Resultat del control de qualitat del codi tipus; revisió sobre la implantació de les mesures de seguretat

El passat **24 de maig de 2019** es va realitzar la sessió de control de qualitat del Codi Tipus de la Unió Catalana d'Hospitals per part del consultor de Faura-Casas assignat, conjuntament amb el Sr. Javier Remacha, Delegat de Protecció de Dades de Fundació Institut Guttmann, referit en endavant també com a DPD.

L'objectiu era avaluar el grau d'adequació i compliment de les mesures de seguretat de l'entitat, segons els requisits legals sobre protecció de dades de caràcter personal establerts al Reglament 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (en endavant, RGPD) i la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, però tenint en compte també les mesures de seguretat previstes a la Llei 15/1999, de 13 de desembre, i al Reglament 1720/2007, de 21 de desembre, i considerant, com també les previsions del Codi Tipus de la Unió Catalana d'Hospitals.

El resultat del control de qualitat per la revisió del nivell d'implantació de les mesures de seguretat es detalla en els següents apartats:

DELEGAT DE PROTECCIÓ DE DADES

L'entitat ha nomenat com a Delegat de Protecció de Dades el Sr. Javier Remacha. S'ha realitzat la notificació corresponent a l'Autoritat Calalana de Protecció de Dades en data 11/05/2018 i s'ha rebut la validació corresponent. D'altra banda, s'han incorporat les funcions de DPD en el document de descripció del lloc de treball, que també preveu funcions transversals organitzatives de suport a Direcció i Gerència, de qui depèn directament. Les funcions que contempla el document i la dependència del càrrec són compatibles amb les pròpies d'un DPD i garanteixen una actuació independent. El DPD no realitza funcions que puguin representar un conflicte d'interessos i no rep instruccions en l'exercici de les tasques pròpies del càrrec.

L'entitat manifesta que es faciliten els recursos necessaris al DPD per realitzar les seves funcions i tenir accés a les dades personals.

L'existència del DPD ja consta a la web de l'entitat, però no consta encara a l'organigrama, ni s'ha fet tampoc una difusió interna generalitzada entre el personal sobre el seu nomenament i les seves funcions. Per tant, es fan les següents recomanacions:

- Presentar com a notícia al portal web el nomenament i existència del DPD.
- Si és possible, enviar també una comunicació per correu electrònic a tot el personal sobre el nomenament i existència del DPD i les seves funcions bàsiques.

- Incloure la figura del DPD en el Protocol de Bones Pràctiques que es lliura a tots els treballadors i col·laboradors de l'entitat.
- Incloure la figura del DPD de forma específica a l'organigrama de l'entitat.

REGISTRE D'ACTIVITATS DE TRACTAMENT

L'entitat manifesta que ha realitzat el RAT, partint de fitxers anteriorment definits, de què proporciona evidència documental.

Es revisa el RAT proporcionat per l'entitat, que és fonamentalment correcte i ajustat a la normativa, si bé presenta algunes deficiències o àrees de millora, de què parteixen les següents recomanacions:

- Caldria incloure-hi un camp de destinataris. Cal fer-hi esment dels tercers externs a qui es comunicaran dades de caràcter personal, bé sigui per cessió de dades o per transferència internacional. En aquest punt no s'han d'incloure els encarregats del tractament, que tractaran les dades per compte de l'entitat.
- Millorar la definició dels terminis de supressió, de manera que es determinin específicament els períodes concrets de conservació o es digui quin és el criteri adoptat per l'entitat per definir els terminis de supressió (per exemple, en el cas de dades de pacients, es pot fer una al·lusió als períodes de conservació obligada previstos en la legislació sanitària vigent).

LEGITIMACIÓ DE LES DADES

Des de Faura-Casas s'explica que amb el RGPD s'exigeix una base jurídica específica que legitimi el tractament de les dades personals. Aquesta legitimitat pot obtenir-se pel consentiment de l'interessat o per l'execució d'un contracte (per exemple, en el cas dels treballadors, la legitimitat del tractament ve pel contracte de treball), o pot basar-se en el compliment d'una obligació legal, entre d'altres. De conformitat amb l'art. 13 RGPD, en el moment d'obtenir les dades de caràcter personal, cal proporcionar a l'interessat una informació legal sobre el tractament.

Analitzem la legitimitat del tractament de les dades dels pacients, que és el que planteja major complexitat i factors de risc.

La base jurídica que legitima el tractament de dades de pacients rau en el servei mateix prestat per l'entitat, que és l'assistència sanitària i social, d'acord amb l'art. 9.2.h) RGPD.

