un catàleg de serveis útil, eficient, competitiu i innovador, i contrastar les necessitats del mercat i els clients finals del projecte, així com de definir un pla de difusió i de comercialització, canalitzant de manera adequada la demanda del mercat nacional i internacional. També haurà d'executar altres projectes o iniciatives relacionades amb VISC+, i haurà de crear un centre de competència en analítica en dades de salut, les funcions i composició del qual es descriuen en l'apartat 3.4.1 del DT.

El Projecte articula un doble procediment de cessió de dades personals:

a) Procediment per a la cessió de dades anonimitzades de salut a l'Adjudicatari per recerca mèdica i avaluació (punt 1 del Document *"Procediment per a la cessió de dades(...)",* que alhora facilitaria les dades als clients finals.

b) Procediment per a la cessió de dades de salut no anonimitzades per recerca mèdica i avaluació a l'usuari final (punt 2 del mateix Document). Aquest segon procediment té la particularitat que les dades serien cedides directament a l'usuari final per part de l'entitat.

Si bé no tots (doncs també es preveu tractar fitxers com ara el Registre sanitari d'empreses i indústries, o el Registre de personal docent, a tall d'exemple), la majoria dels fitxers afectats pel Projecte VISC+ contenen dades de salut. Si ens atenim a l'abast de les dades que l'entitat preveu posar a disposició de l'Adjudicatari tan inicialment com en incorporacions futures (punt 2.2.2 del DT) és clar que les dades de salut conformen la principal font d'informació del Projecte analitzat.

L'LOPD estableix un règim de protecció reforçat en relació amb determinades tipologies de dades personals, entre d'altres, les dades de salut, entenent per 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).

Atès que el Projecte VISC+ té per objectiu desenvolupar un model de gestió que permeti donar valor a la informació que genera el sistema sanitari català, en la mesura que això implicarà, principalment, el tractament de dades de salut, caldrà atendre a aquest règim de protecció previst a l'LOPD per a les dades sensibles, i a les previsions de la normativa sectorial aplicable. Les dades que conformen la HC es recullen per a realitzar el tractament mèdic que requereix el pacient, principalment i, si escau, per a d'altres usos o finalitats, previstos 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. D'acord amb aquesta normativa per tractar les dades que consten a la HC, serà necessari el consentiment del seu titular, llevat que concorri alguna de les excepcions previstes a la llei o que s'anonimitzi la informació (articles 16.3 de la Llei 41/2002 i 11.3 de la Llei 21/2000).

IV

Sobre la informació que es tractarà en el projecte Visc+

Des de la perspectiva de la protecció de dades 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'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.

Aquest principi de proporcionalitat en un projecte com el que ens ocupa desplegarà els seus efectes tant des del punt de vista dels fitxers que han de formar part del projecte, com de la informació que es podrà comunicar als clients finals.

Pel que fa als fitxers afectats pel Projecte VISC+, segons el que es descriu al document relatiu a l'encàrrec de serveis, són fitxers responsabilitat del Departament de Salut (19 fitxers), del CATSALUT(10 fitxers) i l'ICS (3 fitxers), que l'entitat podrà tractar en base a un contracte d'encàrrec del tractament al que ens referirem més endavant. També s'explicita, en el Document relatiu a l'encàrrec del tractament -*"Encàrrec de serveis d'anonimització (...)"-,* determinats fitxers que queden fora de l'abast del projecte.

Ara bé, s'ha de fer notar que segons l'apartat 2.2.2 del DT, l'entitat posarà a l'abast de l'Adjudicatari *"tota la informació anonimitzada"* que es generi en el SISCAT. Hi ha doncs una discordança que hauria de portar a rectificar l'apartat 2.2.2.

En qualsevol cas, pel que fa als fitxers afectats, cal valorar positivament que, malgrat el gran nombre de fitxers esmentats en el Document d'encàrrec de serveis d'anonimització, el DT prevegi un "*abast inicial*" limitat de les dades que estaran disponibles en un primer moment del Projecte (apartat 2.2.2.1 del DT). En aquesta línia l'apartat 5.2.1 del DT preveu que "*En la Fase 1 del projecte es consensuaran quines fonts de dades, d'entre les incloses en l'abast inicial, es posaran a disposició de l'Adjudicatari una vegada s'hagi construït i validat el procés d'anonimització d'acord amb el model de seguretat* (...)". D'això sembla poder inferir-se que, en atenció als resultats que es puguin obtenir inicialment, la incorporació de nous fitxers i de noves dades tindrà en compte l'experiència assolida a l'hora de valorar-ne la viabilitat i la proporcionalitat.

Però aquest principi, a banda de regir en el moment de la posada a disposició de l'entitat dels fitxers afectats, s'ha de tenir present també en el moment de la comunicació de les dades concretes necessàries per a les finalitats que pretenguin dur a terme els clients finals. Especialment si es tracta de dades personals, però també si es tracta de dades anonimitzades.

La informació lliurada als clients finals seria, en bona part, dades de salut dels afectats, contingudes en la HC – o dades anonimitzades obtingudes a partir d'aquestes-. Des de la perspectiva del principi de qualitat, cal tenir en compte que el contingut de la HC, definit en la normativa (fonamentalment article 15.2 Llei 41/2002, i article 10 Llei 21/2000) 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. Tenint en compte això, quan es dugui a terme la cessió i quan s'articuli el corresponent consentiment informat, cal limitar 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 client final.

Això, que és essencial en el cas de les dades personals no anonimitzades, és rellevant també per al cas de les dades anonimitzades, perquè no s'ha de perdre de vista que en l'entorn del *big data* l'encreuament d'informació obtinguda d'orígens diversos, fins i tot si ha estat anonimitzada pot acabar fent identificable una persona. Per això, per intentar reduir en aquests casos els riscos de re-identificació també seria necessari limitar les dades comunicades a les mínimes indispensables per a assolir la finalitat pretesa pel client final. I dins de les dades anonimitzades, és encara més rellevant en

aquelles que s'ofereixen en obert. Per això, atesos els riscos inherents, cal ser molt restrictiu amb la informació de salut que s'ofereixi en obert, llevat que s'ofereixi amb nivells d'agregació sobradament amplis.

Quan l'apartat 3.2.1del DT es refereix a les dades obertes no es concreta quines seran aquestes dades ni els criteris i el procediment que es seguiran per decidir quines dades hauran d'estar accessibles en obert. Seria convenient que ja des d'aquesta fase de disseny del projecte s'aclarissin aquests extrems.

En qualsevol cas, aquest és l'únic supòsit (serveis de dades obertes) en què el DT examinat explicita que es treballarà amb "dades anonimitzades", mentre que en la resta de serveis identificats no s'explicita si els clients finals podrien rebre i tractar informació anonimitzada o dades personals no anonimitzades.

El principi de minimització en el tractament de les dades personals, del qual es deriva que si una finalitat es pot assolir sense necessitat de tractar dades personals, s'ha d'optar per aquesta possibilitat, s'hauria d'incorporar d'una forma més visible en el projecte, de manera que –amb independència que es pugui aconseguir el consentiment de les persones afectades- només es basi un determinat tractament en informació de persones identificades en aquells casos que resulti imprescindible.

Cal acotar en quins casos pot ser, no ja necessari, sinó imprescindible, treballar amb dades no anonimitzades. Com s'ha vist, el projecte es refereix a la comercialització d'informes de diversa naturalesa, en relació amb alguns dels quals només s'esmenta que responen "a necessitats específiques" del sol·licitant, sense més concreció, respecte quin tipus i volum d'informació agregada o no agregada poden requerir.

V

Sobre la finalitat del tractament

Tal com hem vist, l'article 4.1 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.*"

I a més, l'apartat 2 del mateix article 4 afegeix:

> *2. 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.

En la documentació aportada es fa esment a que l'objectiu del Projecte és donar valor a la informació generada pel sistema sanitari català. Més en concret, es fa referència a la finalitat de "recerca mèdica i avaluació" (Document d'encàrrec de serveis, Document de Procediment de cessió de dades, i DT).

Ara bé, pel que fa a les finalitats concretes per a les quals els clients finals poden sol·licitar les dades, hi ha alguna discordança:

En l'Annex 1 del DT, referit al *"Model de seguretat, disponibilitat i ús de les dades",* s'exposa el següent: *"L'Adjudicatari només podrà utilitzar les dades, tant si són personals com anonimitzades, per alguna de les finalitats següents: estudis de recerca mèdica, estudis d'epidemiologia, docència, assistència sanitària, administració i gestió de centres sanitaris, inspecció per part de l'administració sanitària, gestió sanitària per l'administració sanitària o estadística oficial declarada al Pla Estadístic.".* I això sembla que abastaria tant els supòsits de dades obertes com els altres en què es sol·liciti la informació per l'usuari final, segons les diferents modalitats previstes.

També en el Document *"Procediment per a la cessió de dades personals (...)"*, en l'apartat 1.3.1 *"Supervisió de les sol·licituds dels usuaris a l'Adjudicatari",* i en l'apartat 2 relatiu a la cessió de dades no anonimitzades, es fa una referència general a totes les finalitats d'ús de la HC anàloga a l'Annex 1 del DT.

En canvi, en els encapçalaments dels apartats relatius als procediments 1 i 2 es fa referència només a "*recerca mèdica i avaluació*". I en el Document d'encàrrec de serveis d'anonimització, que s'adjunta, i al que després ens referirem amb més detall, es preveu que la finalitat del servei és la *"Gestió sanitària per l'administració sanitària; Estudis d'epidemiologia; Recerca".*

És a dir, es constata que **les referències a les finalitats del projecte no sempre coincideixen en els diferents apartats de la documentació aportada**. Així, se'n fa una referència, en alguns documents, acotada a la recerca mèdica i avaluació, i en uns altres, a la pràctica totalitat de les finalitats descrites en la normativa sectorial per a les dades de la HC.

