Fundació Josep Carreras CONTRA LA LEUCÈMIA | 30 Aniversari	**Informe Progrés RGPD**
Delegada de Protecció de dades: Iris Bargalló	Data: 15/09/2020

1 Introducció

La FIJC ha finalitzat el procés d'implementació les mesures de protecció de dades necessàries per complir amb els nous requisits de protecció de dades personals establerts per el nou Reglament general de protecció de dades (RGPD 2016/679) i la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

Al Novembre 2019 la FIJC ve rebre la auditoria externa de protecció de dades realitzada per Faura & Cases on no es van detectar no conformitats, encara que es van fer recomanacions de millora.

2 Objectiu

L'objectiu d'aquest informe és informar sobre el procés d'implementació de les recomanacions fetes per Faura & Cases durant l'auditoria i les accions que s'han dut a terme en el 2020.

3 Responsabilitats

Gerent – Sr. Antoni Garcia Prat

Delegada de Protecció de dades – Sra. Iris Bargalló Arraut

4 Auditoria: Observacions i Accions Correctores

4.1 Protecció de dades

4.1.1 Registre d'Activitats de Tractament (RAT):

Observacions:

1. Categoria d'interessats: En aquesta camp del RAT hem d'identificar els col·lectius de persones de qui tenim dades, no la font de les dades.
2. Destinataris de les dades: Caldria incorporar un camp de destinataris de les dades, d'acord amb l'art. 30.1.d) RGPD.

Acció Correctora: Revisió i adaptació del RAT segons recomanació

Responsable: DPD

4.1.2 Procediment Fuites de Seguretat.

Observacions:

Tot i que el procediment que ja preveu l'entitat és correcte, és possible millorar-lo a través d'accions que permetin que tot el personal sigui conscient de l'existència d'aquest procediment i de l'obligació de comunicar fuites de seguretat a la DPD. En especial, recomanem que aquesta obligació que té tot el personal de l'entitat s'incorpori al Codi de Conducta de Seguretat de la Informació en forma d'instrucció.

Acció Correctora: Incorporar procediment de fuites de seguretat en Codi de conducta de seguretat de la informació.

Responsable: DPD

4.1.3 Períodes de Retenció.

Observacions:

Cal establir terminis i criteris de destrucció de la documentació més antiga i innecessària, ja que es corre el risc que la informació o documentació que conté dades de caràcter personal es conservi durant més temps del que sigui necessari i això sigui, per tant, un tractament indegut. Cal que l'entitat estableixi criteris i terminis legals de conservació més clars al registre d'activitats de tractament i que procedeixi a l'eliminació de documentació antiga i innecessària.

Acció Correctora:

Revisió de períodes de destrucció i arxiu. S'han indicat en el registre de tractament de dades.

Responsable: DPD

4.1.4 Confidencialitat

Observacions:

D'acord amb l'art. 24 RGPD, forma part de la responsabilitat del responsable del tractament aplicar les mesures de seguretat més adequades per a assegurar-se que no hi ha accessos ni tractaments indeguts de les dades. En aquest sentit, si hi ha proveïdors que, sense tenir un accés autoritzat a les dades, per la naturalesa del servei que presten, poden tenir un accés involuntari o accidental a dades de caràcter personal (per exemple, serveis de neteja), és molt recomanable fer-los signar un compromís de mantenir la confidencialitat sobre la informació a què puguin tenir accés.

Acció Correctora:

Es facilita model de contracte per Implementar contracte confidencialitat amb proveïdors de serveis que tinguin accés circumstancial a dades.

Responsable: DPD

4.2 Botiga Online

Observacions:

Recomanem, en tot cas, que la informació més bàsica sobre l'art. 13 RGPD sigui visible a la mateixa pàgina del formulari de recollida de dades (no només a través de l'enllaç), i que la informació completa sigui accessible igualment a través de l'enllaç. D'altra banda, recomanem revisar la informació que es proporciona actualment, per tal que sigui més ajustada a la finalitat de la botiga online.

Acció Correctora: Revisió de la part de privacitat de la botiga online.

1. S'ha d'afegir petit text legal al formulari de la botiga online per cobrir requeriments de l'article 13.
2. Versió en Català de la Política de Privacitat no estava corregida adequadament, es faciliten de nou els textos per adequar la versió en Català al Reglament

Responsable: DPD i Botiga On-line

4.3 IT

4.3.1 Procediments de Còpia

Observacions:

Tot i que els procediments de còpia descrit són correctes, com a aspecte millorable, caldria implementar un procediment de revisió d'aquests procediments (per exemple, cada 6 mesos) i documentar-ne el resultat.

Acció Correctora: La revisió dels procediments de còpia es farà anualment, així s'ha inclòs en el pla de recuperació i es realitzarà a les instal·lacions del IJC.

Responsable: IT

4.3.2 Accessos indeguts

Observacions:

Segons les informacions proporcionades i el Document de Seguretat TIC, l'entitat ja realitzaria un registre d'accessos i un control informal de possibles accessos indeguts, però caldria formalitzar i definir aquest procediment. No hi ha actualment una evidència documental d'aquest procediment.

Així, per exemple, es podria establir un procediment de revisió mensual, fent una selecció a l'atzar de registres i dates, i documentar de forma convenient per part de la DPD la detecció o no de possibles accessos indeguts. Els registres i dates que podrien ser objecte de la revisió podrien triar-se a l'atzar, o tenir en compte criteris de risc d'accés indegut (casos en què donants o pacients siguin familiars de persones treballadores, VIPs, etc.).

Acció Correctora: Incloure en la auditoria de procés del REDMO a final d'any revisió de accessos indeguts.