Es revisa el full d'informació que es proporciona als pacients en el moment que es recullen les seves dades, que és fonamentalment correcte des del punt de vista de la informació sobre el tractament. No obstant, hi ha dos aspectes millorables, com són la referència al "*caràcter indefinit*" de les dades, que no és adient, i a la possibilitat de revocar el consentiment, que implica que les dades "*s'esborraran*". Sobre el primer aspecte, caldria definir els terminis de supressió de les dades

o fer una referència al criteri de supressió, que pot ser als terminis de conservació obligada de la legislació vigent en matèria sanitària. En el segon dels aspectes de millora, cal tenir present que la base jurídica del tractament és l'art. 9.2h) RGPD i el propi servei que es presta i no pas el consentiment de l'interessat. Per tant, no és correcte dir que l'interessat té la possibilitat de retirar el consentiment respecte al tractament de les seves dades de salut i encara menys que això implicarà l'eliminació de les dades, sobretot quan hi ha terminis de conservació obligada que cal respectar, com hem comentat més amunt. Per tant, recomanem eliminar la línia que diu "*si es revoqués el consentiment, les dades s'esborraran del tractament*".

D'altra banda, juntament amb la informació sobre el tractament, es proporciona als pacients un document titulat "*Autorització i consentiment de cessió de dades de caràcter personal*", que inclou un text sobre altres 3 tractaments que el pacient autoritza amb la seva signatura, i per sota, tres tractaments més que l'usuari té la possibilitat de consentir expressament a través de marcar una creueta. Les autoritzacions que es preveuen són correctes, ja que responen a tractaments que requereixen el consentiment exprés. No obstant, caldria millorar aquest quadre segons les següents recomanacions:

- Respecte als tres tractaments sobre els quals el text diu que el pacient autoritza amb la seva signatura, es poden plantejar com a una informació, excepte el de recerca i investigació. Tant la comunicació de dades a l'entitat medico-sanitària amb qui tingui concertada la prestació del servei com l'emissió de justificants no requereixen el consentiment exprés i, per tant, seria millor que apareguessin al text com a una informació i no pas com a una prestació de consentiment. En canvi, l'ús de les dades per a investigació sí que hauria de consentir-se expressament mitjançant un quadre de checkbox com els altres tres tractaments de sota.

- Els quadres de checkbox haurien d'incloure la possibilitat que el pacient marqui *sí* o *no* amb dos quadres diferents, per tal de garantir que el consentiment es presta de forma inequívoca, tal com requereix el RGPD.

- En tractar-se de prestacions de consentiment que legitimen els citats tractaments, caldria incloure-hi una frase recordant el dret que té el pacient a revocar els consentiments prestats en qualsevol moment.

L'entitat du a terme diverses activitats de tractament que comprenen dades de pacients, personal, administració, reclamacions, externs de relacions públiques, externs amics, usuaris i possibles usuaris de Guttmann Barcelona Life, participants de Sports&Life Guttmann Club, externs de docència, voluntaris, persones de treballs en benefici de la comunitat, videovigilància, investigació, usuaris de la plataforma GNPT, participants al projecte BBHI i blanqueig de capitals. Totes aquestes activitats es troben reflectides al RAT de l'entitat.

Durant la darrera auditoria sobre protecció de dades que es va realitzar de forma exhaustiva a l'entitat el passat mes de maig de 2018, es va poder comprovar com tots els procediments de recollida de dades ja implicaven majoritàriament proporcionar una informació sobre el tractament de les dades que era ajustada a la normativa llavors vigent. A partir de l'entrada en aplicació del

RGPD el mateix mes de maig de 2018, l'entitat manifesta que ja ha estat treballant en l'adaptació de tota aquesta documentació i informació per tal que sigui conforme als requeriments de l'article 13 RGPD.

Pàgina web

Es comprova com a mostra de compliment de l'article 13 RGPD que l'avís legal de la web i política de privacitat ja inclou una informació actualitzada i completa sobre els tractaments de les dades recollides a través de la web. Aquest avís legal, que és conforme a l'article 13 RGPD, ha de ser acceptat per tots els usuaris de la web que vulguin realitzar una sol·licitud d'inscripció a la borsa de treball i enviar el seu currículum, per exemple.

Pel que fa als nous serveis que l'entitat té previst inaugurar a partir del proper mes de gener sota el nom de Guttmann Barcelona, ja està previst que la nova web vinculada dugui un avís legal actualitzat.

Consentiment

Sempre que s'utilitzen les dades per a finalitats diferents de les que van justificar la recollida incial, l'entitat ja empra procediments d'obtenció del consentiment exprés de l'interessat, que pot revocar en qualsevol moment. En particular, es recullen consentiments per a l'enviament de la revista, per a investigació mèdica i per a l'ús de la imatge, entre d'altres. L'entitat recull alguns d'aquests consentiments en el full d'informació del pacient; en aquest cas, el document original s'escaneja i s'envia original a l'arxiu, de manera que sempre es guarda una evidència de la prestació del consentiment.

