CNS 20/2015

Dictamen en relació amb el Projecte per donar valor a la informació del sistema sanitari català en el marc de les polítiques públiques, VISC+ (versió març de 2015)

Es tramet a l'Autoritat Catalana de Protecció de Dades, en data 20 de març de 2015, documentació relativa al nou enfocament del Projecte VISC+, en base a la que es sol·licita, en relació amb les previsions de la Moció parlamentària sobre VISC+, l'elaboració d'un dictamen en què s'analitzin els elements que s'han incorporat al projecte després del Dictamen 34/2014, emès per aquesta Autoritat el 23 de juliol de 2014, sobre el Projecte VISC+ del Departament de Salut.

En concret, es tramet a l'Autoritat els següents documents, en la versió de març de 2015:

1 Canvis aplicats als documents en base a les recomanacions de l'APDCAT
2 Informació sobre el tipus de dades i el procés d'anonimització de VISC+
3 Informació d'interès social del projecte (Memòria social)
4 Anàlisi de riscos (per al CatSalut, la ciutadania i la continuïtat de VISC+)
5 Valoració dels models de gestió de VISC+ (AQUAS o col·laboradors externs)
6 Estàndards de recol·lecció de dades
7 Garanties ètiques d'ús de les dades (codi ètic)
8 Informe d'avaluació d'impacte sobre la privacitat de VISC+
9 Encàrrec de gestió del Departament de Salut, CatSalut i ICS a l'Agència.

Analitzada la documentació aportada, relativa al nou enfocament del Projecte VISC+, i la normativa aplicable, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

Antecedents

L'any 2014 una entitat de dret públic (en endavant, l'entitat), va formular consulta a aquesta Autoritat en relació amb el "Projecte VISC+", referit a la licitació d'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 (en endavant, projecte VISC+). En relació amb la consulta formulada, aquesta Autoritat va emetre el Dictamen 34/2014.

Posteriorment a l'elaboració del Dictamen 34/2014, l'Autoritat va mantenir diverses reunions amb els responsables del Projecte, a fi i efecte d'analitzar el contingut del mateix i els canvis incorporats a arrel de les recomanacions i suggeriments formulats per l'Autoritat, des de la perspectiva de la protecció de dades personals (Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD), i la resta de normativa aplicable).

Cal fer menció de la Moció 150/X, del Parlament de Catalunya, sobre el Projecte VISC+ (BOPC, núm. 421, de 3 de novembre de 2014), en el que el Parlament insta el Govern, entre d'altres, a aturar la licitació del projecte VISC+ fins que s'hagi acabat el procés participatiu i deliberatiu a què fa referència la moció. Segons la Moció, aquest procés participatiu ha de comptar amb la participació de representats dels grups parlamentaris, col·legis professionals d'especialitats implicades, professionals i direccions dels centres assistencials i de recerca, experts en recerca social i biomèdica, així com amb representants de l'Apdcat, entre d'altres.

La Moció del Parlament insta a aportar, a tots els agents convidats al procés deliberatiu esmentat i al Parlament de Catalunya, diversa documentació, entre d'altres, *"l'informe de l'Apdcat sobre el Projecte VISC+, i correccions fetes al projecte per ajustar-se a les recomanacions i advertències que fa aquest informe, especialment quant a les garanties que només s'utilitzaran dades degudament anonimitzades."*

A arrel de les previsions de la Moció del Parlament, en data 14 de gener de 2015 es va fer una Jornada de debat sobre la reutilització de dades i el projecte VISC+ amb representants dels grups parlamentaris, en què també va participar l'Apdcat. En aquesta Jornada, l'Apdcat va fer avinents les consideracions principals fetes tant en el Dictamen 34/2014 com posteriorment, sempre des de la perspectiva de la protecció de dades de caràcter personal.

Finalment, cal fer avinent que abans de l'emissió d'aquest dictamen s'ha publicat la Resolució SLT/570/2015, de 16 de març, per la qual es fa públic un encàrrec de gestió que formalitzen el Departament de Salut, el Servei Català de la Salut i l'Institut Català de la Salut amb l'Agència de Qualitat i Avaluació Sanitàries de Catalunya (DOGC, núm. 6843, d'1.4.2015).

III

Objecte del dictamen

Tal com ja s'ha exposat, aquesta Autoritat ja va emetre el Dictamen 34/2014 sobre el projecte VISC+. En aquell document s'analitzaven les implicacions generals d'un projecte d'aquesta naturalesa i els aspectes concrets derivats dels documents que formaven part del projecte sotmesos a dictamen. Aquell dictamen es concloïa amb un seguit de consideracions sobre aspectes que calia millorar en el projecte.

El dictamen que s'emet ara, es centrarà bàsicament en l'anàlisi de les modificacions introduïdes en el projecte arran d'aquell primer dictamen, com també sobre altres qüestions noves que es plantegen a la vista de l'evolució que ha sofert el projecte.

La sol·licitud de dictamen que es formula es refereix específicament al conjunt de documents de resposta a la Moció 150/X del Parlament de Catalunya, sobre VISC+, en la seva versió de març de 2015, que s'aporten amb la consulta. En concret es tracta dels documents següents:

1 Canvis aplicats als documents en base a les recomanacions de l'APDCAT
2 Informació sobre el tipus de dades i el procés d'anonimització de VISC+
3 Informació d'interès social del projecte (Memòria social)
4 Anàlisi de riscos (per al CatSalut, la ciutadania i la continuïtat de VISC+)
5 Valoració dels models de gestió de VISC+ (entitat de dret públic o col·laboradors externs)

6 Estàndards de recol·lecció de dades
7 Garanties ètiques d'ús de les dades (codi ètic)
8 Informe d'avaluació d'impacte sobre la privacitat de VISC+
9 Encàrrec de gestió del Departament de Salut, CatSalut i ICS a l'entitat

Per facilitar la lectura d'aquest dictamen, es farà referència, en endavant, al número dels nou documents esmentats (Document núm. 1; Document núm. 2, etc).

Cal tenir en compte que amb la tramesa de la documentació que cal analitzar en aquest dictamen (versió de març de 2015), l'entitat fa avinent que, com a resultat del debat amb els grups parlamentaris, s'ha re-enfocat el projecte VISC+, de manera que alguns dels documents que formaven part de les versions anteriors del Projecte i que havien estat analitzats per aquesta Autoritat en el Dictamen 34/2014, ja no són d'aplicació.

En concret es tractaria, segons la informació aportada per l'entitat, dels següents documents:

- Document de solució final Tècnic
- Document de solució final Administratiu
- Procediment VISC+ de tractament i cessió de dades anonimitzades

El fet que aquests tres documents ja no resultin d'aplicació al Projecte VISC+ i, per tant, ja no hagin de ser tinguts en compte de cara a l'elaboració del present dictamen, no desvirtua algunes de les consideracions que, des de la perspectiva de la protecció de dades personals, ha formulat aquesta Autoritat a través del Dictamen 34/2014, al qual ens remetem.

En qualsevol cas, l'objecte d'aquest dictamen és l'anàlisi i la valoració del contingut dels documents aportats en data 20 de març de 2015, especialment pel que fa als canvis introduïts respecte la versió analitzada al Dictamen 34/2014.

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, respectivament).

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

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

El principi de proporcionalitat desplega els seus efectes tant en relació amb els fitxers de dades que, segons la documentació aportada, han de formar part del projecte, com, en definitiva, de la informació que es podrà comunicar als possibles cessionaris o receptors de la informació.

