CNS-60/2015

Dictamen en relació amb una consulta sobre la formalització de la proposta de conveni entre dues administracions públiques en l'àmbit de la cessió de dades i l'accés als sistemes d'informació necessaris per a la realització dels reconeixements mèdics d'embarcament marítim

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit emès per un departament de l'Administració de la Generalitat de Catalunya en què se sol·licita l'emissió d'un dictamen en relació amb la proposta de conveni de col·laboració entre aquest departament i una altra administració en l'àmbit de la cessió de dades i l'accés als sistemes d'informació necessaris per a la realització dels reconeixements mèdics d'embarcament marítim.

En concret, el departament sol·licita el parer d'aquesta Autoritat pel que fa a les previsions del conveni relatives a la seguretat en l'accés a les dades personals. Així mateix, planteja la necessitat d'adoptar altres previsions en matèria de seguretat.

S'adjunta a l'escrit de consulta còpia de l'esmentada proposta de conveni.

Analitzada la petició, vista la normativa vigent aplicable, l'informe del Coordinador d'Auditoria i Seguretat de la Informació de l'Autoritat i l'informe de l'Assessoria Jurídica, es dictamina el següent:

I

(...)

II

La proposta de conveni de col·laboració entre el Departament i una altra administració que s'examina té per objecte *"articular la cessió de dades de caràcter personal i l'accés als sistemes d'informació necessaris per a complir les funcions encomanades a (...) relatives als reconeixements mèdics d'embarcament marítim, permetent l'accés a les dades personals relatives a antecedents sanitaris necessaris per obtenir uns resultats més eficaços en matèria de salut laboral i de protecció de la salut dels treballadors que van a desenvolupar la seva activitat laboral embarcats"* (clàusula 2.1).

Tal com es recull en els antecedents de la proposta de conveni, correspon a aquesta altra administració la realització dels reconeixements mèdics d'embarcament marítim a què, de conformitat amb la normativa aplicable, s'han de sotmetre obligatòriament aquelles persones que desitgin exercir una activitat professional a bord d'un vaixell de bandera espanyola (Reial decret 1696/2007, de 14 de desembre, pel qual es regulen els reconeixements mèdics d'embarcament marítim).

Aquest tipus de reconeixements mèdics, equiparats als exàmens de salut previstos a la Llei 31/1995, de 8 de novembre, de prevenció de riscos laborals, tenen per finalitat detectar qualsevol malaltia que pugui presentar el treballador i agreujar-se especialment amb el treball al mar, o bé que pugui suposar un risc per a la resta de la tripulació o del passatge, fins i tot, un risc per a la navegació marítima (article 1 Reial decret 1696/2007).

Amb aquest propòsit, el Reial decret 1696/2007, citat, estableix les proves mèdiques a què hauran de sotmetre's les persones sol·licitants del reconeixement mèdic d'embarcament marítim (annex I), així com uns llistats d'aquells processos patològics i limitacions psicofísiques que el personal mèdic que efectua el reconeixement haurà de tenir en compte en la valoració de l'aptitud dels sol·licitants (annex II).

Disposar de la informació relativa als antecedents sanitaris de les persones que se sotmeten a aquests reconeixements mèdics, tal com pretén (...), sembla, en atenció a aquestes previsions, que podria permetre al personal mèdic efectuar una valoració més precisa de l'aptitud d'aquestes persones per a treballar al mar, així com establir una més eficient protecció de la seva salut.

Segons es manifesta a la consulta, aquesta informació personal es troba recollida en el fitxer Registre d'informació sanitària de pacients, relatiu a la història clínica compartida de Catalunya (HC3), del que n'és responsable el Departament.

No obstant això, al segon paràgraf del model d'obtenció de consentiment previst a l'annex de la proposta de conveni es fa referència genèrica a *"les bases de dades del Servei de la Salut".* Caldria, per tant, que en aquest document es concretés que la informació personal de salut a què (...) pretén accedir consta en l'esmentat fitxer del Departament.

La història clínica dels pacients dels serveis sanitaris de Catalunya es troba regulada en 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.

L'article 9.1 d'aquesta llei defineix la història clínica com *"el conjunt de documents relatius al procés assistencial de cada malalt tot identificant els metges i la resta de professionals assistencials que hi han intervingut*." I afegeix que *"s'ha de procurar la màxima integració possible de la documentació clínica de cada pacient. Aquesta integració s'ha de fer, com a mínim, en l'àmbit de cada centre, on hi ha d'haver una història clínica única per a cada pacient."*

Per la seva part, el seu article 10 defineix el contingut de la història clínica, distingint la informació que hi consta segons es tracti de dades d'identificació del malalt i de l'assistència, dades clinicoassistencials –entre les que consten els antecedents familiars i personals fisiològics i patològics del pacient- i dades socials.