A banda d'això, s'han de fer notar dues precisions:

L'Annex 1 del DT es refereix a que "*l'Adjudicatari només podrà utilitzar les dades*..." amb alguna d'aquestes finalitats. En realitat però, l'ús principal que en faci l'adjudicatari no sembla que hagi de ser aquest, sinó posar-les a disposició de tercers segons les diferents modalitats previstes, per a que siguin aquests qui duguin a terme aquestes finalitats.

Per altra banda, en el cas que el client final sol·liciti les dades, es pot comprovar en aquest tràmit la finalitat prevista, per tal que encaixi en alguna d'aquestes finalitats. Però en canvi, quan es tracti de dades obertes, l'anàlisi de la finalitat cal fer-lo en el moment de la prèvia posada a disposició i, en conseqüència, limitar la publicació de dades en obert a aquelles que des del punt de vista de les finalitats esmentades resultin imprescindibles.

En segon lloc, segons la documentació aportada, les finalitats del tractament de dades en el context del Projecte VISC+ abasten des de l'assistència sanitària (article 11.1 Llei 21/2000), a funcions d'inspecció (article 11.5 Llei 21/2000), a tasques d'administració de centres sanitaris (article 11.4 Llei 21/2000), i a finalitats epidemiològiques i d'investigació o docència (article 11.3 Llei 21/2000). Si ens atenim a les previsions de la normativa sectorial (Lleis 41/2002 i 21/2000), algunes d'aquestes finalitats poden no requerir el consentiment dels titulars, mentre que d'altres (principalment, als efectes que ens ocupen, la finalitat d'investigació o recerca mèdica), requereixen ineludiblement del consentiment dels afectats llevat que es procedeixi a l'anonimització, en uns termes que assegurin la protecció de la privacitat dels afectats.

Per això cal fer avinent que resulten confuses algunes de les previsions de la documentació aportada, en el sentit que no queda clar si el tractament de dades personals del Projecte VISC+ ha de tenir per finalitat, principalment o, fins i tot,

únicament, la investigació o "recerca mèdica" (com semblaria deduir-se d'alguns dels Documents citats), o si es pot produir un tractament i cessió als "clients finals" per, en definitiva, la pràctica totalitat de les finalitats o usos de la HC descrits en l'article 11 de la Llei 21/2000 (i article 16 de la Llei 21/2000). Tampoc no queda clara quina és la finalitat d"avaluació" a què fan referència alguns dels Documents aportats, com ha quedat dit. En relació amb aquesta finalitat d'avaluació, es recomana que es concreti la referència, en atenció als usos de la HC previstos en la Llei 21/2000.

Caldria explicitar, en la mesura del possible, que els "clients finals" només podran tractar la informació personal (singularment, informació no anonimitzada) necessària, en atenció a la finalitat per a la qual l'hagin sol·licitat, i tenint en compte les limitacions que es puguin derivar de la normativa aplicable.

En aquest sentit, cal fer avinent **que es troba a faltar, en el conjunt de documentació aportada, una connexió clara entre "client final", la finalitat a complir, la concreció de la informació a què podria tenir accés, i si aquesta informació ha de ser anonimitzada o pot comportar una cessió de dades personals.**

Sobre això, cal fer notar que en el DT s'identifiquen una sèrie de serveis o productes, que, a proposta de l'entitat, l'Adjudicatari haurà de configurar. En concret:

- Serveis de dades obertes: publicació sense cost de subsets (subconjunts) de dades anonimitzades.
- Serveis de dades no obertes: comercialització de subsets de dades per una finalitat de recerca concreta. Es destinen a usuaris que disposin de subvencions, fons competitius o que hagin passat un Comitè ètic d'investigació.
- Serveis de llicenciament, per explotació i anàlisi de les dades incloses a l'abast del contracte.
- Serveis d'informes estàndard: comercialització d'informes d'anàlisi i avaluació, basats en les dades incloses en l'abast del present contracte.
- Serveis d'informes ad-hoc, adaptats a necessitats específiques del sol·licitant.
- Serveis d'optimització de la gestió de serveis sanitaris o de pràctica clínica.
- Altres serveis Ad-hoc.

D'entrada, es preveuen serveis de dades obertes ("*open data*"), és a dir, subconjunts de dades que es posen lliurement a disposició de tothom per a la seva reutilització tant per a finalitats comercials com no comercials (segons definició de la Comunicació de la Comissió Europea COM(2014)442 final, *"Hacia una economía de los datos próspera").* En aquest context, i amb l'evolució que s'està produint en l'àmbit del big data, en funció del volum de dades que siguin posades a disposició de qualsevol persona (l'apartat 3.2.2 del DT es refereix tant a ciutadans com a indústria o institucions privades en l'àmbit de les ciències de la vida, però en realitat pot ser qualsevol persona o empresa) 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 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).

A això cal afegir l'àmplia tipologia de clients identificats en el Projecte (apartat 3.2.2 *"Gestió de clients",* del DT), que inclouen agents del sistema sanitari integral d'utilització pública de Catalunya (SISCAT); investigadors; indústria o institucions privades en l'àmbit de les ciències de la vida; ciutadania (persones físiques,

associacions de ciutadans, de pacients, empreses especialitzades o amb interès en l'ús i re-ús de les dades, i "altres destinataris".

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 –que es pot consultar al web www.apd.cat-, **l'exigència de legitimitat**, present en relació amb qualsevol tractament de dades, ha de ser més estricta en casos en què es preveu el tractament de dades sensibles, com és el cas que ens ocupa.

A tall d'exemple, tenint en compte la normativa aplicable, els usos i finalitats de la HC, i vista la tipologia de clients finals de la informació a tractar, que pot ser, insistim, segons el Projecte, informació personal no anonimitzada, des de la perspectiva de la protecció de dades i dels usos admesos per a la HC, pot ser difícilment assumible que una associació de ciutadans o determinades empreses, hagin de poder accedir, a través del Projecte, a informació personal sensible no anonimitzada, independentment que es vehiculi a través del consentiment. Per contra, si els clients finals són investigadors i requereixen les dades per a finalitats de recerca (article 11.3 Llei 21/2000), en alguns casos sí podria ser necessari accedir i tractar informació no anonimitzada, si es disposa dels necessaris consentiments, si bé, en d'altres casos, es podrà dur a terme la investigació amb informació agregada.

Contràriament, la normativa preveu determinades finalitats que han de permetre l'accés a informació continguda en la HC, sense consentiment. A tall d'exemple, segons l'article 11.5 de la Llei 21/2000, es preveu l'accés a les HC per a funcions d'inspecció, acotat al personal al servei de l'Administració sanitària.

Per tot això, atesa la casuística àmplia i diversa que es pot donar en relació amb els clients potencials, les finalitats previstes, els serveis identificats, i els fitxers que serien font d'informació en el context del Projecte VISC+, i sens perjudici que en la Documentació aportada es faci referència a la necessitat de consentiment dels afectats en determinats supòsits, des de la perspectiva de la protecció de dades, **seria convenient una major claredat i concreció en el Projecte VISC+**, **respecte quins serveis i tipologies de clients poden arribar a requerir la utilització d'informació personal sensible no anonimitzada, i quins no, i per a quina finalitat concreta.**

VI

Règim de comunicació de dades personals

Pel que fa al règim de comunicació de dades personals, l'article 11 de l'LOPD disposa el següent:

> *"1. Les dades de caràcter personal objecte del tractament només poden ser comunicades a un tercer per al compliment de finalitats directament relacionades amb les funcions legítimes del cedent i del cessionari amb el consentiment previ de l'interessat.*
> *2. El consentiment que exigeix l'apartat anterior no és necessari:*
> *a) Quan la cessió està autoritzada en una llei.*
> *(...)".*

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.

Com s'ha apuntat, el Projecte VISC+ s'emmarcaria principalment en la finalitat de recerca, si bé la documentació aportada fa referència, també, a d'altres finalitats. Atès que la informació objecte de tractament (inclosa en els diferents fitxers descrits) és informació sensible, i pot provenir en bona part de la HC, als efectes de la previsió de l'article 11.2.a) LOPD cal tenir en compte les previsions de la normativa sectorial.

Segons disposen els articles 16.3 de la Llei 41/2002, i 11.3 de la Llei 21/2000, l'accés a la HC amb finalitats d'investigació, entre d'altres, requereix el consentiment exprés dels titulars a menys que les dades es tractin de forma anonimitzada en els termes previstos en la normativa citada (Llei 41/2002 i Llei 21/2000).

El Projecte VISC+ comporta, en part, l'accés dels clients finals a dades anonimitzades –Apartat 1. del Document *"Procediment per a la cessió de dades (...)"*-. Ara bé, també es preveu la cessió a l'usuari final de dades personals de salut que no han estat anonimitzades per recerca mèdica i avaluació. En aquest darrer supòsit caldrà disposar del consentiment informat dels titulars de les dades, per aplicació de la normativa sectorial citada.

L'article 5.1.d) del RLOPD defineix el consentiment com "qualsevol manifestació de voluntat, lliure, inequívoca, específica i informada, mitjançant la qual l'interessat consent el tractament de dades personals que el concerneixen."