El Document núm. 2 explicita que la informació que serà objecte de tractament *"està continguda en els fitxers declarats responsabilitat del Departament de Salut, del Servei Català de la Salut i de l'Institut Català de la Salut, que es troben regulats per l'Ordre SLT/25/2014, de 3 de febrer:"* En concret, el Document núm. 2 fa referència a:

El Fitxer estadístic d'enquesta de salut; el Fitxer estadístic d'estadística de causes de mort; el Fitxer de la història clínica; el Fitxer de patologies específiques; el Fitxer de prestació farmacèutica; el Fitxer de registre del conjunt mínim bàsic de dades (CMBD); el Fitxer de pacients de l'Institut Català de la Salut.

Respecte d'això, a efectes de claredat, es recomana fer referència al títol exacte dels fitxers regulats en l'Ordre SLT/25/2014, entre d'altres, en relació amb el "Registre de prestació farmacèutica" o el "Fitxer de pacients de la Divisió d'Atenció Primària de l'Institut Català de la Salut". Pel que fa al "Fitxer de la història clínica", cal dir que no es troba amb aquesta denominació regulat en la citada Ordre, i per tant convindria referir-se a la denominació exacta del fitxer regulat en la dita Ordre.

El fitxer estadístic d'enquesta de salut i el fitxer d'estadística sobre causes de la mort, citats, no són fitxers regulats per l'Ordre SLT/25/2014, citada, ja que són dos fitxers de tipus estadístic, inscrits a l'Institut d'Estadística de Catalunya (Idescat). En qualsevol cas, el Document núm. 2 inclou l'enllaç al web de l'Idescat, de manera que queda clar que aquests fitxers són fitxers estadístics.

Encara en relació amb la informació que serà objecte de tractament en el projecte VISC+, **es considera adequada la inclusió de la descripció dels fitxers que contenen la informació que tractarà VISC+, així com dels principals sistemes d'informació que generen, emmagatzemen i gestionen aquesta informació** (pàgines 5 a 16 Document núm. 2). Aquests quadres explicatius identifiquen la finalitat dels fitxers i els sistemes d'informació i clarifiquen la informació que es tractarà en el context del projecte.

No obstant això, en la documentació tramesa es fa referència a la futura incorporació de nova informació *"complint amb totes les mesures legals i de seguretat necessàries"* (pàg. 4 Document núm. 2). Òbviament la incorporació de nova informació requereix complir amb la normativa i les mesures de seguretat exigibles, però més enllà d'això, si la informació que s'incorpora difereix substancialment de la que s'ha previst inicialment (això succeiria, per exemple, si es pretengués incorporar al projecte informació de tipus genètic) seria necessari dur a terme, de nou, una avaluació dels riscos inherents a aquesta incorporació i de l'impacte que això pot tenir en la privacitat de les persones afectades.

En qualsevol cas, aquesta previsió haurà de ser interpretada d'acord amb les exigències del principi de qualitat, en la seva vessant de proporcionalitat i de minimització.

V

Encàrrec del tractament

L'apartat 4 del Document núm. 8, relatiu als *"Fluxos d'informació",* preveu el següent:

"Actualment les dades personals de salut resideixen en diferents ubicacions sota la responsabilitat dels titulars dels diferents fitxers.

Per tant, l'AQUAS, com a responsable de desenvolupar el Projecte VISC+, serà l'encarregada del tractament de dades personals de salut per a anonimitzar-les i posar-les a disposició de tercers interessats segons es descriu en l'apartat anterior. En aquest sentit i per donar compliment als requeriments de l'article 12 de la LOPD, els responsables dels fitxers encarreguen a l'AQUAS aquest tractament."

En relació amb aquesta qüestió, el Document núm. 9, aportat, consisteix en un *"Encàrrec de gestió que formalitzen el Departament de Salut, el Servei Català de la Salut i l'Institut Català de la Salut amb l'Agència de Qualitat i Avaluació Sanitàries de Catalunya."*

Aquest encàrrec de gestió, signat amb data 13 de novembre de 2014, ha estat objecte de publicació a través de la Resolució SLT/570/2015, de 16 de març, per la qual es fa públic un encàrrec de gestió que formalitzen el Departament de Salut, el Servei Català de la Salut i l'Institut Català de la Salut amb l'Agència de Qualitat i Avaluació Sanitàries de Catalunya (DOGC, núm. 6843, d'1.4.2015).

Aquest encàrrec de gestió inclou com a annex 2 el model d'encàrrec del tractament, d'acord amb l'art. 12 de l'LOPD, que haurà de signar cadascuna de les entitats responsables dels fitxers amb l'AQUAS.

Cal fer notar que pel que es desprèn de l'apartat referit a l'*"Abast i contingut de l'activitat encarregada"* del Document núm. 9, l'abast d'aquest encàrrec de gestió supera l'àmbit propi del projecte VISC+. Així, en l'encàrrec de gestió s'hi inclou:

"a) Anonimització de la informació continguda en els fitxers que contenen dades de caràcter personal del Departament de Salut, del Servei Catala de la Salut i de l'Institut Catala de la Salut amb dades de salut o centres assistencials d'interès per a la recerca i l'avaluació mediques, els quals es relacionen en l'Annex 1 del present encàrrec de gestió. Resten fora d'aquest encàrrec els fitxers de gestió interna del Departament de Salut, del Servei Català de la Salut i de l'Institut Catala de la Salut.

b) Utilització de la informació anonimitzada per algunes de les finalitats assenyalades en l'Annex 2.

c) Cessió a tercers d'informació anonimitzada per algunes de les finalitats assenyalades en l'Annex 2.

d) Cessió a tercers d'informació personal per a algunes de les finalitats assenyalades a l'annex 2, sempre que hi hagi consentiment previ de cadascun dels afectats per a la realització de la cessió i que es comprovi que el cessionari disposa d'una auditoria que demostra el compliment en totes les fases del tractament de la informació de totes les mesures exigides per la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, així com per la normativa que la desplega.

La cessió de dades identificables comporta que el cessionari es constitueix en responsable dels fitxers amb les obligacions que la normativa estableix a aquest respecte.

Les utilitzacions i cessions de dades indicades únicament abastaran les dades estrictament necessàries per a la finalitat concreta de cada actuació segons les finalitats assenyalades a l'annex 2 i que no resultin excessives, i de conformitat amb el

que estableixi la normativa vigent. Les cessions a tercers només es faran a entitats dedicades a la finalitat que es justifiqui per a la cessió de les dades i la qual estigui inclosa dins de les assenyalades a l'annex 2."

A la seva vegada, l'annex 2, al qual es remet l'apartat que acabem de reproduir, dins l'apartat "Serveis encarregats" inclou no només finalitats de recerca i avaluació (de fet no hi ha una referència expressa a l'avaluació del sistema sanitari) sinó també finalitats de tipus assistencial, administració i gestió de centres sanitaris, gestió sanitària per l'administració sanitària, inspecció per l'administració sanitària, estudis d'epidemiologia, docència i activitat estadística dins el Pla estadístic.

Per altra banda el document analitzat no explicita el nivell de mesures de seguretat alt que correspondria a les dades que són font d'informació del projecte VISC+, sinó que sembla admetre també fitxers de nivell de seguretat inferior.

Igualment, a la relació de fitxers inclosos en l'Annex 1 del Document núm. 9, es segueix incloent la següent fórmula (que aquesta Autoritat ja va considerar desaconsellable des de la perspectiva del principi de qualitat (FJ XIV del Dictamen 34/2014):

"I en el futur qualsevol altre fitxer del (responsable) amb dades de salut o centres assistencials d'interès sempre que es justifiqui per a algunes de les finalitats assenyalades en l'annex 2 (...)".

El Pacte segon de l'encàrrec de gestió (Resolució SLT/570/2015, citada), preveu expressament que *"L'encàrrec de gestió previst al pacte primer s'articula mitjançant un encàrrec de tractament que reuneix els requisits establerts en l'article 12 de la LOPD i del qual en té constància l'Autoritat Catalana de Protecció de Dades."*

Sobre això cal fer notar que el Dictamen 34/2014 es refereix només al projecte VISC+ que, segons es desprèn de la resta de la documentació adjuntada, inclou només l'anonimització de dades de salut per a la seva cessió amb finalitats de recerca i d'avaluació del sistema sanitari.

