

	Informe d'Avaluació RGPD
Delegada de Protecció de dades: Iris Bargalló	Data: 21/03/2019

1	Introducció.....	2
2	Objectiu	2
3	Responsabilitats	2
4	Avaluació i anàlisi de situació	2
4.1	Definició de Fluxos de dades personals	2
4.2	Unitats	2
4.3	Registre d'Activitats de Tractament (RAT)	3
5	GAP anàlisi i Accions Correctores	3
5.1	Introducció	3
5.2	Riscos principals i Accions Correctores	3
5.2.1	Tots els Unitats	3
5.2.2	Finances	3
5.2.3	Comunicació	4
5.2.4	Biobank i Lab Managing	4
5.2.5	Biobank	4
5.2.6	Grups de Recerca	4
5.3	Terminis d'implantació	5
6	Avaluació, manteniment i avaluació de les pràctiques de protecció de dades.	5
7	Referències	5
8	Annexa	5
9	Aprovació	5

1 Introducció

L'IGTP està en procés d'implementar les mesures de protecció de dades necessàries per complir amb 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.

2 Objectiu

L'objectiu d'aquest informe és identificar les àrees que s'han de resoldre i les accions que s'haurà de dur a terme per adaptar-se als requeriments del reglament i llei esmentats anteriorment.

3 Responsabilitats

Gerent – Sr. Carles Esquerrè

Delegada de Protecció de dades – Sra. Iris Bargalló

4 Avaluació i anàlisi de situació

4.1 Definició de Fluxos de dades personals

S'ha realitzat un exercici de mapatge de dades personals amb l'objectiu d'identificar les dades personals recollides i tractades en cada unitat de l'IGTP. A més definir les activitats de tractament de dades personals.

L'exercici de cartografia de dades personals s'ha realitzat per a tots els unitats de l'IGTP amb la col·laboració i l'aprovació de tots els representants de les unitats. Els resultats de cada exercici de definició de flux de dades personals ha quedat documentat i s'ha facilitat una còpia a cada unitat corresponent.

4.2 Unitats

Els següents unitats han participat en les diferents reunions de definició de fluxos de dades personals:

- IT
- Amics de Can Ruti
- Biobank
- CEIC
- CMCiB
- Compres
- Comunicació
- Diagnòstic Genètic
- Finances
- GCAT
- Grant Management
- Grups de Recerca
- HHRR
- Innovation & Transfer Office
- Lab Managing
- Secretaria Direcció
- Serveis Generals
- UPIC

4.3 Registre d'Activitats de Tractament (RAT)

Després de les avaluacions realitzades per les diferents unitats i processos de l'IGTP i les activitats de tractament de tercers, s'ha creat un registre d'activitats de tractament que reuneix tota l'activitat de dades personals.

5 GAP anàlisi i Accions Correctores

5.1 Introducció

Després de l'avaluació de la preparació, s'ha desenvolupat i definit un pla d'acció per mitigar els riscos identificats durant l'exercici de definició de fluxos de dades personals. Aquests s'han prioritzat tenint en compte els riscos implicats per a la persona interessada i la institució, equilibrats amb el nivell d'esforç i recursos necessaris.

Els riscos i el pla d'acció complet estan llistats, definits i prioritzats en el document "Informe CAPA RGPD de IGTP"

El pla serà aprovat per Direcció i inclourà accions per a cada unitat.

5.2 Riscos principals i Accions Correctores

Seguint els resultats de l'avaluació de cada unitat, s'indica a continuació les principals àrees identificades com a risc potencial per a les persones i l'IGTP.

5.2.1 Totes les Unitats

1. **Compliment i coneixement dels requisits del RGPD.** Proporcionar una formació als gestors de dades personals de l'IGTP és fonamental per assegurar-se que entenen completament el seu paper en el compliment i manteniment dels requisits del RGPD, a més d'evitar controls d'informació inadequats que augmentin la probabilitat que la informació sigui compartida de manera inapropiada.

Acció Correctora: Implementació dels següents procediments / acords.

1. Codi de conducta per al tractament de dades personals
2. Política de privacitat de dades personals per a empleats
3. Sessió educativa en GDPR.