Cal tenir present que les finalitats per a les quals podrà utilitzar-se la informació continguda en la història clínica venen determinades per aquesta mateixa llei, en concret, en el seu article 11, que disposa:

> *"1. La història clínica és un instrument destinat fonamentalment a ajudar a garantir una assistència adequada al pacient. A aquest efecte, els professionals assistencials del centre que estan implicats en el diagnòstic o el tractament del malalt han de tenir accés a la història clínica.*
> *2. Cada centre ha d'establir el mecanisme que faci possible que, mentre es presta assistència a un pacient concret, els professionals que l'atenen puguin, en tot moment, tenir accés a la història clínica corresponent.*
> *3. Es pot accedir a la història clínica amb finalitats epidemiològiques, d'investigació o docència, amb subjecció al que estableix la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, i la Llei de l'Estat 14/1986, de 25 d'abril, general de sanitat, i les disposicions concordants. L'accés a la història clínica amb aquestes finalitats obliga a preservar les dades*

d'identificació personal del pacient, separades de les de caràcter clinicoassistencial, llevat que aquest n'hagi donat abans el consentiment.
4. El personal que té cura de les tasques d'administració i gestió dels centres sanitaris pot accedir només a les dades de la història clínica relacionades amb les dites funcions.
5. El personal al servei de l'Administració sanitària que exerceix funcions d'inspecció, degudament acreditat, pot accedir a les històries clíniques, a fi de comprovar la qualitat de l'assistència, el compliment dels drets del pacient o qualsevol altra obligació del centre en relació amb els pacients o l'Administració sanitària.
6. Tot el personal que accedeix en ús de les seves competències a qualsevol classe de dades de la història clínica resta subjecte al deure de guardar-ne el secret."

El règim aplicable al tractament de les dades contingudes en la història clínica –en aquest cas, els antecedents sanitaris-, per tant, es troba en la interpretació conjunta i integrada del règim jurídic previst en la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, l'LOPD)) i de les previsions de la normativa sectorial aplicable a la història clínica.

III

Fetes aquestes consideracions inicials, convé fer avinent que, des del punt de vista de la protecció de dades, facilitar l'accés de (...) al sistema d'informació del Departament en què es conté la història clínica de la persona que se sotmet al reconeixement mèdic d'embarcament marítim en un centre de salut marítima -en concret, als seus antecedents sanitaris- constitueix una cessió de dades personals (article 3.i) LOPD) que, com a tal, s'ha de sotmetre al règim previst, amb caràcter general, per a les cessions o comunicacions de dades a l'LOPD.

L'article 11.1 de l'LOPD estableix que *"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".*

El mateix article disposa, en el seu apartat 2, que el dit consentiment no és necessari quan, entre d'altres excepcions, la cessió està autoritzada per una llei o norma amb rang de llei (lletra a).

Ara bé, tenint en compte la tipologia de dades personals a comunicar en el present cas, això és dades relacionades amb la salut (article 5.1.g) del Reglament de desplegament de l'LOPD, aprovat pel Reial decret 1720/2007, de 21 de desembre (RLOPD)), la dita cessió només és possible *"quan, per raons d'interès general, així ho disposi una llei o l'afectat hi consenti expressament",* de conformitat amb l'article 7.3 de la LOPD.

La proposta de conveni articula aquest accés de (...) al sistema d'informació del Departament relatiu a la història clínica per poder obtenir els antecedents sanitaris d'una determinada persona, als efectes de dur a terme una valoració de la seva aptitud per a treballar al mar, com una cessió de dades personals (clàusules 2.1 i 3.1) i estableix que, per tal de poder efectuar-la, cal obtenir el consentiment de les persones afectades, seguint el model que s'annexa al conveni (clàusula 3.3.b)).

Sens perjudici de valorar positivament aquestes previsions, convé fer avinent que, en atenció a allò establert a l'article 7.3 de l'LOPD, caldria fer constar en el conveni

(clàusula 3.3.b)) que aquest consentiment dels afectats per accedir als seus antecedents sanitaris ha d'ésser exprés.

