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

El passat 2 de juny de 2023 es va realitzar la sessió de control de qualitat del Codi Tipus de la Unió Catalana d'Hospitals per part de la consultora de Faura-Casas assignada, conjuntament amb el Sr. Javier Remacha, delegat de protecció de dades de la Fundació Institut Guttmann.

L'objectiu era fer seguiment de les àrees de millora i no conformitats de la darrera auditoria de protecció de dades, segons els requisits legals respecte la protecció de dades de caràcter personal, establerts en el Reglament 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 referent a la protecció de les persones físiques pel que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades (en endavant el RGPD) i, la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia de drets digitals, així com en el propi Codi Tipus de la Unió Catalana d'Hospitals. Així mateix, es revisen canvis que s'hagin pogut produir en l'entitat que tinguin impacte en aquesta matèria.

El resultat del control de qualitat es detalla en els següents apartats:

AUDITORIA

L'Entitat realitzà la darrera auditoria de protecció de dades el juny de 2022. L'informe de l'auditoria s'elevà a la Direcció General i al Comitè de Direcció en una reunió de setembre de 2022, d'on en derivà un pla d'acció per tal de procedir a les àrees de millora i no conformitats detectades. No obstant, això no va quedar reflectit en cap acta.

ACTIVITATS DE TRACTAMENT

S'aporta el registre d'activitats de tractament (RAT), el qual s'ha treballat d'ençà de l'última auditoria, constant com a última revisió la d'abril de 2023.

En quant a l'àrea de millora que s'havia detectat referent a haver de revisar del RAT els apartats de les transferències internacionals de dades i termini de conservació de les dades, es verifica que s'han complimentat aquests apartats en tots els tractaments del RAT. No obstant, sembla que en alguns estigui en procés de validació, doncs queda identificat en un altre color, és el cas per exemple del tractament Externs RRPP, o en el projecte BBHI.

Es mantenen els 24 tractaments que figuraven en l'última auditoria i a més, s'ha inclòs un nou tractament en el RAT, que és el denominat *Registre assistència pacients*.

En tots els tractaments hi consten els camps requerits per la normativa i també n'hi ha d'addicionals, com base legal del tractament, origen de les dades, procediment d'informació, àrees que accedeixen a les dades, sistemes de tractament, encarregats de tractament (amb indicació de justificació de l'acord), documentació relacionada i accessos remots. Es valora positivament que el RAT contempli tots els extrems indicats, doncs completa i fa més entenedor

cada tractament de dades, el cicle de vida de les dades, així com aspectes clau com la legitimació, o relació dels accessos.

El RAT també incorpora en cada tractament l'anàlisi de riscos, amb indicació de si cal o no realitzar avaluació d'impacte.

ANÀLISI DE RISCOS I AVALUACIONS D'IMPACTE

Tal i com es mencionava, en el RAT hi ha constància de l'anàlisi de riscos i l'avaluació de la necessitat de fer una avaluació d'impacte a cadascun dels tractaments.

Els punts que s'analitzen, entre d'altres, són: la durada i extensió geogràfica del tractament, si es realitza un tractament a gran escala, si es tracten dades de categoria especial, si la recollida de dades té com a finalitat el monitoratge o avaluació sistemàtica i exhaustiva d'aspectes personals, els col·lectius de qui s'obtenen les dades (en especial, si aquests són vulnerables), si les dades seran captades de zones d'accés públic, si intervenen altres proveïdors en el tractament, etc. L'anterior es reforça amb una revisió d'acompliment dels principis de la privacitat des del disseny i per defecte. De tot plegat, en resulta com la conclusió de si es considera que el tractament dona o no factors que impliquin un alt risc pels drets i llibertats dels interessats, i per tant, requereix o no de l'elaboració d'una avaluació d'impacte de protecció de dades (AIPD).

Si bé la metodologia de l'anàlisi de riscos és bona per a valorar si convé o no fer l'avaluació d'impacte, es detecta que en algunes conclusions el resultat no és correcte. Per exemple, en el cas del tractament de Blanqueig, en què es conclou que no és necessària l'AIPD quan sí que és requerida per mandat legal (el Reial decret-llei 7/2021, de 27 d'abril, en el seu article tercer número 15 introdueix l'article 32 bis a la Llei 10/2010 de prevenció de blanqueig de capitals i finançament del terrorisme, i en aquest article s'explicita la necessitat legal de fer una AIPD); o en el tractament d'empremtes digitals, que es conclou que no requereix AIPD en contra del criteri de les autoritats de control que sostenen que per la posada en marxa d'un sistema de control d'aquest tipus, és necessari fer una avaluació de l'impacte relativa a la protecció de dades (veure dictàmens APDCAT com CNS 63/2018 i següents). Aquest darrer punt és especialment rellevant, considerant que durant la sessió de checklist s'ha manifestat que l'Entitat està en procés de valorar la biometria per a accedir al gimnàs, tractament aquest que suposaria igualment una nova AIPD seguint amb els mateixos arguments esmentats.

Durant els treballs de camp s'ha explicat que s'està en curs de dissenyar una nova història clínica en entorn web i una APP pròpia que estaran interconnectades. Aquestes novetats suposen un canvi en el tractament de la informació dels pacients, ús de nova tecnologia, etc. factors tots ells que impliquen realitzar la corresponent AIPD per tal d'identificar els riscos i determinar-ne les corresponents mesures.