En relació, concretament, amb la cessió de dades personals, l'article 12.2 del RLOPD disposa que:

> *"Quan se sol·liciti el consentiment de l'afectat per a la cessió de les seves dades, ha de ser informat de manera que conegui inequívocament la finalitat a què es destinen les dades respecte de la comunicació de les quals se sol·licita el consentiment i el tipus d'activitat que porta a terme el cessionari. En cas contrari, el consentiment és nul."*

Segons disposa l'article 11.3 de l'LOPD:

> *"És nul el consentiment per a la comunicació de les dades de caràcter personal a un tercer quan la informació que es proporcioni a l'interessat no li permeti conèixer la finalitat a què destinen les dades la comunicació de les quals s'autoritza o el tipus d'activitat del receptor de la comunicació."*

Pel que fa, en canvi, a la cessió de dades sense cap dada que permeti la identificació de l'afectat, es tractaria d'una cessió de dades anonimitzades, que ja no requeriria del consentiment dels afectats, atesa la previsió dels articles 11.6 LOPD, 16.3 de la Llei 41/2002 i 11.3 de la Llei 21/2000, citades. Per aplicació de les lleis citades d'autonomia del pacient, l'anonimització de les dades de la HC habilita la comunicació de la informació per a finalitats d'investigació o recerca, de manera que, estrictament, el consentiment del pacient ja no seria necessari.

En aquest punt, recordem que el Considerant 26 de la Directiva 95/46/CE, de protecció de dades personals, disposa que els principis de la protecció s'hauran d'aplicar a qualsevol informació relativa a una persona identificada o identificable, i afegeix que, per determinar si una persona és identificable cal considerar el conjunt dels mitjans que pugui utilitzar raonablement el responsable del tractament o qualsevol altra persona, per identificar aquesta persona; que els principis de la protecció no s'aplicaran a aquelles dades fetes anònimes de manera que ja no sigui possible identificar l'interessat.

Segons l'article 2.a) de la Directiva citada, són "dades personals" tota informació sobre una persona física identificada o identificable, i es considera identificable tota persona

la identitat de la qual es pugui determinar, directament o indirectament, en particular mitjançant un número d'identificació o un o diversos elements específics, característics de la seva identitat física, fisiològica, psíquica, econòmica, cultural o social.

Ja avancem que el procediment de dissociació de la informació de salut que es pugui contenir en els fitxers afectats pel Projecte VISC+, 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"* (art. 3.f) LOPD) haurà de ser adequat, per tal d'assegurar que es cedeixen *"dades dissociades"* (art. 5.1.e) RLOPD), és a dir, dades que no permeten la identificació de l'afectat.

Per això no sembla que pugui ser admissible una previsió com la continguda a l'apartat 3.2.3 del DT. A la pàgina 15 d'aquest document s'afirma el següent:

"*En cas que la petició del client es correspongui a l'accés a un volum de dades anonimitzades que impliqui un risc de desanonimització /personalització d'aquestes dades, serà necessari que (l'entitat), a través del comité de direcció, avaluï i autoritzi aquesta sol·licitud per tal de donar compliment a la LOPD*."

En el cas que existeixi el risc que s'esmenta en aquest paràgraf no sembla que el comitè de direcció pugui autoritzar la petició. **Si existeix un risc de re-identificació, caldrà denegar la sol·licitud o introduir les garanties suficients per fer desaparèixer aquest risc**. Observació aquesta que es pot traslladar també a l'apartat 1.3.2 del Document relatiu al procediment, on es recull aquesta previsió (pàg .7)

Aquestes mateixes consideracions són extensibles a la possibilitat prevista a l'apartat "Disponibilitat de les dades" de l'Annex 1, en què es requeriria autorització de l'entitat així com justificació per l'adjudicatari que la petició es correspon a una necessitat concreta.

Sens perjudici de les consideracions que es puguin fer més endavant, en relació amb els procediments de dissociació o anonimització que s'hagin de dur a terme en el context del Projecte VISC+, resulten d'especial interès el Dictamen del Grup de Treball de l'Article 29 (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.

Fetes aquestes consideracions generals, a continuació es farà referència específica a diverses previsions de la Documentació aportada, relativa al Projecte VISC+.

VII

Responsabilitat i propietat de la informació

En relació amb l'abast del contracte (apartat 5 del DA), es preveu que l'Adjudicatari ostentarà sobre la informació tractada un dret d'ús, tractament, agregació i explotació vinculat a la comercialització dels productes i serveis VISC+, i que l'Adjudicatari *"no ostenta la propietat ni cap dret il·limitat sobre les dades, essent responsable davant aquesta, les autoritats competents i tercers del compliment de la normativa aplicable al tractament de dades de caràcter personal."*

A efectes de claredat, i per tal de deixar constància que les possibles responsabilitats de l'adjudicatari en relació amb el tractament de dades personals no desvirtua les que corresponguin a l'entitat o als diferents responsables (article 3.d) LOPD) dels fitxers de

dades (article 3.b) LOPD) que són font d'origen de la informació tractada, seria bo afegir una referència a que la responsabilitat de l'Adjudicatari és sens perjudici de la que pugui correspondre a l'entitat o als responsables dels dits fitxers.

En qualsevol cas, vistes les mencions fetes a la propietat sobre les dades (en aquest apartat 5 del DA, entre d'altres), convé recordar que la titularitat d'una dada personal (que no la propietat), correspon sempre a la persona física (article 3.e) LOPD).

Per altra banda, la clàusula 39 del DA es refereix, a l'accés a "*dades de (l'entitat)*". Seria més clar referir-se a les *"dades que (l'entitat) cedeix a l'Adjudicatari",* doncs les dades personals que, anonimitzades o no, puguin ser objecte de cessió als efectes del compliment del contracte, no són, des de la perspectiva de l'LOPD, de l'entitat, sinó que la seva titularitat pertany sempre a la persona física afectada. Fem extensiva aquesta consideració a la resta de mencions, de la clàusula 39, a dades de l'entitat i del Departament de Salut, en el sentit que seria més ajustat a l'LOPD referir-se a les dades dels fitxers responsabilitat de l'entitat o del Departament de Salut o, si escau, de fitxers d'altres responsables.

Similars consideracions poden fer-se pel que fa a les referències contingudes a la clàusula 21.1 del DA a la titularitat de les bases de dades, els conjunts o subconjunts de dades o el 21.2 pel que fa a la titularitat de les dades relatives als contactes i als clients de l'Adjudicatari.

Per altra banda, la dita clàusula 21 també preveu que, pel que fa a les dades dels contactes i clients de l'Adjudicatari, aquest garanteix que disposa de les corresponents autoritzacions per a dur a terme la cessió, que es realitzarà de conformitat amb la normativa de protecció de dades personals. Per bé que es valora positivament la menció que aquesta es produiria d'acord amb l'LOPD, no sembla clar de quina cessió es tractaria.

VIII

Deure de confidencialitat

Segons la documentació aportada, l'objecte del contracte de col·laboració publico privada per desenvolupar el Projecte VISC+ ha de consistir en posar en valor les dades generades pel sistema públic català, "mitjançant el tractament, l'anàlisi i l'explotació d'aquestes dades, prèviament anonimitzades, garantint en tot moment el compliment de la normativa en matèria de protecció i tractament de dades (...)" (apartat 4 del DA). S'afegeix que "*la posada a disposició de l'Adjudicatari d'aquesta informació i dades es produirà de forma anonimitzada, en els termes i condicions descrits al DT de solució final*" (apartat 5. DA).

En aquest sentit, la clàusula 39 del DA fa referència al "Deure de confidencialitat i protecció de dades", i obliga l'Adjudicatari a mantenir absoluta confidencialitat i reserva sobre qualsevol dada que pogués conèixer amb ocasió del compliment del contracte incloent una remissió a la LOPD. Sens perjudici que aquesta remissió a l'LOPD resulti adient, convindria fer referència en concret a l'article 10 de la LOPD, que preveu el deure de secret en el tractament de dades personals.

Dit això, la clàusula 39 continua exposant que *"la posada a disposició de l'Adjudicatari de les dades es produirà de forma anonimitzada, per la qual cosa les dades tindran la condició de dissociades al no permetre la identificació dels afectats o interessats. En aquest sentit, la prestació dels serveis no suposa en cap cas l'accés a dades personals*

de (l'entitat) i del Departament de Salut, pel personal posat a disposició per part de l'Adjudicatari, comprometent-se aquest a no accedir en cap moment en virtut de l'execució del contracte a dades de caràcter personal titularitat de (l'entitat) ni del Departament de Salut, ni tractar cap tipus de dada de caràcter personal a l'hora d'exercir les seves funcions."

Sens perjudici de les consideracions que es faran a continuació respecte el procés d'anonimització i el flux informatiu entre l'entitat i l'Adjudicatari, convé assenyalar que difícilment l'Adjudicatari podrà exercir les seves funcions sense "*tractar cap tipus de dada de caràcter personal*". Per això, caldria cenyir aquesta afirmació a les dades facilitades per l'entitat. Però és que a més, en altres apartats (p. ex. a l'apartat "serveis a prestar" de l'Annex 1) no sembla que es pugui descartar que en alguns casos l'Adjudicatari tingui accés a dades personals, atès que per exemple en aquest Annex 1 es preveu que en l'execució del procés d'anonimització l'Adjudicatari participi en la verificació de l'anonimització o que l'entitat pugui requerir el suport de l'Adjudicatari.

Per altra banda, en aquesta mateixa clàusula, en el subapartat intitulat "Respecte de la informació confidencial" es fa referència a què tindrà el caràcter de confidencial la informació revelada per l'entitat "per escrit o qualsevol altre suport que garanteixi la seva recepció". S'ha de dir que, d'acord amb l'article 10 de la LOPD el caràcter de confidencial s'ha de predicar de qualsevol dada de caràcter personal, amb independència de la forma o el suport en què s'hagi tramès.

IX

Nivells d'aprovació i gestió de la demanda

El DT, en l'apartat 3.2.3 *"Gestió de la demanda",* preveu **tres nivells** d'aprovació de les peticions dels clients finals, atenent, entre d'altres, al client que sol·licita el servei, els objectius pels quals es sol·licita, si la petició requereix incorporar noves fonts d'informació, o en atenció a la quantia econòmica del servei, entre d'altres.