2. **Gestió de violacions de seguretat de dades personals.**

Acció Correctora: Per satisfer els requisits del RGPD, s'haurà d'actualitzar / implementar el procés de gestió de violacions de seguretat de dades personals, inclosos els sistemes d'identificació d'infraccions de dades, procediments de notificació i plans de resposta. IGTP produirà els següents procediments.

1. Procediment de gestió de violacions de seguretat de dades personals
2. Registre de violacions de seguretat de dades personals
3. Formulari de Notificació a l'autoritat de control
4. Formulari de notificació als interessats.

5.2.2 Finances

1. **Finances rep informació identificativa dels pacients** sense codificar o pseudonimitzar de Neurogenètica i les proves diagnòstiques que han realitzat. Aquest tipus de dades estan considerades com a categories especials de dades, segons el RGPD necessàriament s'ha de tenir una base legal específica per al seu tractament.

Acció Correctora: Es recomana rebre la informació identificativa del pacient codificada.

2. **Participants en assajos clínics, es té informació de l'assaig en què estan participant.** Aquest tipus de dades està considerat com a categories especials de dades, segons el RGPD necessiten un licitud específica per al seu tractament, que el unitat de finances no té.

Acció Correctora: Es recomana codificar els assajos amb número i només facilitar aquest a finances.

5.2.3 Comunicació

1. **Política de Privacitat i formularis web** no segueixen les indicacions del RGPD

Acció Correctora Actualitzar Política de privacitat i textos de protecció de dades de les webs.

5.2.4 Biobank i Lab Managing

1. **Recepció de mostres amb nom de pacient en etiqueta i visible** a més de documentació de pacient o petició amb dades personals de categories especials visibles

Accions Correctores:

1. Recodificació de les mostres a recepció.
2. Aplicar mesures de seguretat apropiades en desar documentació i mostres.
3. Informar el responsable de l'enviament del risc de violació de seguretat de dades segons nou reglament.
4. Sensibilitzar i informar els responsables de l'enviament de la importància d'aplicar mesures de seguretat.

5.2.5 Biobank

1. **Mostres biològiques sòlides** en congeladors ubicades en sala amb accés amb clau. A aquesta sala tenen accés mes unitats i no hi ha registre d'accés.

Accions Correctores:

1. Implementar Registre d'accés a les mostra i congeladors
2. Aplicar mesures de seguretat apropiades perquè solament el personal de l'Biobanc tingui accés a les mostres.

5.2.6 Grups de Recerca

1. **Recepció de correus electrònics amb nom de pacient** en o amb dades personals de categories especials visibles en el cos del correu electrònic.

Accions Correctores:

1. Esborrat de dades identificatives a recepció.
 2. Aplicar mesures de seguretat apropiades en desar documentació i mostres.
 3. Informar el responsable de l'enviament del risc de violació de seguretat de dades segons nou reglament.
 4. Sensibilitzar i informar als responsables de l'enviament de la importància d'aplicar mesures de seguretat.
2. No es fa **doble control d'entrada de dades** en les bases de dades dels assajos.

Accions Correctores: Implementar i documentar doble control en entrada de dades en els assaigs i projectes de recerca.

5.3 Terminis d'implantació

Els terminis i les persones responsables assignades per mitigar i prevenir els riscos identificats durant l'exercici d'avaluació de protecció de dades s'han detallat a l'Informe Informe CAPA RGPD de IGTP. No obstant això, el termini objectiu per implementar totes les accions correctives és el 31 de Juliol de 2019.

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

Per satisfer contínuament el RGPD, L'IGTP farà un seguiment i documentaran evidència del compliment del RGPD mitjançant la creació d'un Pla d'auditoria de protecció de dades, que s'haurà de seguir i utilitzarà per recollir els resultats d'auditoria i establirà les bases per a un pla continu de millora de la protecció de dades.

7 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 IGTP

8 Annexa

- Informe CAPA RGPD de IGTP

9 Aprovació

Aquest pla d'acció RGPD ha estat aprovat i signat per el Sr. Carles Esquerrè, Gerent de l'IGTP.

Signatura:

Data:

.....

.....