Dit això, convé fer, en aquest punt, algunes consideracions en relació amb el model d'obtenció del consentiment previst a l'annex de la proposta de conveni, atès que, en atenció a la finalitat perseguida en el present cas, les previsions que s'hi recullen no resultarien adequades.

Com s'ha vist, de conformitat amb la clàusula 3.3.b) de la proposta de conveni, l'accés del personal mèdic de (...) a la informació sobre els antecedents sanitaris de què disposa el Departament parteix de la base de l'obtenció prèvia del consentiment (exprés) de la persona afectada. Aquesta mateixa clàusula estableix *in fine* que cal informar-ne al Departament (al Servei de la Salut).

Per tant, d'aquesta clàusula del conveni es desprèn que en el moment en què l'afectat acudeix a un dels centres de salut marítima de (...) a efectuar-se el corresponent reconeixement mèdic d'embarcament marítim el personal mèdic que l'atén li sol·licitarà el seu consentiment exprés per accedir als seus antecedents sanitaris, informació en poder del Departament.

En la petició d'aquest consentiment, per tant, (...) haurà d'informar l'afectat, de manera expressa, precisa i inequívoca, dels extrems de l'article 5 de l'LOPD, en concret:

> *"a) De l'existència d'un fitxer o un tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.*
> *b) Del caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades.*
> *c) De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.*
> *d) De la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.*
> *e) De la identitat i la direcció del responsable del tractament o, si s'escau, del seu representant."*

És a dir, d'entrada, en la sol·licitud del consentiment exprés de l'afectat (...) haurà d'informar-lo de:

- Les dades personals a què es pretén tenir accés. En aquest sentit, (...) haurà d'informar clarament l'afectat sobre les dades de salut a què es vol accedir. Si es tracta d'accedir al conjunt dels antecedents sanitaris que consten en la seva història clínica, caldrà informar-ne de manera clara.

- La finalitat per la qual es vol accedir a aquestes dades relatives als seus antecedents sanitaris. En aquest sentit, (...) haurà d'informar clarament l'afectat que l'accés té fins de salut laboral i de protecció de la seva salut com a treballador que pretén desenvolupar la seva activitat a bord d'un vaixell.

- La possibilitat de no donar aquest consentiment i de les conseqüències d'aquesta negativa. En aquest sentit, (...) haurà d'informar clarament l'afectat que l'atorgament del consentiment per accedir als seus antecedents sanitaris és totalment voluntari i que el fet de no atorgar-lo no condicionarà l'avaluació o qualificació del seu grau d'aptitud.

En aquest punt, cal assenyalar que, en atenció a la finalitat perseguida per (...), seria recomanable donar l'opció a l'afectat de consentir l'accés únicament a aquells antecedents sanitaris de la seva història clínica (no en el seu conjunt) que poden ser

rellevants per a la valoració de la seva aptitud professional, així com per a la vigilància de la seva salut. Ens referim, en concret, a aquells antecedents que estiguin relacionats amb els processos patològics i limitacions psicofísiques previstes a l'annex II del Reial decret 1969/2007. De fet, tal com s'explicita en el següent apartat d'aquest dictamen, per aplicació del principi de qualitat de les dades al cas examinat (article 4 LOPD), aquesta seria la informació estrictament necessària a què hauria de tenir només accés (...).

En cas que l'afectat atorgui el seu consentiment exprés per accedir a tots els seus antecedents sanitaris -o, si fos el cas, per accedir només als antecedents relatius a processos patològics i limitacions psicofísiques-, (...) també haurà d'informar-lo de:

- La incorporació de la informació obtinguda (els antecedents sanitaris de què es tracti) al corresponent fitxer de dades personals, del que n'és responsable (...).

- La possibilitat d'exercir els seus drets d'accés, rectificació, oposició i cancel·lació en relació amb el tractament d'aquesta informació amb la finalitat indicada.

Cal tenir present que, en la mesura que la comunicació de la informació personal s'articula en el present cas (clàusula 3.1) com una cessió de dades (article 11 LOPD) i no com un accés per compte de tercers (article 12 LOPD), un cop obtingut l'accés als antecedents sanitaris (...) esdevindrà responsable del tractament d'aquestes dades (article 3 d) LOPD) i restarà obligat a l'observança de la resta de disposicions de l'LOPD (article 11.5).

En atenció a aquestes consideracions, convé assenyalar, en aquest punt, la necessitat de modificar la clàusula 3.3.i) de la proposta de conveni.