El Nivell 1 d'aprovació es refereix a clients qualificats com de baix risc (els tres responsables dels fitxers implicats en el Projecte, citats, agents del SISCAT, la pròpia entitat, investigadors i centres de recerca, i indústria o institucions privades en l'àmbit de les ciències de la vida i la salut). La sol·licitud, en aquests casos, queda pre-aprovada, sens perjudici que es pugui denegar i passar a un nivell 2 o 3 de gestió. Un dels elements a tenir en compte en aquest nivell, per accedir a la sol·licitud del client, és que la petició d'informació estigui alineada i sigui proporcional a l'objectiu perseguit.

Aquesta proporcionalitat predicada en el text respecte de l'objectiu perseguit, caldria posar-la en relació no només amb l'objectiu que es persegueixi, sinó també en els eventuals riscos o perjudicis que es puguin causar en els drets de les persones afectades, i en concret del dret a la protecció de dades de caràcter personal.

Pel que fa a la consideració de clients de baix risc, l'ampli nombre i categories d'aquests no permet inferir que tots ells hagin de tenir accés a tota la informació sol·licitada. Com s'ha fet avinent anteriorment, això només es pot decidir valorant la informació sol·licitada (quantitativa i qualitativament), l'habilitació legal per fer-ho, si escau, i la finalitat pretesa.

En la mateixa línia, pel que fa al Nivell 2 d'aprovació, també caldria explicitar que en avaluar la sol·licitud es tindrà en compte les exigències de la normativa de protecció de dades. En aquest nivell s'avaluen les sol·licituds dels mateixos clients que en el Nivell

1, però es tracta de peticions *"que per ser lliurades es requereix incorporar noves fonts de dades (no disponibles en el moment de fer la petició) o realitzar un tractament específic de les dades ja disponibles."* Als efectes que ens ocupen, una petició de noves dades obligarà a examinar la seva pertinença atenent als principis de qualitat i de finalitat. A banda d'això, no resulta clar quin pot ser aquest tractament específic, ni les implicacions que això pot tenir per a la protecció de dades. Convindria, doncs, aclarir aquests extrems.

Pel que fa al Nivell 3 d'aprovació, es reserva per a les sol·licituds relacionades amb la realització d'un assaig clínic, amb projectes d'investigació que comporten algun risc físic o psicològic per a un ésser humà, o en els que **hi ha consentiment informat associat a la petició.**

Segons el DT, en aquests casos, i els que es prevegin segons la normativa, l'Adjudicatari haurà de comprovar que el sol·licitant acompanyi la petició amb consentiments necessaris i l'aprovació corresponent per realitzar l'estudi per part d'un CEIC, que hagi tingut en compte que s'obtindran dades o informació provinents de VISC+.

Pel que fa a la descripció d'aquest Nivell 3, el fet que es mencioni la concurrència de consentiment informat associat a la petició, permetria deduir que s'està referint a aquells casos en què la cessió de dades es produirà sense anonimització prèvia de la informació. A *sensu contrari*, també es podria inferir d'això que els Nivells 1 i 2, en què no hi ha cap menció al consentiment informat, es reserven per a les cessions de dades anonimitzades.

Ara bé, des de la perspectiva de la protecció de dades, **cal fer avinent que s'hauria d'especificar, en termes prou clars, la vinculació entre cada nivell i la possibilitat de cedir dades anonimitzades o dades personals.** Ja s'ha posat de manifest que en el context del Projecte VISC+ la comunicació de dades anonimitzades en origen presenta un menor risc potencial per a la protecció de dades, i s'hauria de prioritzar en front de cessions de dades de salut no anonimitzades, que hauria de ser excepcional.

Aquesta excepcionalitat, justificada en els principis de qualitat –en la vessant de proporcionalitat i minimització-, i de finalitat, hauria de quedar explicitada en la informació que es refereix als 3 Nivells d'autorització referits. És a dir, caldria explicitar que tots aquells casos en què es prevegi que el client final ha d'accedir i tractar dades sense anonimitzar, hauran de ser validats en atenció als principis i obligacions de la normativa de protecció de dades, i quedaran sotmesos al Nivell 3 d'aprovació.

Novament cal reiterar que, sense descartar que en alguns casos determinats clients finals poden requerir una cessió de dades de salut juntament amb dades d'identificació del pacient, aquesta possibilitat no hauria de ser la norma general, sinó només fruit d'una avaluació que tingui especialment en compte els riscos potencials des de la perspectiva de la protecció de dades.

X

Procediment tècnic d'anonimització

L'Annex 1 del DT i 'annex 3 del document relatiu al procediment, descriuen el procés d'anonimització que s'ha de dur a terme. En concret, es preveu en primer lloc eliminar la informació identificativa de persones físiques (dades identificatives i "informació

genètica"), i també eliminar o reduir al mínim imprescindible el detall de la informació o altres variables que puguin donar lloc a identificacions indirectes.

Semblaria en un principi que l'actuació de l'adjudicatari no ha de comportar l'accés a dades de caràcter personal, atès que la informació que se li trametria, seria informació anonimitzada prèviament. Així es desprèn de la pàgina 1 del document relatiu al procediment de cessió, i també de la clàusula 39 del DA. No obstant això, hi ha diferents previsions a l'Annex 1 del DT que semblen apuntar el contrari. Així trobem diferents referències que podrien comportar el tractament de dades personals per l'adjudicatari:

- A l'apartat "Procés d'anonimització: s'afirma que l'adjudicatari participa en el procés de verificació de l'anonimització.
- A l'apartat "Serveis a prestar" s'afirma que l'entitat podrà requerir el suport de l'adjudicatari en el procés d'anonimització.
- A l'apartat "Ubicació de les dades" s'afirma que hi poden haver dades que permetin la identificació indirecta.

Igualment a l'apartat 2.2.2.1 del DT es manifesta que es lliurarà a l'adjudicatari una mostra representativa d'aquestes fonts de dades, per tal que l'adjudicatari dissenyi el catàleg de serveis, el procés de comercialització i el procés d'anonimització.

Essent així, en la relació jurídica que s'estableixi entre l'entitat i l'Adjudicatari, caldria recollir de forma expressa les clàusules previstes a l'article 12.2 LOPD, en configurar-se l'adjudicatari com un encarregat del tractament. En canvi, a l'apartat 1.3 del document relatiu al procediment no s'hi troba cap referència a aquesta qüestió.

Respecte les variables a eliminar, en atenció a la finalitat, es podria valorar eliminar també la informació sobre el centre sanitari, en línia amb la previsió d'anonimitzar, si escau, la dada sobre el professionals sanitaris que atenen un pacient.

L'Annex 3 citat preveu que s'estableixi un *"codi anònim de la persona".* Es preveu que l'entitat facilitarà les dades estructurades ja anonimitzades a l'Adjudicatari utilitzant, per a una mateixa persona, un mateix codi anònim de persona per tal de permetre relacionar els diferents conjunts de dades. A això s'afegeix que *"L'Adjudicatari haurà d'utilitzar un sistema d'anonimització diferent per cada entitat jurídica usuari final. L'Adjudicatari haurà d'aplicar un segon procés sobre el codi de cas anònim que faciliti (l'entitat) perquè cada entitat jurídica usuari diferent tingui un codi de cas anònim calculat de forma diferent."*

L'Annex 3 del Document *de "Procediment per a la cessió de dades (...)",* en línia amb l'Annex 1 del DT, afegeix informació relativa a l'algorisme de càlcul que aplicaria l'entitat per calcular el codi anònim de persona, a la que ens remetem. En línia amb el que s'ha apuntat, es preveu l'eliminació d'identificacions directes (eliminar les dades identificatives de persones físiques -pacients, professionals sanitaris, etc-) i també les identificacions indirectes, com ara, a tall d'exemple, substituir la data de naixement per l'any, o l'alçada i el pes per rangs de l'alçada i pes. Per últim, es preveu en aquest document informar sobre riscos d'identificacions directes o indirectes, i sobre riscos derivats de l'excessiva informació sobre un mateix afectat, sobre codis anònims mal calculats, o sobre la revelació de la clau de xifrat. En aquest punt fem extensiva la consideració anterior sobre l'eliminació, si escau, d'informació sobre el centre sanitari, si no és rellevant per a la finalitat pretesa.

Es valora positivament que en el Document *"Procediment per a la cessió de dades (...)"* , en l'apartat 1.3.3 *"Supervisió de la formalització del contracte",* es preveu que

l'entitat podrà supervisar en tot moment els contractes que es formalitzin amb els usuaris finals, i que comprovarà "*que en els contractes s'indiqui que s'aplicarà una transformació del codi anònim de persona per obtenir un codi de cas específic i diferenciat per a cada usuari final*".

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 VISC+, les previsions de l'Annex 3, citat, s'han de valorar positivament, ja que han de suposar no només anonimitzar la informació personal sobre un individu, sinó que s'explicita que cada client final rebrà la informació en uns termes que no haurien de permetre, en principi, la vinculació amb la informació que haurà rebut un altre client final, degut a que el codi de cas anònim no coincidirà en un i altre cas.

De tota manera, per tal de reduir els riscos de re-identificació d'informació anonimitzada (qüestió que concretarem a continuació), es recomana preveure que, quan es tracti de peticions que, tot i ser formulades per un mateix client final, no estiguin vinculades a un mateix projecte, convindria atribuir un codi de cas diferent.

No obstant això, en virtut del principi de minimització al qual ja hem fet referència, no sembla que l'atribució d'un codi hagi de ser necessari en tots els casos. Per això caldria plantejar-se que, en aquells casos en què la finalitat no ho requereixi, s'anonimitzi sense atribuir cap tipus de codi.

També és rellevant i s'ha de valorar positivament, que es tinguin en compte mesures concretes d'anàlisi de riscos. Sobre aquestes qüestions, ens remetem novament al Dictamen del GTA29 5/2014, sobre tècniques d'anonimització.