En quant a les AIPDs, es reiteren els punts que ja figuraven en l'últim informe d'auditoria respecte a la necessitat de distingir entre el risc inherent i el risc residual, i també, el fet d'incloure als informes d'avaluació d'impacte les mesures proposades per a la minimització del risc i, posteriorment, disposar d'evidències de seguiment de l'aplicació dels informes.

S'ha de senyalar que en l'article 73.t) de la LOPDGDD es disposa que constitueix una infracció greu *El tractament de dades personals sense haver dut a terme l'avaluació de l'impacte de les operacions de tractament en la protecció de dades personals en els supòsits en què aquella sigui exigible*.

Sobre aquesta qüestió, també recordar que de conformitat amb la normativa i amb les interpretacions de les Autoritats de Control, el delegat de protecció de dades no està habilitat ha realitzar les avaluacions d'impacte en matèria de protecció de dades. Les funcions del DPD són supervisar i assessorar, però en cap cas realitzar l'AIPD.

LEGITIMACIÓ DE DADES

Dels aspectes de millora que es detectaren sobre aquest punt en l'auditoria, es relaciona a continuació quin és l'estat actual:

- S'ha completat la informació deguda en el formulari de donatius del web.
- No s'ha rectificat la normativa derogada que consta en la informació del formulari "hazte amigo" del web.
- Manca incorporar la política de privacitat del formulari de contacte del web.
- S'ha completat la informació deguda del formulari de voluntaris.
- S'ha modificat la política de privacitat del web.
- Manca incorporar l'enllaç de privadesa a les activitats de "Life&Sports".
- No consta compromís de no reidentificació del personal investigador.

FUNCIONS I OBLIGACIONS

L'Entitat continua formant a tot el personal en protecció de dades cada any.

Així mateix, es confirma que el delegat de protecció de dades segueix fent cursos i assisteix a sessions per ampliar els seus coneixements en la matèria.

En aquests moments, s'està actualitzant el contingut del Manual de Bones Pràctiques. En aquest, s'hi corregiran les indicacions a la normativa derogada i també, s'hi inclourà el deure de notificar incidències. El document es troba en fase d'esborrany amb previsió que estigui validat aquest exercici.

MESURES DE SEGURETAT

- ASPECTES DE SEGURETAT INFORMÀTICA

S'ha revisat la política de seguretat de l'Entitat i s'ha elaborat el Pla de Protecció de Dades 23-25. Aquest Pla és el document que desenvolupa el sistema de gestió de la protecció de dades per a la millora continuada del nivell de seguretat de les dades, integrant-se en el sistema general de gestió de l'organització, mitjançant l'aplicació de processos, procediments i pràctiques preventives. Segons es manifesta, es preveu tenir aprovat al llarg d'aquest exercici.

En relació amb la sala de servidors del departament d'informàtica que es va detectar que no quedava tancada, en aquests moments ja ho està.

- **ASPECTES DE SEGURETAT FÍSICA**

Respecte als suports documentals, es reitera la conveniència de revisar l'oportunitat i la conveniència de dur a terme accions de destrucció segura de la documentació més antiga, sempre que es pugui acreditar que ja no n'és necessària la conservació. Sobre aquest punt, no s'aporten evidències de cap canvi.

ENCARREGATS DEL TRACTAMENT

Resta pendent de validar el protocol de criteris i verificació dels proveïdors, garantint un procés de selecció que s'ajusti als principis de protecció de dades.

Es manifesta que els nous proveïdors amb accés a dades segueixen signant el contracte d'encarregat de tractament adequat als requeriments del RGPD. El darrer que se signà fou el desembre de 2022.

Respecte als contractes amb durada indefinida anteriors a l'aplicació del RGPD, s'està en curs de revisar-los.

D'altra banda, s'informa que actualment els docents només signen el compromís de confidencialitat, ja que no accedeixen a dades personals i per tant, no tindrien consideració d'encarregats del tractament.

REGISTRE D'INCIDÈNCIES I NOTIFICACIÓ DE FUITES DE SEGURETAT

L'Entitat manifesta que se segueix amb el registre semestral de les incidències. El procés és que qualsevol persona pot notificar-les al DPD i aquest és qui les reporta en el registre específic, en el qual s'hi deixa constància dels camps: ID, títol, data obertura, sol·licitant, ubicació, tècnic, categoria, descripció, seguiment.

Es manifesta que en el darrer any es produí una bretxa de seguretat en la plataforma Liferay, la qual fou comunicada a l'autoritat de control. S'aporten evidències de la valoració efectuada, notificació a l'Agència Espanyola de Protecció de Dades i arxiu d'actuacions de l'autoritat de control.

DRETS DE LES PERSONES INTERESSADES

L'Entitat informa que s'han seguit donant resposta a les peticions rebudes en termini i forma. Tots els drets d'accés de la HC es gestionen des de l'Àrea d'Admissions.

Resta pendent acabar d'elaborar un registre de drets per tal de tenir relació de tots els produïts. Així mateix, convindria que el delegat de protecció de dades fes seguiment i/o participés dels drets que s'adrecin a l'Entitat.

Per tant, atesa la situació actual, considerem que l'Entitat **FUNDACIÓ INSTITUT GUTTMANN**, garanteix els principals requeriments de la normativa, si bé manca acabar de treballar alguns dels aspectes descrits en l'acta per acomplir satisfactòriament tots els aspectes que es 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, 28 de juny de 2023.