Ara bé, d'acord amb el model de l'annex de la proposta de conveni, sembla desprendre's que el Departament seria qui sol·licitaria el consentiment exprés de l'afectat per a la cessió de les seves dades relatives als seus antecedents sanitaris a (...), fet que, en atenció al clausulat de la proposta de conveni a què s'ha fet referència, resultaria contradictori, atès que la comunicació al Departament de les persones que passen el reconeixement mèdic a (...) només té sentit si es compta amb el consentiment previ i exprés de la persona afectada.

Tampoc és adequada la informació que es dóna en aquest model pel que fa al fitxer de dades personals en què s'incorporaran els antecedents sanitaris de l'afectat. En aquest imprès s'estableix que la dita informació personal s'inclourà en dos fitxers dels que és responsable el Departament quan en realitat hi hauria de constar la denominació del fitxer de (...), atès que és aquesta entitat la que recull, previ consentiment exprés, les dades de salut de l'afectat.

En atenció a aquestes consideracions, caldria modificar la informació que es facilita a l'afectat a través d'aquest imprès d'obtenció del consentiment, de tal manera que quedi clar que el consentiment el sol·licita (...).

Així mateix, caldria incloure en aquest imprès la informació a què s'ha fet referència abans: dades a què es pretén accedir, finalitat de l'accés, caràcter voluntari del consentiment, conseqüències de la negativa a atorgar-lo i, en cas de consentir l'accés, fitxer en què s'inclouran les dades personals, identitat de (...) com a responsable del fitxer i possibilitat d'exercir els drets d'*habeas data*.

IV

Establert que l'accés de (...) al sistema d'informació del Departament es configura com una cessió de dades, és important que aquesta comunicació es dugui a terme de conformitat amb els principis i obligacions de la normativa de protecció de dades, especialment, amb el principi de qualitat de les dades (article 4 LOPD).

Aquest principi estableix que *"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"* (article 4.1 LOPD).

Així doncs, l'accés de (...) (del seu personal mèdic) a la informació de què disposa el Departament haurà de respondre a l'exercici d'una finalitat legítima, haurà de limitar-se a les dades personals mínimes necessàries per assolir aquesta finalitat i només haurà de produir-se en relació amb les persones que se sotmetin al reconeixement mèdic d'embarcament marítim i que, com s'ha vist, hagin prestat el seu consentiment previ i exprés.

La clàusula 2.3 de la proposta del conveni ve a recollir aquestes previsions relatives al principi de qualitat de les dades en establir que *"(...) pot tenir accés i tractar les dades de caràcter personal contingudes en els sistemes als quals se li concedeixi permís d'accés, sempre que això sigui imprescindible per a l'execució dels treballs, activitats i/o de les obligacions contretes en virtut del present conveni, i en tot cas es limita a la informació de caràcter sanitari dels candidats que vulguin exercir una activitat professional a bord d'un vaixell de bandera espanyola."*

Tot i valorar aquesta previsió de manera positiva, per tal d'adequar-la plenament al citat principi de qualitat de les dades, caldria especificar que:

- El sistema d'informació a què el personal mèdic de (...) tindrà accés és el relatiu a la història clínica compartida de Catalunya.

- La informació de caràcter sanitari a què es tindrà accés correspon exclusivament als antecedents sanitaris dels candidats que vulguin exercir una activitat professional a bord d'un vaixell de bandera espanyola i que hagin prestat el seu consentiment previ i exprés (no el conjunt d'informació sanitària continguda en llur història clínica).

Dit això, convé puntualitzar que aquest accés als antecedents sanitaris resultaria més adequat, des del punt de vista del principi de qualitat de les dades, si es limités només a aquells antecedents de la història clínica dels candidats relacionats amb els processos patològics i les limitacions psicofísiques que el personal mèdic que efectua el reconeixement mèdic ha de tenir específicament en compte en l'avaluació de l'aptitud de l'afectat, de conformitat amb l'annex del Reial decret 1969/2007, en tractar-se de la informació personal mínima necessària per assolir la finalitat pretesa per (...).

Per aquest motiu, es recomana valorar la conveniència d'establir en la proposta de conveni que l'accés de (...) al sistema d'informació del Departament relatiu a la història clínica compartida de Catalunya, als efectes d'obtenir la informació personal necessària per assolir uns resultats més eficaços en matèria de salut laboral i de protecció de la salut dels treballadors al mar, a banda d'efectuar-se previ consentiment exprés de l'afectat, es limitarà en qualsevol cas als antecedents sanitaris relatius a processos patològics i limitacions psicofísiques en els termes previstos en la normativa sectorial aplicable.