Per altra banda, en la clàusula 5 del DA es preveu que l'Adjudicatari *"no podrà fer cap acció per re-identificar dades que (l'entitat) hagi facilitat de forma anonimitzada i haurà de comunicar a (l'entitat) qualsevol dada que se li hagi facilitat en principi anonimitzada però que es detecti que pot ser possible associar-la a una persona concreta."*

Es valora positivament aquesta menció, en el sentit que, des de la perspectiva de la protecció de dades, fins i tot en el cas d'anonimització prèvia de la informació personal (en el cas que ens ocupa, en bona part dades sensibles), cal tenir en compte les possibilitats que aquesta informació pugui permetre la identificació del seu titular. Així ho ha posat de manifest el GTA 29 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.

En aquest sentit, resulta positiu que en el context del Projecte VISC+ es prevegi que la detecció, per part de l'Adjudicatari, de la possibilitat de re-identificacions del titular de les dades, hagi de ser posat en coneixement de l'entitat. Tornarem sobre aquesta qüestió en l'apartat d'aquest dictamen relatiu a les mesures de seguretat.

En qualsevol cas, es recomana que es tinguin en compte, en el context del Projecte VISC+, les consideracions del Dictamen 5/2014 del GTA29, citat, respecte la necessitat de fer una anàlisi de riscos en funció de les tècniques d'anonimització emprades i les possibilitats de re-identificació inherents a aquestes tècniques.

Pel que fa a la re-identificació, fer notar també que a l'apartat "Re-identificació de les dades" de l'Annex 1 del DT es fa referència com a supòsit en què es podrà desanonimitzar, els casos en què es faci "*amb traça dels accessos*". No sembla que aquesta sola circumstància hagi d'habilitar la re-identificació. En qualsevol cas tampoc queda clar en aquest apartat qui podria dur a terme aquesta desanonimització.

També es fa referència a la re-identificació en el pacte novè de l'Acord d'encàrrec del tractament, al que ens referirem més endavant, recollit en el Document *"Encàrrec de serveis d'anonimització de dades (...)",* aportat amb la consulta, i que s'ha de signar entre el Departament de Salut, CATSALUT i l'ICS com a responsables dels fitxers, i l'entitat, com a prestador de serveis (encarregat del tractament). En aquest pacte novè es preveu que *"En el cas que el Prestador de Serveis sigui coneixedor de possibles perills per la salut present o futura dels afectats com a resultat de l'anàlisi d'una combinació de dades, concreta, aquest es compromet a informar als Responsables de fitxers perquè prenguin les mesures pertinents i reidentifiquin l'afectat, en cas que fos necessari. En cap cas s'autoritza el Prestador de Serveis a fer la reidentificació dels casos en situació de risc."* Aquesta previsió es valora positivament, ja que fa recaure en el responsable del fitxer la decisió d'una possible re-identificació. D'aquesta manera, és clar que és aquest responsable qui haurà de dur a terme la re-identificació en els casos en què pugui ser justificat.

Finalment, fem notar que en l'apartat 3.2.3 *"Gestió de la demanda",* del DT, en què es fa referència als 3 Nivells d'autorització de sol·licituds de dades, també es té en compte aquells casos en què la petició del client es refereixi a un volum de dades anonimitzades que impliqui un risc de desanonimització/personalització de les dades, respecte els quals es preveu que l'entitat haurà d'avaluar i autoritzar aquesta sol·licitud per tal de donar compliment a la LOPD. Es considera positiva aquesta previsió general de detecció de casos en què, pel volum de la informació sol·licitada, es pugui detectar un risc de re-identificació, que exigirà una anàlisi més acurada des de la perspectiva de la protecció de dades.

Dit això, en la línia de l'observació formulada al Fonament jurídic VI, es recomana que s'incorpori una referència a les mesures compensatòries que en aquests casos puguin minimitzar tant el risc potencial de re-identificació, com els efectes negatius en les persones afectades, per tal que es pugui autoritzar.

XI

Procediment establert per a la cessió de dades

En aquest apartat s'analitzen les particularitats del procediment de cessió de dades previst en el context del Projecte VISC+, incloses en el Document *"Procediment per a la cessió de dades personals anonimitzades de salut a l'Adjudicatari de VISC+ per recerca mèdica i avaluació".*

D'entrada, cal fer notar que el títol del Document és confús, ja que les cessions de dades previstes no es limiten a dades anonimitzades, com es podria deduir del títol

citat, sinó que el propi Document que analitzem estableix el procediment per cedir, també, dades personals que no han sofert un procés d'anonimització. Convindria, a efectes de claredat, referir-se en el títol a la cessió de anonimitzades i de dades personals. Pel que fa a les mencions d'aquest document a la finalitat d'*"avaluació",* ens remetem al que ja s'ha apuntat sobre la manca de concreció del tipus d'avaluació a què s'està referint.

Aquest document defineix dos processos diferents sobre la cessió d'informació en el context del Projecte VISC+:

1) Procediment per a la cessió de dades personals anonimitzades de salut a l'Adjudicatari de VISC+ per recerca mèdica i avaluació.

D'entrada, com s'ha fet avinent en aquest dictamen, des de la perspectiva de la protecció de dades, aquest és el procediment de cessió que convindria prioritzar en el context del Projecte VISC+, tenint en compte que l'anonimització ofereix un tractament menys invasiu i de menor risc per als afectats.

Partint d'aquesta premissa, es fan les següents consideracions.

Es preveu la creació inicial dels conjunts de dades anonimitzades que es posaran a disposició de l'Adjudicatari, per la qual cosa aquest ha d'elaborar un informe en el qual es detalli, entre d'altres, la proposta de procediments i eines per anonimitzar i generar un conjunt de dades no estructurades (imatges mèdiques, PDFs, etc.), i la valoració del risc d'identificacions indirectes, que serà imprescindible quan es tracti d'obtenir dades per a un destinatari i finalitat concreta.

Es valora positivament que es prevegi que es podrà incorporar una proposta de marcatge de dades o de "sembrat de la informació" (introducció de dades ocultes o emmascarades entre les reals que, sense afectar a la qualitat de la informació, permeten la detecció d'usos no autoritzats), tècnica que permetria identificar possibles fuites –o accessos indeguts- que es poguessin produir, i també que aquest marcatge haurà de ser diferenciat per a cada usuari final que sol·liciti les dades. Més enllà de la possibilitat d'aplicar aquestes tècniques de marcatge en un procediment concret de cessió de dades anonimitzades, es suggereix que s'inclogui aquesta qüestió en el contracte i alhora que es valori introduir-la no ja com una possibilitat en mans de l'Adjudicatari sinó com una obligació d'aquest.

També es fa remissió als criteris d'anonimització aprovats per l'entitat (Annex 3), i s'explicita que *"qualsevol excepció a la no aplicació d'algun dels criteris d'anonimització haurà d'acompanyar-se d'una justificació dels motius d'excepcionalitat."*

Tenint en compte que la cessió de dades no anonimitzades ja està prevista al Procediment 2, no és clar quin motiu podria justificar la no aplicació de l'anonimització prevista en l'Annex 3, ni com –o per part de qui- s'hauria d'avaluar aquesta excepció. Cas que no existeixi consentiment exprés de les persones afectades o una llei que habiliti la comunicació, la informació haurà de ser inevitablement anonimitzada, sense que puguin existir motius d'excepcionalitat.

En la valoració que l'entitat ha de fer de les sol·licituds de l'Adjudicatari (per tal d'obtenir dades anonimitzades), s'explicita que caldrà fer una valoració del compliment de l'LOPD, i es preveu que, en aquesta avaluació, es convidarà a assistir al responsable de les dades objecte de sol·licitud, *"especialment en cas que es consideri que existeix algun risc significatiu que posi en perill el compliment de la LOPD".*

Aquesta previsió, que s'entén referida al responsable del fitxer o fitxers afectats, es considera pertinent, doncs el responsable podrà participar, en aquests casos, de l'avaluació en qüestió. Ara bé, de la redacció d'aquest apartat *("... es podrà convidarà a assistir...")* no queda clar si convidar el responsable és una opció, o bé un compromís. En qualsevol cas, l'opció més garantista aconsellaria la implicació en tots aquests casos del responsable.

2) Procediment per la cessió de dades personals de salut per recerca mèdica i avaluació a l'usuari final.

Ens referim, en aquest cas, al procés que recull totes les activitats necessàries per a la creació inicial dels **conjunts de dades personals** per sol·licitud de l'Adjudicatari amb motiu d'un encàrrec d'un usuari final.

En principi, en aquest procediment, tot i que l'Adjudicatari intervindria en la presentació de la sol·licitud de l'usuari final davant de l'entitat (apartats 2.1 i 2.2 del document relatiu al procediment), pel que es descriu en aquest apartat semblaria que l'Adjudicatari no ha d'intervenir en el lliurament de les dades. Així es desprèn també de l'apartat 2.2.2 del DT.

No obstant això, de l'apartat "Usos del les dades" de l'Annex 1 del DT sembla desprendre's el contrari, atès que es manifesta que l'Adjudicatari haurà de preservar el model de seguretat, disponibilitat i ús de dades que estigui vigent a cada moment i no podrà utilitzar-les per a cap altra finalitat que les enumerades anteriorment ni facilitar-les a tercers, sense consentiment exprés per part de l'entitat. També sembla desprendre's això de les mencions a l'adjudicatari contingudes als apartats 2.3.1, 2.3.3.1 i 2.3.3.2 del document relatiu al procediment.

També sembla desprendre's de la referència a l'elaboració d'un informe de l'apartat 2.3.2 del document relatiu al procediment, perquè, tot i que en aquest cas no s'esmenta directament l'adjudicatari, sembla que s'està referint a ell.