D'altra banda, tal com s'ha informat més amunt en relació al full d'informació del pacient, la forma de recollir aquests consentiments no seria correcte, ja que haurien de permetre a l'interessat marcar una opció negativa -garantint així que el consentiment prestat és inequívoc- i haurien d'incloure una informació sobre la possibilitat de revocar el consentiment en qualsevol moment.

DRETS DELS INTERESSATS

L'entitat manifesta que ja té implementat el procediment d'atenció dels drets dels interessats de conformitat amb el RGPD i disposa dels formularis d'exercici d'aquests drets. També coneix i informa sobre la possibilitat que els interessats presentin una reclamació a l'autoritat de control, i coneix l'obligació de donar resposta a qualsevol exercici de drets dins els terminis previstos legalment.

ENCARREGATS DEL TRACTAMENT I TERCERS SENSE ACCÉS A DADES PERSONALS

De conformitat amb l'article 28.3 del RGPD, recordem la necessitat de tenir contractes de d'encàrrec de tractament de dades amb totes aquelles entitats o persones que tinguin accés o realitzin un tractament de dades de l'entitat per compte de la mateixa entitat i sota les seves

instruccions. Caldrà que aquests contractes estableixin l'objecte, la durada, la naturalesa, la finalitat del tractament, el tipus de dades personals a què té accés l'encarregat, les categories d'interessats, a més de les obligacions i drets de les parts.

D'acord amb les explicacions i evidències proporcionades per l'entitat, ja hi ha un control sobre els contractes d'encàrrec de tractament que manté signats, de manera que, a mesura que s'han d'anar renovant els contractes de prestació de serveis relacionats, ja es van signant nous contractes d'encàrrec de tractament actualitzats i adaptats al RGPD. Així passa per exemple amb les empreses Sodexo (menjador), Saba (pàrking), Aspy (prevenció de riscos), Pearson (recerca), Ucae (prevenció externa), etc. Actualment, aproximadament un 25% dels contractes d'encàrrec de tractament de l'entitat ja estarien actualitzats.

Recordem que el Reial Decret Llei 5/2018, de 27 de juliol, de mesures urgents per a l'adaptació del dret espanyol a la normativa de la Unió Europea en matèria de protecció de dades manté la licitud dels contractes d'encàrrec de tractament que tinguin caràcter indefinit i estiguin signats de conformitat amb l'antiga LOPD fins al 25 de maig de 2022. En tot cas, recordem també que qualsevol de les dues parts pot requerir la signatura d'un contracte d'encàrrec de tractament actualitzat i adaptat a l'article 28 RGPD.

Per tot plegat, atès que l'entitat ja disposa del model de contracte d'encàrrec de tractament de dades facilitat des del Codi Tipus i ja n'està controlant la seva signatura respecte de tots els seus encarregats de tractament de dades, ja estaria complint l'obligació de l'article 28 RGPD. L'entitat, d'altra banda, també fa signar un model de compromís de confidencialitat amb tercers que no fan cap tractament de les dades personals, però pel servei que presten podrien tenir-hi un accés accidental.

REGISTRE D'INCIDÈNCIES I NOTIFICACIÓ DE FUITES DE SEGURETAT

L'entitat ja disposa i manté un registre d'incidències i, segons les informacions proporcionades, coneix el procediment de comunicació de violacions de seguretat. No obstant, no consta encara registrada una fuita o violació de seguretat que hagi hagut de notificar-se a l'autoritat de control i/o als interessats.

Es planteja si és possible que hi hagi empleats que participin d'activitats de tractament de dades i no coneguin la seva obligació de col·laborar amb el delegat de protecció de dades en la comunicació de violacions de seguretat. En aquest sentit, revisem el manual de bones pràctiques, que conté les instruccions que l'entitat transmet als treballadors en relació al tractament de les dades, i constatem que realment no conté una indicació clara sobre la necessitat de comunicar al delegat de protecció de dades qualsevol incidència o fuita relativa al tractament de les dades.

Caldria que, entre les instruccions que es proporcionen als treballadors dins el manual de bones pràctiques, s'inclogués l'obligació d'informar de forma immediata al delegat de protecció de dades sobre qualsevol incidència en la seguretat de les dades de caràcter personal, per tal que, si

es valora que pot posar en perill drets i llibertats, pugui comunicar-se com a violació de seguretat a l'autoritat de control en un màxim de 72 hores des del moment que se'n té coneixement i, si és el cas, també a les persones afectades.