Per tant, la referència continguda al Pacte segon de l'encàrrec de gestió segons la qual l'Autoritat Catalana de Protecció de Dades té constància de l'encàrrec de gestió, és errònia, atès que aquesta autoritat només s'ha pronunciat respecte el projecte VISC+.

Respecte l'Annex 2 del Document núm. 9, que inclou el model relatiu a*"l'Encàrrec de tractament d'anonimització de dades i de cessió de dades anonimitzades i personals per a finalitats assenyalades en aquest annex."*, vistos els canvis substancials operats pel nou enfocament del projecte VISC+, que s'analitzen en aquest dictamen, l'encàrrec del tractament de dades a través del qual els responsables dels fitxers encarregaran a l'entitat el tractament i l'anonimització de dades, no pot referir-se a la "cessió de dades anonimitzades i personals", doncs VISC+ només pot comportar, en la seva concepció actual, cessió de dades anonimitzades.

Per tant, les mencions a cessions de dades personals i les remissions a finalitats que van més enllà de les de recerca i avaluació, no s'ajusten al dit nou enfocament de VISC+.

VI

Sobre el model de gestió del projecte

El model inicial de VISC+, s'articulava a través de la constitució d'un encàrrec del tractament 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 havia de permetre a l'entitat anonimitzar la informació per tal que un cop anonimitzada l'Adjudicatari la facilités als clients o usuaris finals.

En aquest esquema inicial, l'Adjudicatari s'havia 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. L'Adjudicatari també havia d'executar altres projectes o iniciatives relacionades amb VISC+, i crear un centre de competència en analítica en dades de salut, les funcions i composició del qual es descrivien en documentació que en el moment actual ja no és vigent (Document Tècnic).

Aquest esquema s'ha modificat substancialment en la versió del projecte que és objecte d'aquest dictamen (versió de març de 2015), tot i que hi ha alguns aspectes que no resulten prou clars:

En la Memòria del projecte (Document núm. 3), s'explicita que *"VISC+ serà gestionat i operat en la seva totalitat per l'Agència. També es comptarà amb un col·laborador extern que, mitjançant un contracte de serveis, desenvoluparà alguns elements necessaris perquè l'Agència pugui gestionar i operar VISC+ (per exemple: una plataforma que permeti l'anàlisi de les dades anonimitzades, continguts per al web o la creació d'algoritmes d'anàlisi estadístic)."*

En el mateix Document núm. 3 (apartat 6.2), es preveu que:

"La gestió del projecte VISC+ és pròpia des de l'Agència, que aportà la seva expertesa i coneixement sobre el sistema de salut català i les dades que s'hi generen. L'Agència també és qui tindrà tota la relació amb els potencials sol·licitants de serveis VISC+ (els centres de recerca públics de Catalunya).

No obstant, l'Agència comptarà amb un col·laborador extern que, mitjançant un contracte de serveis resultat d'un procés de diàleg competitiu, desenvoluparà alguns elements necessaris perquè l'Agència pugui gestionar i operar VISC+ (com per exemple: una plataforma que permeti l'anàlisi de les dades anonimitzades, continguts per al web o la creació d'algoritmes d'anàlisi estadístic)."

En el Document d'Anàlisi de riscos (Document núm. 4, pàgs. 6 i 7), s'explicita que aquesta anàlisi *"s'ha realitzat assumint la hipòtesi que el model de gestió del projecte VISC+ és el que implica una gestió realitzada de forma íntegra per l'Agència, amb els possibles col·laboradors externs participant exclusivament en la prestació de serveis a l'Agència."*

En aquest mateix apartat del Document núm. 4, es concreta, com a minimització del risc de dependència d'aquests col·laboradors, que l'entitat ostentarà el control, governança i execució del projecte, deixant les tasques més tècniques al possible col·laborador extern (mitjançant una col·laboració assimilada a un contracte de

serveis). S'afegeix la previsió que aquest contracte de serveis reguli uns acords de nivell de servei (ANS) dels quals se'n farà un control exhaustiu.

En l'apartat 3.2 del Document núm. 8, s'explicita que la governança del projecte és *"sempre i en exclusiva de l'Agència que serà qui farà tant l'anonimització de les dades i la seva custòdia, l'anàlisi de les sol·licituds que es rebin així com la seva aprovació (...)".)*

Sobre el model de gestió, el Document núm. 4, citat, remet al Document núm. 5, en el que s'analitzen els dos models alternatius:

- "VISC+ gestionat i operat integralment per l'Agència"
- "VISC+ gestionat i operat conjuntament entre l'Agència i col·laboradors"

Als efectes que ens interessen, en el primer model es preveu que l'entitat executi tots els aspectes tècnics i operatius, i s'afegeix que l'entitat és la responsable, entre d'altres, de *"construir tots els elements tecnològics del projecte: plataformes o programes d'explotació de les dades anonimitzades, pàgines web de comunicació, programes de control i auditoria, servidors i infraestructura de suport, etc".* En aquest primer model no es fa cap menció a la participació de cap col·laborador o agent extern, ni tan sols en relació amb tasques purament tècniques.

Pel que fa al segon model, sí admet la participació de col·laboradors, els quals seran responsables de (veure pàg. 8 Document núm. 5):

"- Crear els serveis VISC+, analitzant les necessitats concretes dels sol·licitants i construint-los (incloent els serveis d'anàlisi i estadística de dades, serveis d'informes maquetats en diversos formats com ara PDFs, infografies o pòsters, etc.). També caldrà assegurar que els serveis siguin flexibles (estiguin adaptats a les necessitats constants dels sol·licitants) i es creen i es lliuren el més ràpidament possible (en un temps raonable per al peticionari) i amb la qualitat esperada.

- Construir tots els elements tecnològics del projecte: plataformes o programes d'explotació de les dades anonimitzades, pàgines web de comunicació, programes de control i auditoria, servidors i infraestructura de suport, etc.

- Fer totes les inversions requerides, tant per l'adquisició de productes i serveis tecnològics (per exemple: llicències o serveis de desenvolupament), com la formació continuada en matèria d'anàlisi estadístic de grans volums de dades."

Ara bé, el citat Document núm. 5 no explicita quins dels dos models és el seleccionat, més enllà d'exposar els pros i contres dels dos models.

Analitzats conjuntament els documents 3, 4, i 8 de la nova versió de març de 2015, sembla deduir-se que el model triat és el segon dels dos models analitzats en el Document núm. 5, ja que el primer no preveu cap mena de col·laboració externa, i en base a la informació dels docs. 3 i 4 sí s'admetria la concurrència de col·laboradors externs.

Pel que fa a les funcions dels col·laboradors externs, malgrat que els docs. 3 i 4 fan referència a que el/s col·laborador/s durien a terme qüestions merament tècniques i de suport a l'entitat, el Document núm. 5 explicita, com s'ha esmentat, que els col·laboradors durien a terme tasques que clarament van més enllà de meres qüestions tècniques (crear serveis, analitzar sol·licituds, construir tots els elements tecnològics...).

Per tot això **seria molt recomanable que aquest Document núm. 5 explicités una conclusió i clarifiqués quin model es tria**, per tal de transmetre una informació clara als afectats. **També caldria aclarir el rol del/s col·laboradors/s,** en el sentit de si han de dur a terme qüestions merament tècniques com les que s'exemplifiquen (una plataforma que permeti l'anàlisi de les dades anonimitzades, continguts per al web o la creació d'algoritmes d'anàlisi estadístic, tal com es desprèn del Document núm. 3 (apartat 6.2)), o si seran responsables de tot el que es preveu al Document núm. 5 (pàg. 8, esmentada).

