CNS 29/2012

Dictamen en relació amb la consulta formulada per una Administració Pública competent en matèria de salut sobre la possibilitat d'utilitzar mecanismes d'accés a les dades de salut alternatius al certificat digital

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'una Administració Pública competent en matèria de salut, amb el qual sol·licita el parer d'aquesta Autoritat sobre la possibilitat d'aplicar mecanismes d'accés alternatius als certificats digitals per l'accés dels ciutadans a les seves dades de salut usant la "Carpeta Personal de Salut" o altres sistemes electrònics que pugui promoure l'Administració Pública competent en matèria de salut o les entitats sanitàries de Catalunya, així com el nivell de seguretat que es requereix per accedir a la informació mèdica d'un mateix.

Analitzada la consulta, i vist l'informe de l'Assessoria Jurídica s'emet el següent dictamen.

I

(...)

II

La carpeta personal de salut, segons definició del web de la mateixa Administració Pública, és *"un espai digital, personal i intransferible de consulta que permet a la ciutadania disposar de la seva informació personal de salut i utilitzar-la d'una forma segura i confidencial, a més de facilitar-li la realització de tràmits electrònics".* Permetrà doncs als ciutadans un accés a les dades més rellevants de la seva història clínica.

En el mateix web es dóna la següent informació sobre la carpeta personal de salut:

> "La carpeta personal de salut conté la informació generada durant els actes assistencials que hagin tingut lloc en algun dels centres que formen part del Sistema sanitari integral d'utilització pública de Catalunya (SISCAT). Aquesta informació ha de ser publicada pels centres a la Carpeta per tal que els pacients la puguin visualitzar i consultar." (...).
>
> "Entre la informació i els serveis als quals els ciutadans poden accedir a través de la carpeta cal destacar:
>
> - Les dades de salut més rellevants publicades pels centres proveïdors d'atenció sanitària i contingudes a la historia clínica compartida a Catalunya.
> - El pla de medicació vigent de la recepta electrònica.
> - Les vacunes administrades.
> - Els diagnòstics.
> - Els informes clínics (urgències, ingressos, atenció ambulatòria).
> - Els resultats de les proves i les exploracions complementàries generades en l'atenció mèdica.
> - La realització de gestions, de forma personalitzada, a través de l'Oficina Virtual de Tràmits (OVT) de la Generalitat de Catalunya. (...)"
>
> "Per garantir la seguretat i la confidencialitat en l'accessibilitat a les dades, només hi tindran accés les persones majors d'edat que disposin de la targeta sanitària individual (TSI) i d'algun mecanisme de certificació oficial digital de la seva identitat.

Actualment, els dos certificats habilitats per accedir a la carpeta personal de salut són:

- Certificat idCAT
- DNI electrònic."

III

L'ordenament jurídic atribueix una protecció especial a les dades referides a la salut. En concret, l'article 7.3 LOPD, que regula les dades especialment protegides, assenyala que les dades de caràcter personal que facin referència a l'origen racial, a la salut i a la vida sexual només podran ser recollides, tractades i cedides quan, per raons d'interès general, així ho disposi una llei o l'afectat hi consenti expressament.

En aquest punt, convé assenyalar que la normativa de protecció de dades atorga una protecció reforçada a aquest tipus d'informacions més sensible, considerades dades especialment protegides (article 7 LOPD), ateses les conseqüències negatives que del seu tractament se'n poden derivar per la persona que n'és titular. Així, si amb caràcter general, qualsevol tractament de dades (com, per exemple, la veu) exigeix comptar amb el consentiment inequívoc de l'afectat, llevat que una llei disposi una altra cosa (article 6.1 LOPD), en el cas de les dades especialment protegides el consentiment atorgat per les persones afectades ha de ser exprés, quan es prevegi tractar dades que es refereixen a l'origen racial, a la salut i a la vida sexual, tret que una llei, per motius d'interès general, ho permeti (article 7.3 LOPD), i/o exprés i per escrit, quan es prevegi tractar dades que revelen la ideologia, la religió, les creences o l'afiliació sindical (article 7.2 LOPD).

En tractar-se de dades sensibles, s'ha de garantir, des de la vessant del dret a la protecció de dades personals, que terceres persones alienes a aquest entorn no puguin accedir fàcilment a aquesta informació. En aquest sentit, 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).

L'article 81.3 del RLOPD estableix que:

"A més de les mesures de nivell bàsic i mitjà, les mesures de nivell alt s'han d'aplicar en els següents fitxers o tractaments de dades de caràcter personal: a) Els que es refereixin a dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual."

En el cas examinat, i d'acord amb la tipologia de dades personals que seran tractades, entre les quals, dades de salut, les mesures de seguretat a implementar corresponen a les de nivell alt. 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. Cal tenir en compte, que aquestes mesures tenen un caràcter acumulatiu, de tal manera que les establertes per a cada nivell exigeixen incorporar les previstes per als nivells inferiors.