Les referències a l'adjudicatari en aquests apartats només tindrien sentit si l'adjudicatari intervé en el tractament de dades no anonimitzades (què són les dades a què es refereixen aquests apartats). Per això caldria corregir aquesta manca de congruència.

Aquest procediment implica no ja un flux informatiu d'informació anonimitzada, sinó de dades personals de salut. Per això, cal insistir en què, a banda de la necessitat del consentiment de les persones afectades, qualsevol cessió s'haurà de fonamentar en una finalitat legítima, caldrà comprovar que l'usuari final està habilitat per tractar dades per a aquesta finalitat, i valorar que les dades no són excessives per a la dita finalitat, qüestió que es preveu en el document (punt 2.1.1). Val a dir que en el mateix apartat 2.1.1, que comentem, es fa esment que l'informe de l'Adjudicatari ha de tenir en compte, entre d'altres, *"el grau de detall dels valors de les variables, quan són tan detallades que podrien donar lloc a identificacions indirectes".* Tenint en compte que en aquest segon procediment es tractaran dades personals, cal fer notar que la possibilitat d'identificació dels afectats serà més que probable, i no només de manera "indirecta". Tenint en compte això, com ha estat abastament exposat en aquest informe, cal extremar les precaucions, en atenció a la normativa de protecció da dades, a l'hora de donar viabilitat a qualsevol petició d'usuaris finals en el marc d'aquest procediment.

En relació amb el consentiment dels afectats, en l'apartat 2.1.1 *"Sol·licitud de l'adjudicatari",* es preveu que l'informe de l'Adjudicatari ha de tenir, entre d'altres, el següent contingut:

"Els consentiments informats de les persones incloses al conjunt de dades sol·licitat. Aquests consentiments hauran de complir amb els requeriments de la LOPD i cobrir explícitament la cessió de dades sol·licitades."

L'Annex 1 del DT fa referència a que si es faciliten dades de persones identificables, perquè el client final necessita enriquir dades personals que ja té amb dades del Departament de Salut (o, se suposa, dels altres responsables dels fitxers implicats en el projecte), caldrà que aquell faciliti una auditoria que demostri que complirà amb les obligacions de l'LOPD, en referència, entre d'altres, al *"consentiment vàlid de tots els afectats".*

D'entrada, a banda de preveure els requeriments de l'LOPD, caldria incloure una referència explícita als requeriments que es puguin preveure en la normativa aplicable en cada supòsit. Com s'ha dit, en matèria d'investigació mèdica, les lleis d'autonomia del pacient, o d'altres lleis aplicables als assajos clínics, a la investigació biomèdica, etc, preveuen particularitats respecte el consentiment informat dels afectats, que caldrà tenir en compte en cada cas.

En connexió amb això, en l'apartat 2.1.3 *"Generació i lliurament del conjunt de dades personals"*, es disposa que l'entitat executarà el procés per obtenir efectivament aquestes dades, i que *"quan s'hagin obtingut aquestes dades es realitzarà una prova de l'aplicació i una verificació de la selecció de pacients amb consentiment.* A continuació, l'entitat elaborarà l'informe de verificació i prova sobre la correcta selecció dels casos, i sobre *"la comprovació que els casos dels conjunts de dades es corresponen amb els casos en què l'usuari final aporta consentiments dels afectats."*

Cal fer avinent que no és prou clar el mecanisme descrit per a l'obtenció del consentiment dels afectats. Sembla clar que és l'usuari final el que aporta els consentiments (s'ha d'entendre, els fulls de consentiment informat degudament emplenats en base al que pugui preveure la normativa aplicable en cada cas), però aquests consentiments es refereixen a persones incloses en els conjunts de dades sol·licitades, en definitiva, en fitxers de dades als quals l'usuari final no té accés, ni n'és el responsable, ni l'encarregat del tractament (article 12 LOPD).

Cal tenir present que, en el marc de les previsions relatives al consentiment dels titulars de les dades (articles 6 i 11 LOPD), l'article 12 del RLOPD concreta el següent:

> *"1. El **responsable del tractament ha d'obtenir el consentiment de l'interessat** per al tractament personal excepte en els supòsits en què el consentiment no sigui exigible d'acord amb el que disposen les lleis.*
>
> *La sol•licitud del consentiment ha de fer referència a un tractament o sèrie de tractaments concrets, amb delimitació de la finalitat per als quals se sol•licita, així com de les restants condicions que concorrin en el tractament o sèrie de tractaments.*
>
> *2. Quan se sol•liciti el consentiment de l'afectat per a la cessió de les seves dades, ha de ser informat de manera que conegui inequívocament la finalitat a què es destinen les dades respecte de la comunicació de les quals se sol•licita el consentiment i el tipus d'activitat que porta a terme el cessionari. En cas contrari, el consentiment és nul.*
>
> *3. Correspon al responsable del tractament la prova de l'existència del consentiment de l'afectat per qualsevol mitjà de prova admissible en dret."*

En principi, és doncs al responsable (article 3.d) LOPD), en el cas que ens ocupa, el Departament de Salut, el CATSALUT i l'ICS, responsables dels fitxers implicats en el Projecte VISC+, a qui correspon sol·licitar el consentiment per a poder cedir dades personals.

En aquests termes, no és clar com un tercer aliè als responsables, i a priori indeterminat (doncs els usuaris finals poden ser entitats de molt diversa naturalesa), podrà identificar, contactar i obtenir el consentiment dels afectats, les dades dels quals es tracten en aquests fitxers. Sense prejutjar que en alguns casos aquest esquema pugui ser realitzable (p. ex. quan les mateixes persones ja hagin donat el seu consentiment per participar en altres fases d'un estudi) i pugui facilitar dur a terme aquest tipus d'estudis, caldria deixar oberta la possibilitat de que pugui ser el mateix responsable del fitxer, o si escau l'entitat, qui obtingui el dit consentiment. En qualsevol cas convé recordar que la responsabilitat sobre l'adequat tractament de les dades seguirà corresponent al responsable del fitxer.

Encara en relació amb el consentiment, el punt 2.2 del procediment que descrivim (cessió de dades personals) preveu que a l'hora d'actualitzar la informació ("actualitzacions temporals acordades"), l'entitat revisarà *"si hi ha altes o baixes en els consentiments informats que es varen facilitar inicialment."*

Si, com sembla, els consentiments informats els ha d'obtenir l'usuari final, sembla lògic inferir que serà aquest el que, havent informat adequadament els afectats sobre la possibilitat de revocació del dit consentiment (articles 6.3 11.4 LOPD), disposarà de la informació relativa a possibles revocacions, o possibles nous consentiments. Seguint aquest esquema, es preveu que l'entitat haurà de contrastar aquesta nova informació (nous consentiments o revocació dels anteriors) abans de donar nova informació. Aquesta mesura suposa una garantia, doncs condiciona la cessió de dades a les oportunes comprovacions.

A això afegim que el punt 2.2, que comentem, preveu que l'actualització de la informació haurà de tenir en compte possibles modificacions a conseqüència de l'exercici de Drets ARCO (Títol III LOPD i Títol III RLOPD), per part dels pacients de centres sanitaris, que són els que hauran modificat informació a conseqüència de l'exercici d'aquests drets. Si bé aquesta previsió suposa una garantia respecte l'actualització de la informació que arribaria als usuaris finals, seria recomanable substituir l'expressió "*centre sanitari*" per "*responsable del fitxer*".

També fer notar que en l'apartat 2.1.3, a banda de les qüestions relatives al consentiment que hem apuntat, es preveu que *"finalment es realitzarà una validació de seguretat",* però no es concreten els aspectes a verificar.

Finalment, fem un apunt formal, atès que en la pàgina 7 del Document per a la cessió de dades, es fa una referència a l'Annex 3 (condicions de seguretat, ús i disponibilitat de dades), enlloc de referir-se a l'Annex 1.

XII

Mesures de seguretat

Si bé amb caràcter general el Projecte VISC+ suposa el tractament d'informació que a priori haurà estat anonimitzada per l'entitat, de tal manera que l'activitat principal de l'Adjudicatari no implica, amb caràcter ordinari, el tractament de dades de caràcter

personal, també es preveu el tractament i cessió de dades personals. En conseqüència, sens perjudici de les consideracions ja fetes, convé plantejar un **model integral de seguretat de la informació per al conjunt del contracte VISC+, aplicable tant al tractament de dades anonimitzades com de dades personals.**

El Projecte VISC+ implica el tractament de dades de caràcter personal que requereixen l'aplicació del **nivell alt de mesures de seguretat** (article 9 LOPD i títol VIII del RLOPD).

El Pacte Quart de l'Acord d'encàrrec del tractament, inclòs al document *"Encàrrec de serveis d'anonimització de dades i de cessió de dades anonimitzades i personals per finalitats d'avaluació i recerca mèdiques",* aportat amb la consulta, explicita que, d'acord amb l'article 9 de l'LOPD, l'entitat es compromet a adoptar les mesures de seguretat del nivell que s'indica a l'encapçalament. Atès que l'encapçalament del document no es refereix expressament al nivell de seguretat (la referència al nivell de seguretat aplicable no es troba fins a la pàgina 7 de l'"Encàrrec de serveis ..."), seria recomanable fer una referència directa al nivell alt en el Pacte Quart.

En qualsevol cas, queda clar que el nivell alt de mesures de seguretat resulta de necessària aplicació, com s'ha apuntat, tenint en compte la informació que es tracta en els fitxers del Departament de Salut, de CATSALUT i de l'ICS, que són la font d'on s'extrauran les dades per al tractament objecte del Projecte VISC+.

Ara bé, les especials característiques dels tractaments i les activitats que deriven del contracte VISC+ aconsellen plantejar-se un **model de seguretat que vagi més enllà** de les previsions de seguretat que preveu el títol VIII del RLOPD.