VII

Sobre la finalitat del tractament, els destinataris de la informació i els serveis previstos

Tal com hem vist, l'article 4.1 de l'LOPD preveu que la informació només pot tractar-se "*en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut."*

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

a) Finalitats del tractament

Pel que fa al principi de finalitat, l'LOPD exigeix que les finalitats per a les quals es tracti la informació siguin determinades, explícites i legítimes. Per això, caldrà examinar les previsions relatives a les finalitats que ha de tenir el projecte VISC+, per tal de verificar si s'ajusten a les exigències del dit principi.

En la documentació aportada, referida al nou enfocament del projecte VISC+, es defineix com un aspecte clau del mateix que la informació anonimitzada i descontextualitzada *"pot ser utilitzada només amb una finalitat de recerca mèdica o d'avaluació del sistema de salut."* (pàgs. 3 i 8 Document núm. 3).

Aquesta limitació de finalitats (estudis de recerca mèdica o d'avaluació del sistema de salut) també es preveu en l'apartat 2.2 del Document núm. 7, referit al *"Principi de compliment de finalitats legals".*

En versions anteriors del projecte, es preveia la possibilitat de tractar les dades en relació amb qualsevol de les finalitats legalment previstes, en el context de la normativa d'autonomia del pacient (Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i dels drets i obligacions en matèria d'informació i documentació clínica, i Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia dels pacient i la documentació clínica). Tenint en compte les consideracions del Dictamen 34/2014 referides al principi de finalitat, a les que ens remetem, es valora positivament que la nova versió del projecte reculli amb major claredat l'objectiu de VISC+, referit a les finalitats de recerca i d'avaluació del sistema de salut.

Ara bé en algun document (primer paràgraf de l'apartat 1 del Document núm. 3) la redacció que s'empra segueix essent força ambigua atès que es refereix a "alguna de les finalitats que preveu la llei", en lloc de referir-se expressament a la investigació i l'avaluació del sistema sanitari.

b) Destinataris de la informació

A diferència de les previsions inicials del projecte respecte les múltiples tipologies dels potencials "clients finals" de la informació, la documentació que ara s'analitza explicita que podran sol·licitar serveis a VISC+ els centres de recerca acreditats pel CERCA en l'àmbit de les ciències mèdiques i de la salut, i que VISC+ està orientat als investigadors dels centres de recerca públics de Catalunya que realitzin estudis de recerca i investigació (pàgs. 3 i 4 Document núm. 3). La documentació objecte d'anàlisi també limita els potencials sol·licitants de VISC+ als centres acreditats pel CERCA en d'altres apartats (Document núm. 5, Document núm. 3, entre d'altres).

Segons la informació disponible al web http://cerca.cat, i les previsions de la Llei 7/2011, del 27 de juliol, de mesures fiscals i financeres (arts. 64 i ss), la Institució CERCA (Centres de Recerca de Catalunya), és el mitjà propi i servei tècnic de l'Administració de la Generalitat de Catalunya per al seguiment, suport i facilitació de l'activitat dels centres de recerca del sistema CERCA, els quals es troben referenciats en el mateix web. Segons l'article 64.1 de la Llei 7/2011, els centres CERCA han d'ésser creats o participats per l'Administració de la Generalitat i, si escau, juntament amb una o més universitats o amb altres entitats públiques o privades.

Vist això, es recomana que les mencions fetes en la documentació aportada (Docs. 3 i 5), als "centres de recerca públics", es faci a "centres de recerca acreditats pel CERCA", a efectes de claredat, atès que, per la informació disponible, no es descarta que algun centre integrat a CERCA pugui tenir naturalesa jurídica privada.

Ara bé, segons l'apartat 5.2 del Document núm. 3, els serveis previstos de VISC+ van dirigits als següents grups de col·lectius:

- Centres de recerca acreditats pel CERCA (...).
- Agents del sistema sanitari integral d'utilització pública de Catalunya (SISCAT), que plantegin una necessitat de coneixement en relació amb la qualitat, efectivitat, eficiència, etc, dels serveis sanitaris o dels tractaments.

Aquesta previsió es confirma en l'apartat 2.1 (Document núm. 7), en el que també s'explicita l'exclusió de VISC+ de determinades tipologies de peticionaris (farmacèutiques, consultores, asseguradores de salut, empreses de col·locació o de contractació de personal, empreses publicitàries, de màrqueting o de prospecció comercial, etc). Si bé es considera pertinent que aquestes entitats no formin part de l'objectiu del projecte, no sembla clara la justificació que, en el cas de les empreses asseguradores, l'exclusió es limiti a les asseguradores en l'àmbit de la salut. Pensi's que tot i que el risc assegurat no sigui pròpiament la salut, la informació sobre la salut pot ser rellevant en altres tipus d'assegurances (p. ex. assegurances de vehicles).

En aquests termes, vistes les finalitats úniques de VISC+ (recerca i avaluació), és clar que no només els centres acreditats pel CERCA són els destinataris o "clients" de VISC+, sinó que també ho són els Agents del sistema sanitari d'utilització pública de Catalunya.

Per tant, als efectes de transmetre una informació el més clara i coherent possible entre tots els documents objecte de consulta, convindria afegir la referència als Agents del SISCAT com a destinataris dels serveis de VISC+, en aquells documents en què només es fa referència als centres acreditats de CERCA (entre d'altres, apartat 6.2 del Document núm. 3).

En la versió sotmesa a dictamen s'han suprimit les referències anteriors a l'àmbit internacional del flux informatiu en el context del projecte (Document núm. 5, entre d'altres) i en algun punt s'especifica que està orientat als investigadors dels centres de recerca públics de Catalunya (apartat 2 i apartat 6.2 del Document núm. 3). No obstant això, en algun altre document sí que es dóna entrada a la possibilitat que es tracti de centres d'investigació d'altres països (pàgina 5 del Document núm. 4 o pàgina 15 del Document núm. 8). Convindria aclarir aquest aspecte.

En definitiva, la informació aportada reflecteix que s'ha limitat les tipologies de clients finals, si bé segueix mancant algunes concrecions que s'han apuntat en aquest apartat.

c) Tipologia de serveis que són objecte de VISC+

La documentació aportada permet comprovar que s'ha reduït el nombre d'aquests serveis. Si inicialment VISC+ preveia el tractament de dades, anonimizades o no, en relació amb serveis de dades obertes; serveis de dades no obertes; 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, o altres serveis ad-hoc que no es concretaven, la documentació aportada (apartat 5.1 Document núm. 3) limita les tipologies de serveis a facilitar dades per a la realització d'estudis, realització d'anàlisis estadístiques i preparació d'informes.

La menció a que els conjunts de dades es destinen a investigadors en biomedicina que disposin de projectes de recerca, s'hauria de complementar amb la menció que aquests han d'estar integrats en centres CERCA, per coherència amb les previsions del projecte respecte els seus destinataris.

En qualsevol cas, vista la informació aportada, relativa a les finalitats previstes, als serveis oferts i als destinataris de les dades anonimitzades en el context del nou enfocament del projecte VISC+, i sens perjudici de les consideracions que s'acaben de fer, es considera adequat, des de la perspectiva dels principis de finalitat i de qualitat, que s'hagin clarificat i acotat tant **les finalitats** per a les quals es justifica el tractament de dades (investigació i avaluació), com **els grups o tipologies de clients finals o destinataris** (centres acreditats de CERCA i Agents del sistema sanitari integral d'utilització pública de Catalunya), així com **la tipologia de serveis oferts** (dades per a la realització d'estudis, realització d'anàlisis estadístiques i preparació d'informes).