Això, val a dir, no treu que (...) pugui, tal com s'estableix ara en el conveni, accedir al conjunt d'antecedents sanitaris que consten en la història clínica de l'afectat si ha obtingut el seu consentiment previ i exprés. Ara bé, convé reiterar que, en aquest cas, (...) ha d'haver informat expressament l'afectat que el consentiment sol·licitat es refereix a l'accés a la totalitat dels antecedents sanitaris de llur història clínica, entre d'altres qüestions (article 5 LOPD).

Per altra banda, aquest mateix principi de qualitat de les dades, en la seva vessant de conservació, estableix que *"les dades de caràcter personal han de ser cancel·lades quan hagin deixat de ser necessàries o pertinents per a la finalitat per a la qual han estat recollides o registrades. No han de ser conservades de manera que permetin identificar l'interessat durant un període superior al necessari per a les finalitats d'acord amb les quals hagin estat recollides o registrades"* (article 4.5 LOPD).

En aquest sentit, la clàusula 3.3.f) de la proposta de conveni disposa que *"(...) no pot fer còpies, bolcats o qualsevol altra operació de conservació de dades amb finalitats diferents de les establertes en aquest conveni amb relació a les dades de caràcter personal a les que tingui accés*".

És clar que, un cop obtingut l'accés als antecedents sanitaris i incorporada aquesta informació personal al corresponent fitxer de dades personals, (...) només podrà conservar aquestes dades mentre siguin necessàries per assolir la finalitat per a la qual han estat recollides, això és valorar l'aptitud de l'afectat per al desenvolupament de la seva activitat professional com a treballador al mar i per establir una més eficient protecció de la seva salut. En aquest sentit, cal valorar també positivament aquesta previsió.

V

Dit això, s'analitza a continuació la qüestió concreta plantejada pel Departament en el seu escrit de consulta, això és l'adequació de les previsions de la proposta de conveni en matèria de seguretat en l'accés a les dades personals, així com la necessitat, si escau, d'afegir-ne d'altres.

La normativa de protecció de dades personals imposa l'obligació al responsable del tractament i, si s'escau, a l'encarregat del tractament d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries per tal de garantir la seguretat de les dades personals que seran tractades, així com per evitar la seva alteració, pèrdua, tractament o accés no autoritzat (article 9 LOPD).

Aquestes mesures de seguretat venen regulades en el Títol VIII del RLOPD, que les classifica en tres nivells diferents –bàsic, mitjà i alt- en funció de la tipologia de dades personals que en cada cas es prevegin tractar. Aquestes mesures tenen caràcter acumulatiu, de tal manera que les establertes per a cada nivell exigeixen incorporar les previstes per als nivells inferiors.

Quan la informació personal sotmesa a tractament comprèn dades relatives a la salut (com en aquest cas), cal tenir implantades, a banda de les mesures de nivell bàsic i mitjà, les mesures de nivell alt (article 81.3.a) RLOPD), en concret, tractant-se d'un tractament automatitzat, les descrites en els articles 89 a 104 del RLOPD consistents en:

a) L'elaboració d'un document de seguretat on es fixin les obligacions i funcions dels usuaris o perfils d'usuaris que accedeixin a les dades, una descripció del sistema

informàtic i una definició de les funcions de control o autoritzacions delegades pel responsable del fitxer o tractament (article 89 RLOPD).
b) L'establiment d'un registre d'incidències (articles 90 i 100 RLOPD).
c) L'establiment d'un control d'accés (article 91 RLOPD).
d) La correcta gestió de suports i documents (articles 92, 97 i 101 RLOPD).
e) L'adopció de mesures que garanteixin la correcta identificació i autenticació dels usuaris (articles 93 i 98 RLOPD).
f) L'establiment de processos de còpies de seguretat i recuperació de les dades (articles 94 i 102 RLOPD).
g) L'assignació d'un o diversos responsables de seguretat (article 95 RLOPD).
h) La realització d'auditories de seguretat (article 96 RLOPD).
i) L'establiment d'un control d'accés físic (article 99 RLOPD).
j) L'establiment d'un registre d'accessos (article 103 RLOPD).
k) L'establiment de mecanismes de xifratge, en cas de transmissió de les dades a través de xarxes públiques o xarxes sense fil de comunicacions electròniques (article 104 RLOPD).