El conjunt de la documentació aportada evidencia una clara voluntat d'oferir les màximes garanties de seguretat per a les dades, establint mesures tècniques i organitzatives que donin com a resultat un "model de seguretat, disponibilitat i ús de les dades" orientat a la protecció del conjunt del sistema VISC+.

Amb caràcter general convindria que, com a punt de partida, la seguretat de la informació exigible a l'Adjudicatari estigués alineada amb algun dels **conjunts de bones pràctiques** existents (Tipus ISO27001). Si bé no seria necessari que el contracte determini un conjunt concret de bones pràctiques, si caldria determinar que les que finalment implanti l'Adjudicatari hauran de basar-se en la gestió de riscos, ser susceptibles de ser certificades per un tercer independent i poder 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, a continuació es fan les següents consideracions.

En els criteris de valoració del contracte, previstos en l'apartat 8.2 del DA, aparentment no s'inclouen els aspectes de gestió de la seguretat que pugui aportar l'Adjudicatari. Aquest extrem hauria de ser rellevant a l'hora de valorar les propostes. Respecte la valoració de la "*gestió i operació dels serveis d'anàlisi, tractament i explotació de dades*" (fins a 17 punts), on a priori s'inclourien les qüestions de gestió de la seguretat, només es fa referencia a que es valorarà com es dóna resposta al requeriments especificats a l'apartat 3.2 del DT, sense fer esment a l'apartat 3.1 del mateix document, que detalla la "seguretat i anonimització de les dades".

Segons l'apartat 2.2.2 del DT, es preveu posar a disposició de l'Adjudicatari una mostra de dades, per tal de dissenyar les infraestructures i procediments relacionats

amb el contracte. En conseqüència, caldrà tenir en compte, també en aquesta fase, les mesures de seguretat previstes als articles 87 del RLOPD (fitxers temporals o còpies de treball de documents) i 94.4 RLOPD (proves anteriors a la implantació o modificació dels sistemes d'informació). Aquesta consideració es fa extensible a l'apartat 2.1.3 del Document *"Procediment per a la cessió de dades",* en què es preveu la generació i lliurament del conjunt de dades personals.

En qualsevol cas, seria oportú que en l'apartat 4.1 del DT ("Fase de preparació i construcció"), s'explicités que el tractament de dades en aquesta fase inicial resta subjecte a la normativa de protecció de dades, específicament, en relació amb les mesures de seguretat aplicables.

En relació amb les previsions sobre la realització d'auditories (article 96 RLOPD), l'apartat 5.3 del DT *"Auditories i governança de la seguretat",* preveu que l'entitat "*podrà realitzar auditories* (...)". Sobre aquesta previsió, convindria fer una definició més oberta del paper de l'entitat, en el sentit que pugui "realitzar" o bé "encarregar a tercers" l'auditoria del model de seguretat.

A l'apartat 1.4.1 "Auditories" del Document *"Procediment per a la cessió..."* , es preveu, entre d'altres, una auditoria anual, l'abast de la qual seria del 50%. Això podria generar certs riscos, doncs pot resultar complex determinar quin 50% donaria suficient evidència de que les mesures de seguretat donen el resultat esperat i s'adeqüen a les previsions del contracte i la normativa aplicable.

Per tal de simplificar el model d'auditoria, aquesta Autoritat proposa un model més senzill d'implementar i potencialment més eficaç, això és, **un model d'auditoria continuada,** en base a la verificació de l'aplicació dels procediments i resultats dels processos de seguretat, realitzada internament per l'Adjudicatari, i amb emissió d'informes periòdics (potser trimestrals, o inclús semestrals) per ser analitzats per l'entitat, i una auditoria formal cada 2 anys, realitzada per una entitat externa i independent, que finalitzi amb un informe d'auditoria amb els continguts mínims exigits per la normativa de protecció de dades (article 96.2 RLOPD).

També fem esment que en l'Annex 3 del Document de *"Procediment per a la cessió de dades personals (...)",* comentat, es preveu que *"L'enviament de les dades que realitzi (l'entitat), tant a l'Adjudicatari en cas de dades anonimitzades com a l'usuari final en cas de dades personals, el realitzarà mitjançant un sistema de transmissió de fitxers (FTP) xifrat.*" De fet, es fa esment d'aquesta qüestió (sistema de transmissió xifrat) en diversos punts d'aquest Document. Aquestes previsions s'ajustarien a l'article 104 del RLOPD, segons el qual, quan es requereix la implantació de mesures de nivell alt, la transmissió de dades de caràcter personal a través de xarxes públiques o xarxes sense fil de comunicacions electròniques s'ha de fer xifrant les dades, o bé utilitzant altres mecanismes que garanteixin que la informació no és intel·ligible ni manipulada per tercers. Ara bé, per la transcendència i els riscos inherents a aquesta operació, doncs presumiblement l'intercanvi d'informació es farà mitjançant xarxes públiques de telecomunicacions, seria molt recomanable concretar més alguns aspectes tècnics, com ara la xarxa de comunicacions que s'utilitzarà; els requisits del programari utilitzat per a la transmissió de les dades; les restriccions a nivell de xarxa pel que fa al filtrat d'adreces IP (origen i destinació); els requisits mínims dels algoritmes de xifratge a utilitzar, etc.. També es recomana preveure xifrar el canal de transport, així com xifrar en origen les dades objecte de transmissió.

També cal fer esment de la previsió relativa a la tecnologia emprada pel "centre de competència", citat, que centralitza la tasca duta a terme per l'Adjudicatari en el Projecte VISC+ amb l'objectiu que els serveis d'anàlisi i explotació de dades que ha

d'oferir l'Adjudicatari es prestin des d'un mateix espai (apartat 3.4 del DT). Així, es preveu que l'Adjudicatari haurà de dotar el centre de competència dels components i eines tecnològiques adequades per prestar els productes i serveis VISC+ (apartat 3.4.3 del DT). Es preveu que la tecnologia emprada ha de ser, entre d'altres, interoperable, per integrar-se amb altres sistemes corporatius i relacionar-se amb sistemes externs a l'entorn de la Generalitat, i segura a nivell de dades i a nivell lògic, per garantir l'accés segur a la informació i al sistema, per custodiar les dades i evitar fugues o accessos no desitjats als serveis i la informació, d'acord amb el model de seguretat, disponibilitat i ús de les dades (Annex 1 del DT). Per tant, cal entendre que el centre de competència queda vinculat per les mesures previstes en el dit Annex 1. Pel que fa al centre de competència, des de la perspectiva de les mesures de seguretat aplicables, a nivell organitzatiu es suggereix identificar i incorporar les funcions bàsiques del delegat de protecció de dades, especialment per part de l'Adjudicatari, a fi de començar a alinear les previsions del contracte VISC+ amb el que preveu el Projecte de Reglament Europeu de Protecció de Dades, actualment en tramitació.

Pel que fa a la gestió de les incidències, se'n fa referència en els apartats 1.4.3 i 2.3.3 del Document del Procediment per a la cessió de dades, analitzat. En síntesi, es preveu que l'Adjudicatari i l'entitat poden detectar casos mal anonimitzats o qualsevol incidència que afecti a la seguretat de les dades, i que en aquests casos, es farà una anàlisi i una proposta de pla d'acció (que ha de tenir un contingut mínim que es detalla), el qual haurà de ser aprovat per l'entitat. En connexió amb això, com s'ha esmentat, en la clàusula 5 del DA es preveu que l'Adjudicatari no pot fer cap acció per re-identificar dades, i que ha de comunicar a l'entitat qualsevol dada que se li hagi facilitat en principi anonimitzada però que es detecti que pot ser possible associar-la a una persona concreta.

Des de la perspectiva de les mesures de seguretat previstes al RLOPD, caldria considerar aquesta casuística com un incident de seguretat. En cas de produir-se un accés no autoritzat a dades de caràcter personal, aquest supòsit hauria de ser registrat formalment com un incident de seguretat. Per la rellevància de la qüestió, caldria establir en el contracte l'obligació de l'Adjudicatari de mantenir un registre d'incidències en els termes del RLOPD (articles 90 i 100 del RLOPD).

Finalment, atès que es preveu la comunicació a l'entitat, per la importància d'aquest tipus d'incident seria recomanable concretar en el contracte alguns aspectes d'aquesta comunicació: termini per comunicar-lo; qui comunica a qui; canal de comunicació preferent; i contingut mínim de la comunicació, que en tot cas hauria d'incloure, a banda dels fets ocorreguts, el nombre d'afectats i la seva ubicació en el temps, les mesures preses i les potencials conseqüències d'aquest incident. Com a suggeriment, i per alinear el Projecte VISC+ amb algunes obligacions que es podrien derivar de l'aprovació de Reglament Europeu de Protecció de Dades, citat, seria convenient, amb la intenció de generar confiança en el dit projecte, que la comunicació també es fes efectiva a l'Autoritat Catalana de Protecció de Dades.

Aquests comentaris es fan extensius als punts 1.4.3 i 2.3.3 del Document de "Procediment per a la cessió de dades".

XIII

Ubicació de la informació

També des del punt de vista de la seguretat, cal fer algunes consideracions sobre la ubicació de la informació.

L'Annex 1 del DT, citat, també fa referència a la *"ubicació de les dades".* Des d'un punt de vista formal, convindria esmentar en aquest apartat el RLOPD, que és la norma en què es concreten les mesures de seguretat aplicables, i no només la LOPD.