VIII

Anonimització de les dades personals en el context del projecte VISC+

En origen, tal i com s'exposa en el Dictamen 34/2014, el projecte VISC+ preveia el tractament de dades personals i l'anonimització d'aquestes dades, a efectes de la seva

comunicació posterior a tercers, sense descartar la cessió i el tractament per part de tercers de dades de salut no anonimitzades.

Atès l'esquema plantejat inicialment, basat en un doble procediment de comunicació de dades anonimitzades i de dades personals, aquesta Autoritat va recomanar la prioritització del procediment de cessió de dades prèviament i degudament anonimitzades, tenint en compte que l'anonimització ofereix un tractament menys invasiu i de menor risc per als drets dels afectats. En concret, es va recomanar la prioritització de la cessió de dades 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 (FJ IX Dictamen 34/2014).

L'evolució del projecte VISC+ ha portat, segons la documentació que ara s'analitza, a circumscriure l'abast del projecte, exclusivament, al tractament i comunicació de dades anonimitzades per l'entitat. S'exclou del projecte, doncs, la possibilitat de comunicar dades de caràcter personal, en els termes en què es plantejava inicialment. Tal i com es desprèn de la documentació aportada, el projecte comportarà l'anonimització de tota la informació personal per part de l'entitat, abans de la seva comunicació a tercers, descartant d'aquesta manera la comunicació de dades personals de salut no anonimitzades als destinataris finals.

Així s'explicita en la documentació aportada, segons la qual VISC+ utilitzarà dades anonimitzades de salut (pàg. 3 Document núm. 2). A això s'afegeix, entre d'altres, que *"l'anonimització de les dades de salut i la custòdia de les dades ja anonimitzades serà realitzada per l'Agència, de forma que cap altra organització aliena a l'Agència o cap peticionari de dades tindrà mai accés a dades personals"* (pàg. 17 Document núm. 2, i pàg. 3 Document núm. 3).

En base a les consideracions exposades abastament en el Dictamen 34/2014, així com en ocasions posteriors, i vista la documentació aportada, **cal valorar positivament el nou posicionament del projecte VISC+,** ja que, més enllà de prioritzar, en el sentit apuntat per aquesta Autoritat, el tractament de dades anonimitzades, **limita l'abast del projecte a aquest flux informatiu en particular (comunicació de dades anonimitzades),** descartant la comunicació de dades personals no anonimitzades.

Sens perjudici d'això, i com ja ha posat de manifest l'Autoritat anteriorment, convindria matisar alguna afirmació inclosa en la documentació, per tal de transmetre una informació als afectats el més clara possible, respecte les implicacions de VISC+. En concret, ens referim a la previsió de l'apartat *"Riscos per a la ciutadania"* (pàg. 4 Document núm. 4), en el qual s'afirma que:

"(...) cal remarcar i fer èmfasi que durant el funcionament de VISC+ no s'utilitzaran dades personals, ja que el tractament i l'anàlisi estadístic es farà sobre dades anonimitzades".

Si bé és cert que, atesa la informació aportada, s'ha descartat la cessió de dades personals en el context de VISC+, tenint en compte el concepte de "tractament de dades" (article 3.c) LOPD), s'hauria d'aclarir que VISC+ sí tractarà dades personals en origen, ja que l'anonimització per part de l'entitat és una fase més del "tractament" de les dades. Convindria, doncs, matisar l'afirmació que VISC+ no utilitzarà dades personals.

Per altra banda, al Document núm. 8 a l'apartat 3.2.2.5 s'indica que "*Les dades que continguin informació personal o variables que permetin la identificació indirecta de les persones hauran de complir les mesures de seguretat ...*". Atesa l'evolució del projecte cal entendre que aquesta previsió s'està referint només a les dades que estiguin en poder de l'entitat i que encara no hagin estat sotmeses al procés d'anonimització, però en cap cas es pot referir a les dades disponibles pels clients finals atès que aquestes hauran de ser sempre anonimitzades. Tal com ja vam dir, les dades anonimitzades haurien de complir també les mesures de seguretat, però en aquest cas no es tractaria d'informació personal.

L'anonimització de la informació tractada constitueix doncs l'element clau del projecte i per això s'ha de dur a terme amb les majors garanties possibles. Per això cal tenir present que, ateses les potencialitats del tractament que ofereix l'entorn del *big data,* a l'hora de valorar la possibilitat de reidentificar una determinada persona, s'ha de tenir en compte l'evolució de la tecnologia disponible en cada moment i la informació disponible. I això inclou no només la informació anonimitzada aïllada que sobre aquella persona es pugui facilitar en el marc d'un determinat projecte, sinó també la informació que es pot facilitar en el marc d'altres projectes o la que estigui a disposició del sol·licitant o, en general, de qualsevol persona.

En el procés d'anonimització descrit en la documentació aportada (Document núm. 2, i Document núm. 8), es preveu eliminar la informació identificativa de persones físiques (dades identificatives, així com informació genètica), eliminar o reduir al mínim imprescindible el detall de la informació o altres variables que puguin donar lloc a identificacions indirectes, així com aplicar tècniques d'alteració de les dades. També es preveu atribuir un codi anònim de persona per tal de permetre relacionar els diferents conjunts de dades i aplicar un segon codi diferent per a cada projecte. Aquests codis s'hauran de crear mitjançant algoritmes que no permetin que terceres persones puguin relacionar-lo amb una persona concreta.

Ara bé, cal fer avinent que l'apartat referit al procés d'anonimització contingut en el Document núm. 8 (pàgina 7), difereix del mateix apartat del Document núm. 2 (pàgina 17), que recolliria la darrera versió del projecte. Els dos apartats dels dos documents citats, haurien de tenir el mateix contingut. Per tant, convindria substituir els punts 3 i 4 de l'apartat 3.2.2.2 del Document núm. 8, pels punts 3, 4 i 5 de l'apartat 4.1 del Document núm. 2.

Al marge d'això, aquestes previsions es consideren adequades, i també la previsió d'anonimitzar altres dades, com les dels professionals sanitaris que han atès el pacient, en línia amb les recomanacions del Dictamen 34/2014 (tot i que s'ha de fer notar que hi ha una discordança al punt 4 de l'apartat 3.2.2.2 del Document 8 que preveu anonimitzar les dades dels professionals sanitaris només en funció de la finalitat que es vulgui donar a certes dades. Aquesta previsió s'hauria de corregir en el sentit previst al punt 5 de l'apartat 4.1 del Document núm. 2).

Ara bé, en relació amb aquesta qüestió, aquesta Autoritat ja va posar de manifest que no sembla que la previsió d'eliminació d'informació relativa a persones jurídiques només sigui pertinent en cas de fitxers estadístics (punt 4 de l'apartat 4.1 Document núm. 2), perquè si en la resta de fitxers si ha inclòs informació d'aquest tipus (deduïble per exemple a través de la identificació del responsable del fitxer) també s'hauria d'eliminar. En principi, com a mesura d'anonimització, això s'hauria de preveure per qualsevol supòsit.

I també en la línia del que ja es va posar de manifest en el nostre anterior Dictamen, l'anonimització hauria d'afectar també les dades relatives al centre on ha estat atès el

pacient o codis geogràfics, en línia amb el que ja preveu l'apartat 2.9 del Document núm. 7.

IX

Garanties ètiques d'ús de les dades

Entre els documents nous aportats amb la sol·licitud d'aquest dictamen s'ha inclòs el document "*Garanties ètiques d'ús de les dades*" (Document núm. 7). En general aquest document estableix un seguit de principis a tenir en compte tant en el moment del desenvolupament del projecte, com en l'avaluació de la demanda i en el posterior seguiment de la utilització de la informació, que convé tenir en compte, i que resulten especialment rellevants.