En el cas ara examinat es parteix de la base que el Departament, com a responsable del fitxer en què es conté la història clínica compartida de Catalunya i a què (...) tindria accés pel que fa a la informació relativa als antecedents sanitaris en virtut del conveni que ara s'examina, té implantades totes les mesures de seguretat a què s'ha fet referència en els seus sistemes d'informació i infraestructures tècniques. De la mateixa manera es presumeix que (...) també té implantades aquestes mesures de seguretat respecte els seus fitxers i sistemes d'informació.

Per tant, en el present dictamen s'examinen només aquells aspectes en matèria de seguretat que resulten rellevants en la mesura que en la proposta de conveni es preveu l'accés al sistema d'informació en què es conté la dita història clínica per part d'una entitat aliena al Departament, això és (...).

VI

La clàusula 2.4 de la proposta de conveni estableix que en l'accés a les dades de salut dels ciutadans per part de (...) (i, en general, al seu tractament) és exigible el nivell de seguretat més alt, de conformitat amb el RLOPD, previsió que es valora positivament.

Per la seva part, la clàusula 3 de la proposta de conveni conté una sèrie d'instruccions que el personal mèdic de (...) ha de seguir per tal de poder accedir a aquestes dades (antecedents sanitaris) contingudes en el sistema d'informació del Departament.

Entre d'altres qüestions (examinades en els apartats anteriors d'aquest dictamen), en aquesta clàusula es recullen adequadament diverses previsions en relació amb l'obligació de totes aquelles persones que intervenen en el tractament de les dades personals (el personal de (...) autoritzat per accedir al sistema d'informació) de complir amb les corresponents mesures de seguretat i de mantenir el secret professional pel que fa a aquestes dades, així com en relació amb l'obligació de (...) de garantir que el seu personal compleix el conjunt d'obligacions previstes a l'LOPD. En concret, estableix que:

"2) Als efectes de l'accés i del tractament, (...) queda obligat amb caràcter general pel deure de confidencialitat i seguretat de les dades de caràcter personal.
(...)

3) (...)
c) En totes les previsions de les activitats que formen part de l'exercici de les seves funcions, cal aplicar les mesures d'índole tècnica i organitzativa que

estableix l'article 9 de la LOPD, per tal de garantir la seguretat de les dades de caràcter personal i evitar l'alteració, la pèrdua i el tractament no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposades, tant si provenen de l'acció humana com dels mitjans físic o natural.
d) És imprescindible obligar el secret professional en relació a les dades de caràcter personal a les persones que intervinguin per compte de (...) en qualsevol fase del tractament de les dades. Aquesta obligació subsisteix fins i tot després que s'hagi extingit la seva relació de col·laboració amb el Servei de Salut.
(...)
e) (...) ha de comunicar i fer complir als seus empleats i a qualsevol personal que tingui accés a les dades de caràcter personal les obligacions establertes en els apartats anteriors, especialment les relatives al deure de secret i a les mesures de seguretat.
(...)."

Aquestes previsions, que cal valorar positivament, s'ajusten a l'article 9 de l'LOPD, ja citat, en relació amb l'article 89 del RLOPD, i a l'article 10 de l'LOPD, relatiu al deure de secret i que s'ha d'interpretar en connexió amb l'article 11.3 de la Llei 21/2000, citada. Tot i així, convé fer dues puntualitzacions al respecte:

- Pel que fa a la previsió de guardar el secret professional (clàusula 3.3.d)), fer avinent que l'obligació de mantenir el deure de secret respecte les dades a què s'ha tingut accés persisteix, no només més enllà de la finalització del conveni de col·laboració entre (...) i el Departament, sinó també després d'extingir-se la relació contractual que el personal mèdic mantingui amb (...). Per tant, la referència al Servei de Salut que conté el primer paràgraf d'aquesta clàusula 3.3.d) s'ha de fer a (...).

- Pel que fa a la previsió de que (...) garanteixi que el seu personal compleix amb les obligacions establertes *"en els apartats anteriors"* del conveni (clàusula 3.3.e)), atès que els apartats següents de la clàusula 3 també contenen altres obligacions convindria modificar aquesta previsió per referir-se a tota la clàusula 3.

L'esmentada clàusula 3 de la proposta de conveni també recull adequadament l'obligació del personal de (...) d'informar immediatament el Departament sobre qualsevol incidència que afecti les dades personals a què es tingui accés, en la mesura que, en aquell moment, és usuari del seu sistema d'informació relatiu a la història clínica (apartat 3.g)).