Així doncs, i tenint en compte que el tractament d'aquestes dades s'efectua de manera automatitzada, correspon aplicar les mesures descrites dels articles 89 al 104 del RLOPD i, especialment, pel que ara ens interessa, les relatives a l'establiment d'un control d'accés (article 91) i a l'adopció de mecanismes que permetin la correcta

identificació i autenticació dels usuaris (article 93 RLOPD) (entenent com a "autenticació" el procediment de comprovació de la identitat de l'usuari (art. 5.2.b) i com a "usuaris" els subjectes i processos autoritzats per accedir a dades o recursos (art. 5.2.p)), complementat amb l'article 98 per a les mesures de nivell mitjà i per l'article 103 i 104 per a les mesures de nivell alt:

Article 89. Funcions i obligacions del personal
1. Les funcions i obligacions de cadascun dels usuaris o perfils d'usuaris amb accés a les dades de caràcter personal i als sistemes d'informació han d'estar clarament definides i documentades en el document de seguretat.
També s'han de definir les funcions de control o autoritzacions delegades pel responsable del fitxer o tractament.

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.

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.

Secció segona. Mesures de seguretat de nivell mitjà

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.

Secció tercera. Mesures de seguretat de nivell alt
Article 103. Registre d'accessos
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.

Article 104. Telecomunicacions
Quan conforme a l'article 81.3 s'hagin d'implantar les mesures de seguretat de nivell alt, la transmissió de dades de caràcter personal a través de xarxes públiques o xarxes sense fil de comunicacions electròniques s'ha de fer xifrant les dades esmentades o bé utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers.

La implementació d'aquestes mesures de seguretat és obligatòria per al responsable del fitxer o tractament i, si escau, per a l'encarregat del tractament (article 9 LOPD), amb independència del fet que la persona afectada hagi donat el consentiment per al tractament de les seves dades o de quina sigui la naturalesa del responsable del fitxer o tractament.

IV

En relació amb les mesures de seguretat que es requereix per accedir a la informació mèdica d'un mateix, cal en primer lloc assenyalar que, des de la vessant del dret a la protecció de dades personals, les mesures de seguretat que la normativa requereix tenen per objectiu entre d'altres, que l'accés que un mateix vol realitzar sobre les seves dades sigui un accés segur, i per tant, es vol garantir que terceres persones no puguin accedir a aquesta informació, especialment en aquest cas, en que es tracta de dades sensibles, i per tant, amb la finalitat de donar compliment al que estableix la norma i en atenció a les dades que es tractaran, es requerirà l'aplicació d'unes mesures de nivell alt. Es tracta doncs, de garantir amb les mesures adoptades, no només la confidencialitat, sinó també la integritat i la disponibilitat de la informació per tal de garantir el dret fonamental a la protecció de dades personals.

S'ha de fer referència a la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (LAECSP), que reconeix el dret dels ciutadans a relacionar-se amb les administracions públiques per mitjans electrònics (art. 1) i que té com una de les seves finalitats facilitar l'accés per mitjans electrònics dels ciutadans a la informació i al procediment administratiu (art. 3.2).

Des d'aquest punt de vista, l'accés plantejat s'emmarca plenament dins d'aquests objectius atès que, en definitiva, del que es tracta és de possibilitar l'accés a les dades pròpies de salut per mitjans electrònics directament als titulars de les mateixes.

Ara bé, la consecució dels objectius previstos a la LAECSP es supedita per la pròpia llei al compliment d'un seguit de principis, entre els quals ens interessa destacar, als efectes d'aquesta consulta, el respecte al dret a la protecció de dades de caràcter personal (art. 4.a) i el principi de seguretat (art. 4.f), en virtut del qual la implantació i la utilització de mitjans electrònics per les administracions públiques s'haurà de dur a terme al menys amb el mateix nivell de garanties i seguretat que es requereix per a la utilització de mitjans no electrònics en l'activitat administrativa.

D'acord amb aquests principis, la pròpia LAECSP, als articles 14 a 16, regula els requisits d'identificació i autenticació dels ciutadans en les seves relacions amb l'administració per mitjans electrònics, permetent tant la utilització del Document Nacional d'Identitat electrònic (art. 14), com la utilització dels sistemes de signatura electrònica avançada que cada administració pública hagi admès i inclòs en una relació pública i accessible per mitjans electrònics (art. 15) o també, quan es justifiqui tenint en compte les dades i els interessos afectats, altres sistemes d'identificació com ara els basats en claus d'accés o alguna informació coneguda per ambdues parts i que ofereixi suficients garanties de confidencialitat (art. 16).

D'altra banda, la normativa de protecció de dades, com hem vist, no estableix tampoc un sistema concret d'identificació i autenticació (art. 93) sinó que poden ser admissibles diferents sistemes, sempre que es compleixin determinats requisits.