No obstant això, a la vista de la documentació aportada convindria fer algunes precisions en relació amb diferents aspectes:

a) Procediment de gestió de la demanda:

Tot i que al llarg de la diferent documentació del projecte apareixen diferents mencions a aquest aspecte, la configuració final resulta força confusa.

L'apartat 5.1 del Document núm. 3 indica que, en els casos que ho estableixi la normativa vigent, caldrà que els projectes hagin passat per un CEIC. Per la informació aportada (apartat 6.1 del mateix Document núm. 3 i apartat 3.2.2 del Document 7), es preveu que totes les peticions han de ser sotmeses al CEIC, *"excepte en els casos de peticions d'estadística descriptiva o de peticions d'anàlisis destinades a un ús intern per part del sol·licitant que no hagin de ser publicats."*

Per altra banda, l'apartat 2.6 del Document 7 en preveure que es farà públic si les peticions aprovades *"han comptat amb l'aprovació del CEIC de referència de l'Agència o no"*, està admetent que la intervenció del CEIC no serà vinculant.

Encara respecte el rol del CEIC, fem notar que en l'apartat 3.2.1 del Document núm. 8 (pàg. 6), es preveu que el CEIC *"Tindrà com a principal funció la de vetllar per la correcta aplicació dels criteris científico-ètics en la gestió de la demanda, especialment en aquelles sol·licituds on calgui avaluar l'impacte per a la privacitat de les dades si es preveu que aquestes són de risc elevat."*

A la vista d'aquestes previsions, no queda molt clara quina serà la funció del CEIC en el procés de gestió de la demanda. Per una banda l'apartat 6.1 del Document 3 i 3.2.2 del Document 7 preveuen que totes les peticions han de comptar amb l'aprovació d'un CEIC (sembla que no hauria de ser necessàriament el CEIC al qual s'adscrigui l'entitat) "*excepte en els casos de peticions d'estadística descriptiva o de peticions d'anàlisis destinades a un ús intern per part del sol.licitant que no hagin de ser publicats"*. Per altra banda, l'apartat 5.1 es refereix només als casos en que "*ho estableixi la normativa vigent*", tot i que en aquest cas sembla que no s'està referint a la intervenció del CEIC de l'entitat, sinó al CEIC que correspongui a la institució que realitza la investigació. I l'apartat 6.3 del Document núm. 3 o el Document 8 atribueixen al CEIC vetllar per l'aplicació dels criteris científico-ètics, especialment en els casos de risc elevat.

Ateses aquestes discordances, sinó contradiccions, **convindria clarificar el paper del CEIC o dels CEIC en el procés de gestió de la demanda**, en el sentit de preveure la

necessitat d'intervenció del CEIC al qual s'adscrigui l'entitat en el procés d'aprovació de la demanda en tots els casos, sens perjudici de les funcions de seguiment que se li puguin atribuir especialment en aquells casos de risc elevat.

b) Principi de protecció de la privacitat

L'apartat 2.9 d'aquest document, relatiu al *"Principi de protecció de la privacitat"* inclou diferents principis i obligacions amb l'objecte de protegir la privacitat de les persones afectades.

Tot i que en termes generals el contingut d'aquest apartat resulta adequat des de la perspectiva de la protecció de dades, cal fer notar que en aquest apartat es preveu que: *"L'ús de dades anonimitzades mitjançant serveis VISC+ garanteix que no hi ha risc per a la privacitat de les persones".* Tenint en compte les consideracions del Dictamen 34/2014, convindria matisar aquesta afirmació, tenint en compte que el risc zero respecte la re-identificació d'informació prèviament anonimitzada no és assolible.

Al marge d'això, en aquest apartat es recull també com a principi "*la proporcionalitat de la petició, només accedint a les dades anonimitzades mínimes imprescindibles per donar cobertura a la petició*". Aquesta previsió també resulta pertinent, si bé podria ser bo afegir una referència "*en especial pel que fa a les dades de salut de les quals es pugui derivar unes majors conseqüències discriminatòries o estigmatitzadores per a les persones afectades*".

c) Obligacions que ha d'assumir el sol·licitant de la informació:

Dins d'aquest mateix apartat 2.9 al qual ens acabem de referir, es recull també la necessitat que l'entitat i el sol·licitant signin un conveni que estableixi les obligacions que assumeix el client pel que fa al respecte a la privacitat.

Seria bo que en aquest conveni s'inclogués també la previsió que la informació emprada s'ha de destruir un cop ja no sigui necessària pel projecte, i que això s'ha d'acreditar davant de l'entitat. A aquests efectes seria bo que en la sol·licitud s'indiqués el termini en què el sol·licitant es compromet a fer-ho.

I encara en relació amb aquest apartat resulta pertinent que s'hi incloguin les obligacions que assumeix el sol·licitant de les dades (no fer accions per reidentificar, comunicar situacions de risc de reidentificació, no destinar les altres dades a cap altra finalitat sotmetre's a auditories de l'Agència, o la mesura que s'acaba de proposar per a la destrucció de la informació un cop ja no sigui necessària per al projecte). Ara bé, ni en aquest document, ni en la resta de documents sotmesos a dictamen es fa cap referència a les conseqüències derivades de l'incompliment.

En la mesura que les accions que dugui a terme l'entitat receptora de la informació permetin reidentificar persones físiques, podria entrar en joc el règim sancionador previst a la normativa de protecció de dades o, fins i tot, el dret penal. Ara bé, en el cas que el sol·licitant incompleixi alguna de les seves obligacions sense que això impliqui reidentificar persones (per exemple, utilitzar les dades anònimes amb fins publicitaris, o dur a terme accions encaminades a la reidentificació encara que no s'assoleixi) no seria d'aplicació la normativa de protecció de dades. Per a aquests casos seria bo que aquest document preveiés que en el conveni també s'han d'incloure les mesures que es poden utilitzar en aquests casos (publicitat de l'incompliment, pèrdua del dret a sol·licitar nous conjunts d'informació, penalitzacions econòmiques etc.)

X

Exercici de drets ARCO i possibilitat d'opt-out

L'apartat 2.4 del Document núm. 7, relatiu al *"Principi de respecte dels drets del pacient",* disposa el següent:

"El projecte VISC+ es construeix a partir de dades anonimitzades de salut. D'aquesta manera, quan es tracten dades personals, els drets d'accés, rectificació, cancel·lació i oposició (ARCO) del pacient respecte de les seves dades personals no són d'aplicació.

No obstant això, l'Agència dóna suport al fet que els drets ARCO del pacient puguin continuar exercint-se davant dels responsables dels fitxers i addicionalment i, de forma complementària a aquests drets, l'entitat ofereix la possibilitat als pacients que ho demanin que les seves dades no siguin anonimitzades i incloses a VISC+ per fer recerca."

Respecte d'aquesta previsió, d'entrada, convindria matisar que els drets ARCO continuen essent d'aplicació respecte les dades personals d'origen (tractades en els diferents fitxers i sistemes d'informació que són font d'informació de VISC+), fins que es procedeixi a la seva anonimització per part de l'entitat. Per tant, els drets ARCO, i en especial el dret d'oposició (art. 6.4 LOPD), han de poder continuar exercint-se davant dels corresponents responsables dels fitxers.

En qualsevol cas, i més enllà de la possibilitat d'exercici del dret d'oposició, **cal valorar molt positivament que s'expliciti, en la documentació aportada, la possibilitat que els afectats exercitin *l'opt-out*** per tal de mantenir-se al marge del projecte VISC+, en el sentit que les seves dades no siguin anonimitzades ni incorporades a VISC+. És a dir, es preveu que els ciutadans podran decidir lliurement si volen que les seves dades s'exclouen d'aquest projecte. Cal tenir en compte que el dret d'oposició previst a la normativa de protecció de dades i que es pot exercir davant del responsable del tractament, requereix que la persona que l'exercita al·legui una causa justificada basada en al seva situació personal. En canvi, amb la incorporació del mecanisme *d'opt-out*, seria possible que aquelles persones que malgrat les garanties que ofereixi el sistema, no desitgin participar en el projecte, puguin fer-ho sense haver d'al·legar una justificació específica.