Dit això, en aquest apartat es fa referència a que caldrà garantir, entre d'altres, "*la traçabilitat de tots els accessos*". Sobre això, cal fer notar que el RLOPD exigeix, per als fitxers que requereixen mesures de nivell alt, articular un registre d'accessos, de manera que de cada intent d'accés s'han de guardar, com a mínim, la identificació de l'usuari, la data i l'hora en què es va realitzar, el fitxer a què s'ha accedit, el tipus d'accés i si ha estat autoritzat o denegat (article 103 RLOPD). Es valoren, doncs, en termes positius, les diverses mencions que es fan en la documentació aportada a la traçabilitat dels accessos.

En aquest apartat també es fa referència a la necessitat d'autorització prèvia d'aquesta Autoritat per una transferència internacional de dades, excepte dins l'Espai Econòmic Europeu, entitats *Safe Harbour* d'Estats Units i altres països homologats.

Atès que el propi DT, en l'apartat 2.2.1 *"Abast del model de gestió i operació",* explicita que l'Adjudicatari ha de canalitzar la demanda del mercat nacional i internacional, no es descarta que algun dels clients potencials de la informació objecte de tractament en el context del Projecte VISC+ pugui comportar una transferència internacional de dades. Si és així, aquesta es troba sotmesa al règim establert als articles 33 i 34 de la LOPD.

En cas de no poder garantir, per tant, l'adhesió als principis de l'acord Safe Harbor, en un cas determinat, o de no donar-se cap altra de les excepcions previstes a la LOPD caldrà, a banda de complir amb la resta de principis i obligacions de la LOPD, comptar amb l'autorització del Director de l'Agència Espanyola de Protecció de Dades (article 37.1.l) LOPD). Per tant, la referència que es fa a l'APDCAT en aquesta apartat s'hauria de fer a l'Agència Espanyola de Protecció de Dades.

Finalment, segons aquest mateix punt de l'Annex 1 del DT, s'impedeix utilitzar tecnologies *"cloud computing"* sense restricció de país o que es puguin utilitzar CPDs que prèviament no hagin superat amb èxit una auditoria del compliment de la LOPD, la qual, convé puntualitzar, haurà d'haver-se realitzat dins el termini de 2 anys anteriors a l'ús del centre de procés de dades (CPD). És a dir, aquest haurà d'estar al dia pel que fa a la realització d'auditories de seguretat, en els termes del RLOPD (article 96).

En qualsevol cas, amb aquestes referències a la computació en núvol, es dedueix que el Projecte té en compte que un tractament de dades derivat d'una transferència internacional, en aquests termes, podria no assegurar el correcte compliment del règim citat (articles 33 i 34 LOPD), de manera que cal valorar positivament aquesta previsió.

XIV

Encàrrec del tractament i possibilitat de subcontractació de les prestacions del contracte

La documentació aportada inclou el document *"Encàrrec de serveis d'anonimització de dades i de cessió de dades anonimitzades i personals per finalitats d'avaluació i recerca mèdiques",* ja esmentat.

Aquest document es refereix a l'Acord que han de subscriure, d'una banda, els responsables dels fitxers relacionats amb el Projecte VISC+ (Departament de Salut, CATSALUT i ICS), i de l'altra, l'entitat, com a prestador de serveis, i que ha de constituir un encàrrec del tractament regulat a l'article 12 de l'LOPD, tal i com s'explicita en el punt 4 del dit Acord.

Pel que fa a la *"Descripció dels serveis encarregats",* inclosa en l'Acord d'encàrrec del tractament, convé fer les següents consideracions:

a) Novament es fan referències a l'anonimització "*de la informació dels responsables dels fitxers...*". Com s'ha apuntat, convindria referir-se a la informació continguda als fitxers de dades personals.

b) Es preveu que l'entitat ha de comprovar que el cessionari disposa del consentiment vàlid de cadascuna de les persones afectades per cedir la informació, i que disposa d'una auditoria que demostra el compliment de les mesures de seguretat de l'LOPD. Sens perjudici d'altres consideracions fetes en aquest dictamen respecte d'aquestes qüestions (consentiment informat i auditoria), i de les responsabilitats que, en atenció a la normativa de protecció de dades, corresponguin als responsables dels fitxers, la previsió que serà l'entitat la que comprovarà aquests extrems (consentiments i auditoria) s'ajusta a la previsió feta en l'Annex 1 del DT, segons la qual és l'entitat la que efectivament ha de revisar que el "client final" (receptor de la informació personal) disposa dels dits consentiments i auditoria.

L'Acord d'encàrrec del tractament examinat conté un apartat en què es relacionen els *"Fitxers administratius de caràcter personal als quals pertanyen les dades que se sotmetran a tractament dins dels serveis encarregats".* Des d'un punt de vista formal, i atenent a la terminologia de l'LOPD, caldria referir-se a "fitxers de dades de caràcter personal", i no a "fitxers administratius de caràcter personal".

En concret, es relacionen fitxers titularitat del Departament de Salut, del Servei Català de la Salut i de l'Institut Català de la Salut. En els tres casos també s'exclouen de l'encàrrec determinats fitxers, i es preveu, també en relació amb els fitxers dels tres responsables, la següent fórmula:

"I en el futur qualsevol altre fitxer del (responsable) amb dades de salut o centres assistencials d'interès per la recerca i avaluació mèdiques".

Des de la perspectiva de la protecció de dades, en concret, dels principis de qualitat i de finalitat (article 4 LOPD), cal qüestionar que s'empri aquesta fórmula, doncs obre la porta a que fitxers que fins i tot encara no han estat creats i dels quals, per tant, es desconeix la finalitat i la informació tractada, puguin quedar automàticament afectats per l'encàrrec del tractament i, per tant, ser inclosos en l'objecte del contracte que ens ocupa, referit al Projecte VISC+. Aquesta inclusió automàtica de futurs fitxers és desaconsellable, ja que sembla obviar la prèvia valoració del responsable (sigui el Departament de Salut, el CATSALUT o l'ICS), de la conveniència d'incloure un determinat fitxer en el Projecte VISC+. Per tant, l'Acord d'encàrrec del tractament s'hauria de circumscriure als fitxers existents determinats en el moment de la seva signatura, o d'altres que es pugui establir d'acord amb un previ procés que permeti avaluar la seva adequació.

En qualsevol cas, convé recordar i seria bo recollir de forma expressa que, en finalitzar l'encàrrec, resultarà d'aplicació el que preveu l'article 12.3 de l'LOPD, és a dir, caldrà procedir al retorn de les dades al responsable o bé, si escau, a la seva destrucció.

Encara en relació amb l'encàrrec del tractament, ens referim a la clàusula 27 del DA, segons la qual en els termes previstos als articles 227 i 228 del Reial decret legislatiu 3/2011, de 14 de novembre, que aprova el text refós de la Llei de contractes del sector públic (TRLCSP), les prestacions del contracte que ens ocupa podran ser objecte de objecte de subcontractació, i se n'especifiquen una sèrie de requisits (pàgina 35 del DA).

Atès que entre aquests requisits no es fa menció de qüestions relatives a la protecció de dades, convé fer avinent que en el cas que la subcontractació a què fa esment la clàusula 27, citada, pugui afectar a dades personals, cal tenir en compte que, segons l'apartat 3 de la disposició addicional 26ª del TRLCSP:

> *"En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:*
> *a) Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.*
> *b) Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.*
> *c) Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.*
> *En estos casos, el tercero tendrá también la consideración de encargado del tratamiento."*

Per tant, en la clàusula 27, citada, del DA, convindria fer constar que en cas que l'empresa que resulti adjudicatària subcontracti alguna prestació del contracte, caldrà donar compliment a les obligacions de la LOPD en relació amb l'encàrrec del tractament, en els termes de la disposició addicional 26ª, apartat 3, del TRLCSP.

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

Conclusions

Atesa la casuística àmplia i diversa que es pot donar en relació amb els clients potencials, les finalitats previstes, els serveis oferts i els fitxers que serien font d'informació en el context del Projecte VISC+, seria convenient una major claredat i concreció respecte quines finalitats poden justificar l'accés a la informació, per part de quins clients i en quines condicions. A aquests efectes seria d'utilitat disposar d'una memòria general que descrigui el projecte de manera global que reculli de forma armonitzada les previsions dels diferents documents aportats i clarifiqui els diferents aspectes posats de manifest al llarg d'aquest dictamen, com també una avaluació d'impacte sobre la privacitat.

Des de la perspectiva dels principis de qualitat i de finalitat, i pel volum d'informació sensible generada a través de VISC+, es recomana prioritzar els supòsits de cessió de dades prèviament anonimitzades, associades a un codi no identificable o, si és possible, no associades a cap codi, per davant dels supòsits de cessió de dades personals de persones identificables que hagin prestat el seu consentiment.

El conjunt de la documentació aportada evidencia una clara voluntat d'oferir les màximes garanties de seguretat per a les dades, establint mesures tècniques i organitzatives que donen com a resultat un *"model de seguretat, disponibilitat i ús de les dades*" orientat a la protecció del conjunt del sistema VISC+.

D'acord amb el RLOPD cal aplicar un nivell alt de mesures de seguretat. No obstant això, es recomana l'adopció d'un model integral de seguretat de la informació per al conjunt del contracte VISC+, aplicable tant al tractament de dades anonimitzades com de dades personals, que vagi més enllà de les previsions de seguretat que preveu el títol VIII del RLOPD i que estigui alineat amb algun dels conjunts de bones pràctiques existents.

Pel que fa a les mesures de seguretat previstes al RLOPD, convindria especificar diverses qüestions relatives a les auditories de seguretat, els registres d'incidències, o els requisits de seguretat relacionats amb la transmissió de dades, entre d'altres, en els termes exposats al Fonament Jurídic XII d'aquest dictamen.

Pel que fa a l'encàrrec del tractament entre els responsables dels fitxers implicats en el Projecte i l'entitat, convé tenir en compte les previsions de l'article 12 LOPD, en els termes apuntats en el Fonament Jurídic XIV d'aquest dictamen.

Barcelona, 23 de juliol de 2014