Aquesta previsió concordaria amb l'article 90 del RLOPD, relatiu al registre d'incidències, que exigeix establir un procediment de notificació i de gestió d'incidències, per la qual cosa es valora positivament.

Per altra banda, aquesta mateixa clàusula 3, en el darrer paràgraf del seu apartat 3.d), recull l'obligació de (...) de complir els *"procediments d'identificació, autenticació i control d'accés d'usuaris en els sistemes d'informació del Servei de Salut"* i afegeix especialment que *"ha de comunicar les altes i baixes d'usuaris que es produeixin en relació amb els empleats de la seva organització, d'acord amb les instruccions facilitades en cada moment pel Servei de Salut".*

Els requisits que han de complir aquests mecanismes d'identificació i autenticació, així com el control d'accés a què es fa referència venen establerts, respectivament, als articles 93 i 98 del RLOPD, i a l'article 91 del RLOPD:

"Article 93. Identificació i autenticació
1. El responsable del fitxer o tractament ha d'adoptar les mesures que garanteixin la correcta identificació i autenticació dels usuaris.
2. El responsable del fitxer o tractament ha d'establir un mecanisme que permeti la identificació de forma inequívoca i personalitzada de qualsevol usuari que intenti accedir al sistema d'informació i la verificació conforme està autoritzat.
3. Quan el mecanisme d'autenticació es basi en l'existència de contrasenyes, hi ha d'haver un procediment d'assignació, distribució i emmagatzematge que en garanteixi la confidencialitat i integritat.
4. El document de seguretat ha d'establir la periodicitat, que en cap cas ha de ser superior a un any, amb què s'han de canviar les contrasenyes que, mentre estiguin vigents, s'han d'emmagatzemar de forma inintel·ligible."

"Article 98. Identificació i autenticació
El responsable del fitxer o tractament ha d'establir un mecanisme que limiti la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació."

"Article 91. Control d'accés
1. Els usuaris han de tenir accés només als recursos que necessitin per a l'exercici de les seves funcions.
2. El responsable del fitxer s'ha d'encarregar que hi hagi una relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cadascun d'ells.
3. El responsable del fitxer ha d'establir mecanismes per evitar que un usuari pugui accedir a recursos amb drets diferents dels autoritzats.
4. Exclusivament el personal autoritzat per fer-ho en el document de seguretat pot concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, de conformitat amb els criteris que estableix el responsable del fitxer.
5. En cas que existeixi personal aliè al responsable del fitxer que tingui accés als recursos, ha d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi."

La clàusula 3.3.d) esmentada no especifica en què consisteixen els mecanismes d'identificació i autenticació, així com el control d'accés implantats pel Departament en el seu sistema d'informació relatiu a la història clínica. Si bé s'entén que es troben especificats en llur document de seguretat (article 88 RLOPD) podria ser convenient fer-hi també referència en la proposta de conveni. En qualsevol cas, es recorda que, com a mínim, aquests s'han d'adequar a les previsions del RLOPD citades.

Ara bé, en atenció a què la informació a què (...) tindrà accés comprèn dades relatives a la salut, caldria necessàriament afegir a la proposta de conveni, en aquesta mateixa clàusula o bé en una altra, la previsió de que tots els accessos que realitzi llur personal prèviament autoritzat seran registrats, en aplicació i segons els requisits previstos a l'article 103 del RLOPD.

Aquest article 103 del RLOPD, relatiu al registre d'accessos, estableix que:

"1. De cada intent d'accés s'han de guardar, com a mínim, la identificació de l'usuari, la data i hora en què es va realitzar, el fitxer a què s'ha accedit, el tipus d'accés i si ha estat autoritzat o denegat.
2. En cas que l'accés hagi estat autoritzat, és necessari guardar la informació que permeti identificar el registre a què s'ha accedit.
3. Els mecanismes que permeten el registre d'accessos han d'estar sota el control directe del responsable de seguretat competent sense que hagin de permetre la seva desactivació ni manipulació.

4. El període mínim de conservació de les dades registrades és de dos anys.
5. El responsable de seguretat s'ha d'encarregar de revisar almenys una vegada al mes la informació de control registrada i ha d'elaborar un informe de les revisions realitzades i els problemes detectats.
6. No és necessari el registre d'accessos definit en aquest article en cas que es donin les circumstàncies següents:
a) Que el responsable del fitxer o del tractament sigui una persona física.
b) Que el responsable del fitxer o del tractament garanteixi que únicament ell té accés a les dades personals i les tracta.
La concurrència de les dues circumstàncies a què es refereix l'apartat anterior s'ha de fer constar expressament en el document de seguretat."