Ara bé, més enllà de la menció que se'n fa en el document examinat, amb l'objectiu de donar als afectats la millor informació possible, convindria explicitar l'abast i l'objectiu de *l'opt-out*, el mecanisme per exercir-lo, i les conseqüències que implicarà el seu exercici. A banda d'això, en el seu moment també caldrà preveure els corresponents formularis per exercir *l'opt-out*, així com la difusió informativa de la possibilitat d'exercir-lo.

En definitiva, de la mateixa manera que el correcte compliment del deure d'informació per part dels responsables de les dades (ex. art. 5 LOPD) és clau per tal que els ciutadans puguin exercir els drets ARCO -qüestió que aquesta Autoritat ha posat de manifest abastament-, una informació adequada sobre el projecte VISC+ (sobre l'anonimització que es produirà de les dades, sobre els destinataris de la informació, sobre les finalitats del projecte, etc), i també sobre la possibilitat d'exercir *l'opt-out* permetria als afectats prendre una decisió lliure i informada sobre la no participació en el projecte.

En aquest sentit també resulta positiu que s'hagi reforçat la transparència del projecte mitjançant la previsió de publicar les sol·licituds rebudes, el títol de la investigació, el grup de recerca que la promou, si ha estat aprovada o no i, si escau, els resultats de la recerca (apartat 2.6 del Document núm. 7 o apartats 1.7, 5.2 i 6.1 del Document núm. 3).

XI

Anàlisi de riscos

En el Dictamen 34/2014 es feia avinent la conveniència de tenir en compte, en el context del Projecte VISC+, les consideracions del Dictamen 5/2014 del Grup de Treball de l'Article 29, 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.

La incorporació al projecte d'un informe d'avaluació d'impacte sobre la privacitat de VISC+ (Document núm. 8), així com d'un informe d'anàlisi de riscos en relació amb el projecte (Document núm. 4), és, sense cap mena de dubte, una bona pràctica pel que fa a la protecció de dades.

Sens perjudici d'algunes consideracions que ja s'han fet anteriorment en relació amb el contingut d'aquests documents, i que no cal reiterar, cal assenyalar encara algunes qüestions.

En relació amb la re-identificació, l'apartat 3.2.2.4 del Document 8, preveu que quan s'identifiquin riscos de re-identificació es comunicarà a aquesta Autoritat, i l'Agència endegarà un pla d'acció per mitigar-ho, i evitar que es materialitzi aquest risc o que torni a aparèixer, previsions que es consideren adequades.

Pel que fa a altres previsions de l'apartat 5.2 del Document núm. 8 *"Riscos inicials i mesures de mitigació proposada"* (pàg. 14 i ss), cal fer notar les qüestions següents:

Pel que fa al risc "*No compliment dels requeriments de notificació dels tractaments a les Agències de Protecció de Dades corresponents (Catalana i/o Espanyola)*", s'ha de fer notar que atès que l'única entitat que tractarà dades de caràcter personal en aquest projecte és l'entitat que formula la consulta, les notificacions s'hauran de fer sempre a l'Autoritat Catalana de Protecció de Dades. La intervenció de l'Agència Espanyola de Protecció de Dades només s'hauria de produir, si escau, en el cas de transferències internacionals de dades (art. 41 en relació amb el 37.l) LOPD), però això s'hauria de preveure, si escau en l'apartat dedicat a la descripció dels riscos derivats de les transferències internacionals.

Pel que fa al risc *"No disposar de l'habilitació legal que legitimi a l'AQUAS a fer el tractament i la cessió de dades de salut",* i vista la nova orientació del projecte, s'hauria d'eliminar la menció a la cessió de dades de salut.

Pel que fa al risc "*Enriquiment de les dades personals de forma no prevista en les finalitats inicials al realitzar un creuament amb altres bases de dades de tercers*" s'indica que "*En cas que algun interessat vulgui creuar dades provinents de VISC+ amb altres fonts d'informació, la petició serà rebutjada automàticament*" però no s'indica de quins mitjans disposa l'entitat per detectar els casos en que l'interessat

"vulgui" fer-ho. Més que conèixer la voluntat de dur a terme el creuament, caldria referir-se als casos en què hi hagi indicis de que es pot dur a terme el creuament.

Pel que fa al risc d'ubicació de les dades fora del territori espanyol, s'ha de dir que, d'acord amb l'article 5.1.s) del RLOPD, només es considera transferència internacional el tractament de dades que suposa una transmissió d'aquestes dades fora del territori de l'Espai Econòmic Europeu. D'acord amb això, sembla que el risc s'hauria d'identificar amb la ubicació de les dades fora de l'Espai Econòmic Europeu. En qualsevol cas, convindria una clarificació d'aquest apartat i també de l'apartat 3.2.2.5 del Document núm. 8 atès que si les dades només es poden emmagatzemar a servidors dins l'espai econòmic europeu, i les dades que es comuniquen als clients són sempre anonimitzades, no tindria sentit la referència a l'autorització prèvia de l'AEPD continguda a l'apartat 3.2.2.5.

Pel que fa al risc *"Ús de les dades per finalitats no especificades o incompatibles amb les declarades pel sol·licitant (...)",* com a estratègia de mitigació es preveu *que "No es cediran ni tractaran dades personals ni anonimitzades per finalitats no especificades o no compatibles amb el sol·licitant i el què preveu la Llei."* Atesa la informació aportada, i vista la nova orientació del projecte, segons la qual la cessió de dades personals no es pot produir en cap cas (ni tan sols en relació amb les finalitats d'investigació i avaluació pròpies de VISC+), convindria eliminar d'aquesta frase la menció a la cessió de dades personals.

XII

Mesures de seguretat

Si bé el Projecte VISC+ suposa el tractament d'informació que haurà estat prèviament anonimitzada per l'entitat, aquesta Autoritat ha posat de manifest la conveniència de plantejar un model integral de seguretat de la informació per al conjunt del projecte VISC+, aplicable al tractament de dades, que vagi més enllà de les previsions de seguretat que preveu el títol VIII del RLOPD.

Tenint en compte les consideracions fetes per aquesta Autoritat (FJ XII Dictamen 34/2014, i posteriorment), en relació amb el model integral de seguretat, i vistes les modificacions que s'han anat incorporant al projecte, cal fer les següents consideracions.

En el Document núm. 2 es fa constar que les mesures de seguretat i anonimització han estat sotmeses a consideració de l'Apdcat i que s'han incorporat tots els seus suggeriments i recomanacions. En concret, la documentació aportada (punt 4, Document núm. 2, entre d'altres) explicita que VISC+ aplicarà les mesures de seguretat i control d'accessos que recomanen les ISO 27000/27001, com a millor pràctica en quant a estàndards internacionals respecte la gestió de seguretat de la informació. Això respon a una recomanació específica del Dictamen referit, per la qual cosa resulta adient.

Respecte les auditories de seguretat, la informació aportada hi fa referència en diversos documents. En l'apartat 4.2 del Document núm. 2, es preveu que:

"L'Agència realitzarà auditories per assegurar el correcte funcionament i compliment de les mesures de seguretat que implementi VISC+. Més concretament l'Agència executarà les següents mesures:

- Una auditoria inicial de seguretat, una vegada s'hagin anonimitzat les dades de salut per primera vegada.
- Implementar un model de verificació continua de l'aplicació dels procediments i resultats dels processos de seguretat, fent públics informes periòdics.
- Una auditoria completa cada 2 anys.
- Una auditoria per cada canvi rellevant en el projecte VISC+ que pugui tenir un impacte sobre la privacitat."