Així doncs, ni de la LAECSP ni del RLOPD no es desprèn que l'ús del certificat digital o del DNI electrònic per accedir a informació sensible, com ara les dades de salut, siguin les úniques tecnologies que garanteixin que es compleix amb les mesures de seguretat de nivell alt. Per tant, sempre que es compleixi amb les obligacions que el RLOPD imposa per l'accés a les dades i s'apliquin les degudes mesures de seguretat, ja s'estaria donant compliment a la normativa en matèria de protecció de dades exposada.

En la consulta no es concreta quins són els mecanismes d'accés alternatius que es proposarien per accedir a la informació de la carpeta personal de salut. Ara bé, atès que, tal com ja hem exposat, d'acord amb el que estableix l'article 16 de la LAECSP, la identificació i autenticació dels usuaris que vulguin accedir a la carpeta personal no ha de fer-se necessàriament a través d'un sistema de signatura electrònica basat en un certificat electrònic, o de DNI electrònic es podria plantejar la identificació i autenticació, a través per exemple, d'un usuari i contrasenya.

Si bé, en la línia del que estableix el mateix article 16 LAECSP, la naturalesa de les dades tractades, dades de salut, aconsella implantar mesures d'identificació i autenticació robustes, i en aquest sentit la utilització de certificats electrònics apareixeria com una molt bona opció, no es pot descartar la utilització de mecanismes basats en l'atribució d'un usuari i contrasenya. En aquest cas caldrà vetllar per:

- Establir un procediment de gestió de les contrasenyes que garanteixi la confidencialitat i la integritat de les mateixes.

- Utilitzar un usuari i una contrasenya, i no només un usuari. La utilització simplement d'un usuari com a mecanisme d'identificació i autenticació no és suficient.

- La contrasenya ha de ser robusta, especialment en aquest cas, en que es tracta de protegir dades de caràcter sensible. Per tant s'ha d'evitar atribuir o que l'usuari pugui emprar contrasenyes fàcilment deduïbles i que han de revestir una certa complexitat (p. ex. un determinat nombre mínim de caràcters, o evitar determinades paraules, dates o números).

- El responsable ha d'establir perfils d'usuaris per tal que cada usuari pugui accedir només a aquella informació per a la qual estigui autoritzat.

- Les contrasenyes s'han de canviar de forma periòdica, i en qualsevol cas sempre abans d'un any.

- Establir altres mesures addicionals de protecció com ara que l'aplicació que reculli les credencials d'autenticació (usuari i contrasenya) incorpori mecanismes de protecció específics com ara el xifrat de la sessió (o sigui protocol https), que el sistema bloquegi l'accés (si més no temporalment) després d'un número de intents erronis, que la introducció de la contrasenya no es pugui fer per teclat (per evitar els keyloggers) o, fins i tot, que es valori la possibilitat d'utilitzar dues contrasenyes seguides (per tant per autenticar caldria usuari+password1+password2), ja que així el sistema és més robust de cara atacs de força bruta.

La utilització d'un mecanisme d'aquest tipus, comportaria probablement un augment dels usuaris de la carpeta personal de salut, davant les dificultats per a fer-ne ús que poden tenir determinats col·lectius d'usuaris si el sistema d'accés es basa en un certificat electrònic. Ara bé, resulta evident que, especialment per a aquest col·lectiu de persones –molt nombrós i amb competències tècniques molt diverses-, la utilització d'un sistema basat en un usuari i contrasenya pot suposar un risc addicional.

Per això, atès aquest perfil divers, seria bo proporcionar als usuaris de la carpeta algunes recomanacions en relació a l'accés i l'ús de les dades a les que tinguin accés, informació que quedaria contextualitzada en el que preveu l'art. 89, és a dir, recomanar en el cas d'utilitzar usuaris i contrasenyes, que es configuri el navegador de manera que no emmagatzemi les contrasenyes, que s'esborri l'historial de navegació i la memòria "caché" del navegador en finalitzar, que no es comparteixi la contrasenya, etc.

En qualsevol cas, i sens perjudici que aquelles persones que ho desitgin puguin demanar l'accés a través d'un sistema basat en un usuari i contrasenya, hauria de ser possible que els usuaris que desitgin accedir a través d'un certificat electrònic, sigui el DNI electrònic o d'un altre tipus, ho puguin fer.

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

Conclusions

L'ús del certificat digital o del DNI electrònic per accedir a informació sensible, com ara les dades de salut, no s'estableixen ni en la LAECSP ni del RLOPD com les úniques tecnologies que garanteixin el compliment de les mesures de seguretat de nivell alt per a la identificació i l'autenticació d'usuaris.

Tot i que des del punt de vista de la normativa de protecció de dades sempre serà preferible el sistema que ofereixi majors garanties de seguretat, com ara la utilització de mecanismes basats en certificats electrònics, es poden utilitzar altres sistemes d'accés a les dades contingudes a la carpeta personal de salut per mitjà de sistemes robusts d'identificació i autenticació, com ara usuari i contrasenya, sempre que la política de seguretat implantada en garanteixi la confidencialitat.

Barcelona, 14 de juny de 2012