Dit això, es recomana afegir en la proposta de conveni la previsió que el Departament verificarà periòdicament l'activitat dels usuaris del seu sistema d'informació, amb la finalitat de determinar si algun d'ells no estan fent ús de l'accés atorgat o bé un ús que pugui ser inadequat i, si fos el cas, prèvia consulta amb (...), procedir a la suspensió temporal de l'accés si així es considera convenient.

Per altra banda, es troba a faltar en la proposta de conveni alguna previsió relacionada amb els mecanismes establerts per protegir les dades en la seva transmissió.

L'article 85 del RLOPD preveu que *"les mesures de seguretat exigibles als accessos a dades de caràcter personal a través de xarxes de comunicacions, siguin públiques o no, han de garantir un nivell de seguretat equivalent al corresponent als accessos en mode local, conforme als criteris que estableix l'article 80."*

Addicionalment, l'article 104 del RLOPD, aplicable a l'accés a dades que requereixen l'aplicació de mesures de seguretat de nivell alt, estableix que *"(...) 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 esmentades o bé utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers."*

Atès que correspon al Departament garantir l'adopció d'aquestes mesures respecte el seu sistema d'informació, convé recordar que l'accés a les dades per part de (...) s'haurà de realitzar mitjançant un protocol que impliqui el xifrat de les comunicacions.

Dit això, seria recomanable afegir a la proposta de conveni la previsió que (...), per la seva part, protegirà i configurarà les xarxes des d'on es realitzi l'accés al sistema d'informació del Departament per tal d'impedir que, un cop la comunicació quedi desxifrada, les dades puguin ser accessibles o manipulades per terceres persones.

També seria recomanable afegir a la proposta de conveni la previsió que (...) adoptarà les mesures de seguretat necessàries per evitar que programari maliciós pugui infectar les seves estacions de treball (programari espia o troians) i així capturar la informació a què s'hagi tingut accés o bé les credencials dels seus usuaris del sistema d'informació del Departament (en cas d'emprar, com a mecanisme d'identificació i autenticació, un usuari i contrasenya).

Arribats a aquest punt, convé assenyalar que totes aquestes previsions sobre les mesures de seguretat que es deriven de l'accés previst en la proposta de conveni examinada haurien de recollir-se en el document de seguretat, tant del Departament com de (...) (article 88 RLOPD). Per aquest motiu, caldria que el conveni recollís expressament la previsió de que ambdues entitats actualitzaran en aquest sentit els seus respectius documents de seguretat.

Finalment, en la línia apuntada en l'escrit de consulta, es recomana adequar la informació que amb caràcter preventiu es faciliti als usuaris de (...) abans d'accedir al sistema d'informació del Departament, de tal manera que l'usuari sigui coneixedor sense donar lloc a equívocs de la finalitat per a la qual se li ha concedit l'accés, així com de les conseqüències que es deriven d'aquest accés, com ara, la monitorització de la seva activitat.

D'acord amb les consideracions fetes en aquest dictamen en relació amb la consulta plantejada, es fan les següents,

Conclusions

L'accés de (...) a dades de la història clínica de les persones que ho hagin autoritzat es considera adequat, tot i que caldria modificar determinades previsions establertes en el model d'obtenció del consentiment que figura com annex a la proposta de conveni, com també convindria establir previsions per limitar la informació a la qual s'accedeix a la mínima necessària per assolir la finalitat pretesa.

Examinades les previsions en matèria de seguretat en l'accés a les dades de la proposta de conveni, es considera necessari incorporar-hi informació sobre el registre d'accessos (article 103 RLOPD) i la protecció de les xarxes de comunicacions (articles 85 i 104 RLOPD), així com la previsió que ambdues entitats actualitzaran llurs documents de seguretat (article 88 RLOPD).

Es recomana incloure en la proposta de conveni, com a mesures de seguretat addicionals, la verificació periòdica de la utilització dels comptes d'usuaris per part del Departament, la protecció de les xarxes i estacions de treball per part de (...) i l'adequació dels avisos que es facilitin als usuaris abans d'accedir al sistema d'informació, en els termes apuntats en aquest dictamen.

Barcelona, 17 de desembre de 2015