Com es feia avinent en el Dictamen 34/2014, *"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'AQUAS, 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)."*

En relació amb les previsions sobre auditories, en l'apartat 5.2 *"Riscos inicials i mesures de mitigació proposada"* (pàg. 16 Document núm. 8), es preveu que en *"fase d'operació de VISC+ ja es contempla la necessitat de realitzar noves auditories de qualitat de forma freqüent per detectar casos de risc".*

En el mateix apartat 5.2, citat, del Document núm. 8, es preveu que *"(...) el sol·licitant es compromet a que, si l'AQUAS ho considera, hagi de passar auditories posteriors per comprovar el compliment d'aquestes mesures".*

En la descripció del *"Principi d'avaluació externa"* (apartat 2.8 Document núm. 7), s'explicita que l'entitat implementarà un mecanisme d'auditoria continuada per a l'operació diària del projecte, previsió que s'ajusta a les consideracions del Dictamen 34/2014.

En definitiva, vistes les diferents previsions sobre auditories en la documentació que s'examina, i eliminada la participació d'un Adjudicatari amb el rol que aquest tenia atribuït en versions anteriors del projecte VISC+, sembla deduir-se que serà la pròpia Agència i, si aquesta ho considera oportú, els sol·licitants de dades anonimitzades, és a dir, els Centres de recerca acreditats pel CERCA i els diferents agents del sistema sanitari integral d'utilització pública de Catalunya (SISCAT), els que hauran de passar auditories.

Si és així, **es podria explicitar i clarificar quins han de ser els afectats per les auditories.**

En aquest sentit, vista la documentació aportada, no sembla que s'hagi previst cap mesura d'auditoria respecte els "col·laboradors externs", que realitzarien algunes tasques tècniques (veure, al respecte, l'apartat 4, Document núm. 4, així com el Document núm. 5). Tenint en compte el que s'ha esmentat respecte el rol que han de tenir aquests col·laboradors externs, i en funció de quina hagi de ser finalment aquesta participació de col·laboradors externs, es recomana valorar la previsió que, si l'entitat ho considera oportú, aquests col·laboradors externs hagin de passar un procés d'auditoria, en definitiva, incorporar-se en el procés d'auditoria continuada recomanat en el Dictamen 34/2014.

Tenint en compte els canvis que s'han anat produint en el projecte, aquest apartat referit a les auditories ja no inclou, lògicament, cap referència a l'Adjudicatari.

Ara bé, el contingut de l'apartat 3.2.2.3 del Document núm. 8, referit igualment a les auditories de seguretat, no sembla adaptat als canvis soferts pel projecte. Caldria, doncs, revisar-ne el contingut.

Cal referir-se també al contingut de l'apartat 3.2.2.6 del mateix Document núm. 8, sobre *"Altres requeriments de seguretat".* En aquest apartat es preveu *que "L'Agència haurà de preservar el model de seguretat, disponibilitat i ús de dades que estigui vigent a cada moment i no podrà utilitzar-les per cap altra finalitat ni facilitar-les a tercers. Aquestes obligacions s'estenen també als sol·licitants dels serveis i hauran d'estar recollits en el model de conveni que s'elabori per a ser signat entre l'Agència i el sol·licitant."*

Aquest paràgraf es refereix al model de seguretat, disponibilitat i ús de les dades, que configurava l'Annex 1 del Document Tècnic de la versió del projecte que va ser objecte d'anàlisi en el Dictamen 34/2014. Atès que, per la informació de què es disposa, tant el Document Tècnic com el seu annex ja no són vigents, convindria revisar aquesta previsió.

En el punt 3.2.2.3 del mateix Document 8 (pàg. 8) també es fa referència al dit "Model de seguretat, disponibilitat i ús de les dades", qüestió que caldria revisar en el mateix sentit apuntat.

Resulta pertinent la previsió de designar un delegat de protecció de dades per al projecte, per bé que en la documentació aportada (pàg. 4, Document núm. 4, entre d'altres) es fa constar que aquesta seria una recomanació inclosa en el Reglament CE 45/2001 del Parlament Europeu i del Consell, de 18 de desembre de 2000. Ara bé, cal puntualitzar que aquest Reglament només és aplicable a institucions i organismes de la UE, als quals aquest Reglament no recomana, sinó que imposa, la figura del delegat de protecció de dades a les institucions europees a les quals és d'aplicació.

Més enllà d'aquesta consideració formal, en el Dictamen 34/2014 es recomanava concretar, entre d'altres, alguns aspectes tècnics referits a la transmissió de dades a través de xarxes públiques o xarxes sense fil de comunicacions electròniques (article 104 RLOPD), en concret, concretar 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 recomanava preveure xifrar el canal de transport, així com xifrar en origen les dades objecte de transmissió.

Sobre això, en el Document núm. 2 s'explicita que tot el programari, els protocols i canals de comunicació que s'utilitzin comptaran amb els requisits de seguretat més elevats, entre d'altres, l'aplicació d'algoritmes de xifratge robustos, la restricció a nivell de xarxa filtrant adreces IP, o el xifratge de les transmissions.

L'apartat 4.3 del Document núm. 2 (pàgs. 18 i 19) recull diverses mesures de seguretat a les que es feia referència en el Dictamen, com ara l'aplicació de processos de codi de cas anònim o la comunicació d'incidències a l'Apdcat.

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

Conclusions

Es valora positivament el nou posicionament del projecte VISC+, que limita l'abast del projecte a la comunicació de dades anonimitzades, excloent la possibilitat de cedir dades personals.

Atesos els eixos fonamentals del nou enfocament del projecte VISC+ (l'eliminació de la possibilitat de comunicar dades personals, la limitació de les finalitats del projecte, així com la limitació dels destinataris), es fa avinent que les previsions del document d'Encàrrec de gestió formalitzat pel Departament de Salut, el Servei Català de la Salut i l'Institut Català de la Salut amb l'Agència (Document núm. 9), no s'ajusta al dit nou enfocament sinó que abasta altres aspectes no inclosos al projecte VISC+.

Es recomana explicitar el model de gestió seleccionat, per tal de transmetre una informació clara als afectats, així com aclarir el rol del col·laboradors externs, en el sentit de si han de dur a terme tasques merament tècniques, o de major abast. També es recomana explicitar i clarificar quins han de ser els subjectes afectats per les auditories.

Des de la perspectiva dels principis de finalitat i de qualitat, resulta adequat que s'hagin clarificat i acotat tant les finalitats per a les quals es justifica el tractament de dades (investigació i avaluació), com les tipologies de clients finals o destinataris (centres acreditats de CERCA i Agents del sistema sanitari integral d'utilització pública de Catalunya), així com la tipologia de serveis oferts, sens perjudici de les diverses consideracions fetes en relació amb la documentació analitzada.

Convindria clarificar el procés de gestió de la demanda, en especial pel que fa a la intervenció del CEIC al qual s'adscrigui l'entitat.

Caldria incorporar les previsions adients tant pel que fa a la destrucció de la informació un cop ja no sigui necessària per al projecte de recerca, com també les mesures que es poden aplicar en el cas que el sol·licitant incompleixi les obligacions que ha assumit.

Es valora positivament la transparència prevista pel que fa a les sol·licituds ateses, com també la possibilitat que els afectats exercitin *l'opt-out* per mantenir-se al marge del projecte VISC+. No obstant això, pel que fa a aquesta darrera qüestió convindria donar a aquest tema un protagonisme major en el projecte, a fi de transmetre una informació adequada als afectats.

Barcelona, 16 d'abril de 2015