Responsable: IT & Qualitat

4.3.3 Inventari

Observacions:

Caldria incloure l'inventari de suports i dispositius al Document de Seguretat TIC o en un seu annex, per tal de tenir-lo correctament documentat.

Acció Correctora: Es farà inventari de Hardware durant 2020.

Responsable: IT

4.3.4 Servidors

Observacions:

Com a únic element de millora i amb la finalitat de minimitzar el risc d'accessos indeguts, cal que la sala de servidors estigui tancada no només fora de la jornada laboral, sinó sempre que no se'n faci cap ús, i també particularment dins la jornada laboral.

Acció Correctora: Mantenir porta servidors sempre tancada

Responsable: IT

4.4 Màrqueting

Observacions:

Recomanem disposar d'un model de document de consentiment exprés per a la publicació d'imatge, que s'hauria de fer servir sempre que s'hagi d'obtenir la imatge d'algú i publicar-la en mitjans de comunicació de l'entitat. No és vàlid el consentiment prestat oralment, sinó que s'ha d'obtenir sempre el consentiment exprés i per escrit de la persona interessada.

Recomanem que en els formularis d'inscripció als esdeveniment s'hi inclogui un avís sobre el fet que s'hi faran fotos i se'n farà difusió a través dels mitjans de comunicació de FIJC, i s'ofereixi la possibilitat de manifestar de forma expressa que no s'autoritza la realització de fotos.

Acció Correctora: S'implementa formulari de consentiment per als testimonis.

Responsable: Màrqueting & DPD

4.5 Pisos d'acollida

Observacions:

Caldria fer una reflexió en aquest apartat sobre la proporcionalitat i necessitat de disposar de determinada informació sobre les persones que, en relació a la prestació del servei de pisos d'acollida, pot resultar desproporcionada i innecessària.

Acció Correctora: S'ha demanat als assistents socials que no ens enviïn dades o informació mèdica. Només que es tracta d'una malaltia oncohematològica. S'ha fet una proposta d'informe amb informació mes reduïda. En la pròxima reunió es recordarà la limitació de les dades mèdiques en l'informe.

Responsable: Pisos d'acollida, Qualitat & DPD.

4.6 REDMO

4.6.1 Workups

Observacions:

A l'àrea de donants i en la preparació de workups es té sempre coneixement del nom del pacient, malgrat que es treballi amb un codi. Caldria que efectivament hi hagués aquesta separació funcional de forma efectiva, i que hi hagués un procés de seudonimització amb garanties de seguretat que suposés que a l'àrea de pacients només tenen accés a dades de donants seudonimitzades, i a l'àrea de donants només accedeixen a dades seudonimitzades dels pacients.

Comentari:

Entenem que hi ha hagut un malentès per part de l'auditor, ja que aquesta separació tècnica i funcional entre l'àrea de pacients i donants ja està implementada. L'únic departament que té accés a les dades seudonimitzades de pacients i donants es Workups i es necessari per tal d'assegurar la correcta gestió del trasplant.

Responsable: REDMO

4.6.2 Gestió Econòmica

Observacions:

En la mesura del que sigui possible, s'hauria de procurar que les factures incloguessin dades seudonimitzades (sense identificar persones, sinó només codis), ja que la identificació de les persones resulta innecessària en la facturació de serveis a assegurances o a administracions públiques.

Acció Correctora: En les factures s'ha canviat el nom de la persona per el numero de la Seguretat Social.

Responsable: REDMO

4.6.3 Donants i pacients

Observacions:

Per tal de minimitzar el risc en el tractament de les dades, totes les comunicacions que continguin dades sensibles o de categoria especial (per exemple, dades de salut) no haurien d'enviar-se a través del correu electrònic ordinari, sinó aplicant mesures i procediments d'encriptació, sempre que sigui possible i això no suposi posar en perill la salut de les persones involucrades en els processos de donació. En aquest sentit, cal que l'entitat fomenti el desenvolupament de comunicacions segures amb els seus interlocutors i que només de forma justificada es plantegi fer servir formes de comunicacions poc segures, com ara el correu electrònic ordinari.

Comentari: Som conscients d'aquest punt de millora, i sempre que es possible les comunicacions es fan via EMDIS i encriptades. El problema resideix en que molts dels receptors no accepten les comunicacions encriptades per falta de recursos, en aquests casos s'envia la informació sense encriptar i es para especial atenció a la confidencialitat d'aquesta comunicació. Entenem així que essent la prioritat del REDMO la de trobar un donant per un pacient, tenim que donar prioritat a la ràpida gestió del trasplant abans que a l'encriptació d'aquestes comunicacions concretes.

Responsable: REDMO

5 Avaluació, manteniment i avaluació de les pràctiques de protecció de dades.

Per satisfer contínuament el RGPD, la Delega de de Protecció de dades continua fent seguiment de la correcta aplicació del reglament, donant suport als diferents departaments en l'aplicació del reglament per a nous projectes i resolució de dubtes.

5.1 Procés d'esborrat de dades

Conjuntament amb el departament de donants REDMO s'ha establert un procediment de treball mes detallat per a la gestió de les sol·licituds d'esborrat.

5.2 Sol·licituds de drets dels Interessats

Durant el 2020 s'han rebut i processat 9 sol·licituds d'esborrat de dades de la base de dades de la fundació i del REDMO.

5.3 Contractes

Es segueixen revisant i adequant al RGPD la contractació amb terceres parts.

6 Referencies

- REGLAMENT (UE) 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 i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades)
- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals
- Registre d'Activitats de Tractament FIJC.