FORMACIÓ EN PROTECCIÓ DE DADES

Els empleats de l'entitat ja realitzen cursos de formació sobre protecció de dades, tant en el moment d'incorporar-se a l'empresa per primer cop, com posteriorment a través d'un mòdul de formació que tots els treballadors han de cursar anualment i que inclou la realització d'un examen.

Que el personal de l'entitat estigui familiaritzat amb la protecció de dades és fonamental perquè es pugui donar compliment a les obligacions legals. Des de Faura-Casas s'informa de la possibilitat de realitzar cursos de protecció de dades de la categoria de salut a la Unió Consorci Formació (UCF); aquests cursos poden ser online i subvencionats en la part que correspongui por la Fundació Tripartita.

INSPECCIONS AEPD

L'entitat informa que fins a la data no han tingut cap inspecció per part de l'Agència Espanyola de Protecció de Dades.

CANVIS EN L'ENTITAT

L'entitat manifesta l'existència de dos canvis importants que està a punt d'emprendre. El primer d'ells és la inauguració pròxima dels serveis vinculats a la marca Guttmann BCN, que implica noves instal·lacions i activitats de tractament.

El segon canvi important és la implementació d'una aplicació de missatgeria instantània per a la comunicació entre professionals i amb pacients.

Des de Faura-Casas es recomana realitzar la gestió del risc necessària i valorar la necessitat de realitzar les corresponents avaluacions d'impacte en la realització de nous tractaments i la implementació de noves tecnologies que puguin tenir efectes rellevants en el tractaments de les dades i els riscos per als drets i les llibertats que se'n poden derivar.

AUDITORIES

L'entitat va realitzar la seva darrera auditoria durant el passat maig de 2018 per part de Faura-Casas.

Tot seguit, s'analitza la situació actual de les àrees de millora detectades a l'informe d'auditoria de l'any 2018 que són d'aplicació amb el RGPD, assenyalant els punts rellevants respecte a la seva situació:

Document de seguretat

Amb l'entrada en aplicació del RGPD, cal que es modifiquin i actualitzin tots els documents de seguretat de conformitat amb la nova legalitat sobre protecció de dades. En especial, cal tenir en compte els canvis terminològics i conceptuals, atenent especialment la caducitat del concepte de fitxer i responsable dels fitxers pel de tractament i responsable dels tractaments. De la mateixa manera, caldrà tenir en compte els principis del RGPD i les figures de l'anàlisi de riscos i l'avaluació d'impacte.

Identificació i autentificació d'usuaris

L'entitat ha millorat i perfeccionat els requeriments que s'apliquen a la configuració de contrasenyes que formen part del control d'accés als diferents entorns de tractament de dades de l'entitat.

Registre d'accessos

L'entitat aporta informació i evidències de les revisions efectuades sobre els registres d'accessos. En particular, tant pel que fa al registre d'accessos a la història clínica com pel que fa al de l'entorn GMPT, es realitzen revisions mensuals per part del delegat de protecció de dades.

Còpies de seguretat

L'entitat planteja l'existència de procediments de còpies de seguretat en els mateixos termes que es descriuen en el darrer informe d'auditoria, que ja eren adequats a la normativa i oferien garanties de seguretat.

Conclusions

Per tot plegat, a tall de resum i conclusió, un cop revisada la situació actual de l'entitat en relació a les obligacions en matèria de protecció de dades, constatem que l'entitat **Institut Guttmann** pot treballar en:

- Difondre entre els treballadors el nomenament i funcions del delegat de protecció de dades.
- Millorar el registre d'activitats de tractament, incloent-hi tercers destinataris de les dades i criteris o terminis de conservació.
- Atendre les indicacions sobre les formalitats documentals destinades a la informació sobre el tractament de les dades i l'obtenció dels consentiments necessaris.
- Millorar la informació als treballadors sobre el procediment de comunicació de violacions.
- Valorar, analitzar i gestionar els riscos implícits en la realització de nous tractaments de dades i la implementació de noves tecnologies.

Aquestes recomanacions es realitzen amb la finalitat que es compleixin satisfactòriament els aspectes més significatius que deriven de l'adhesió al Codi Tipus de la Unió Catalana d'Hospitals i de la normativa vigent en matèria de Protecció de Dades, especialment el RGPD.

Barcelona, 12 de juny de 2019

Pere Ruiz Espinós

Fundació Unió Carrer de València, 333 · 08009 Barcelona · Tel 93 209 36 99 · Fax 93 200 86 38
Faura-Casas Carrer Còrsega, 299 6ª · 08008 Barcelona · Tel 902 28 28 30 · Fax 93 302 65 96