EQUIP D'ASSITÈNCIA PRIMÀRIA VIC, S.L.P.

Informe d'avaluació d'impacte de dades personals per implementació de nova tecnologia de signatura electrònica en la recollida i gestió de consentiments en el tractament de dades de pacients, d'acord amb el Reglament (UE) 2016/679 general de protecció de dades.

Protocol número: C-11.631

ÍNDEX

1. IDENTIFICACIÓ DEL PROJECTE

El 25 de maig de 2018 va entrar en aplicació el Reglament (UE) 2016/679 del Parlament 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, també referit com a RGPD). A finals de l'any 2018 es va aprovar la nova Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDiGDD), que adapta el RGPD a l'ordenament jurídic espanyol. Aquest règim legal sobre protecció de dades preveu que, davant la possibilitat que un tractament comporti un alt risc per als drets i llibertats de les persones físiques, es dugui a terme una avaluació d'impacte de protecció de dades (en endavant, AIPD) abans de la posada en marxa del tractament. Aquesta obligació està en consonància amb el principi de privacitat, que contempla analitzar un tractament des de la seva fase de disseny i garantir una adequada gestió dels riscos, a més de complir els principis de necessitat i proporcionalitat.

L'AIPD és una eina que permet avaluar de manera anticipada quins són els riscos potencials a què estan exposades les dades personals, en funció de les activitats de tractament que es duguin a terme.

El GT29, mitjançant una guia (WP248 'Guies sobre les Avaluacions d'Impacte en Protecció de Dades'), defineix un risc com a "*un escenari que descriu un esdeveniment i les seves conseqüències, estimat en termes d'impacte i probabilitat*". Per tant, la gestió de riscos és el conjunt d'activitats i tasques realitzades en una organització per monitoritzar i controlar la seva exposició als riscos.

En data 6 de maig de 2019 les autoritats de control en matèria de protecció de dades han publicat els llistats amb els tractaments de dades en què és obligatòria la realització d'una avaluació d'impacte. En els següents enllaços es poden consultar els llistats publicats per l'Agència Espanyola de Protecció de Dades (AEPD) i l'Autoritat Catalana de Protecció de Dades (APDCAT).

L'AIPD és una eina de caràcter preventiu que ha de realitzar el responsable del tractament per poder identificar, avaluar i gestionar els riscos a què estan exposades les seves activitats de tractament, amb la finalitat de preservar els drets i llibertats de les persones físiques. A la pràctica, l'AIPD permet determinar el nivell de risc que implica un determinat tractament i adoptar les mesures de seguretat que es considerin més oportunes per minimitzar-los. L'execució d'una AIPD implica la consideració de diversos factors que permetin establir una ruta de treball i la seva estructuració en diferents fases.

Caldrà que el resultat de l'AIPD es tingui en compte a l'hora de prendre les decisions relacionades amb el compliment del RGPD, la gestió del risc i l'oportunitat de dur a terme el tractament de les dades en determinades condicions.

1.1 RESPONSABLES DEL PROJECTE I DADES DE CONTACTE

Entitat	Equip d'Assistència Primària Vic, S.L.P. (EAP EL REMEI)
CIF	B-60899622
Domicili	Passatge del Pla del Vent, 10-12 08200 Vic (Barcelona)

1.2 DESCRIPCIÓ DE L'ACTIVITAT DE TRACTAMENT AVALUADA

L'activitat de tractament avaluada és la que correspon al tractament de les dades personals de la història clínica i a la prestació del servei assistencial, tal com es presta des de la societat Equip d'Assistència Primària Vic, S.L.P. (en endavant, EAP VIC), centrada en la implementació d'una nova tecnologia per a la comunicació de la informació rellevant als pacients i la recollida i gestió dels seus consentiments a través de signatura electrònica. En aquest sentit, s'ha avaluat de forma específica la implementació d'aquesta nova tecnologia de signatura electrònica i els riscos que pugui comportar.

L'Equip d'Assistència Primària de Vic és una entitat de base associativa de professionals sanitaris. Està formada per socis i altres professionals no socis que formen l'EAP VIC. Aquest model d'autogestió està pensat per promoure la implicació dels professionals sanitaris. D'aquesta manera s'incrementa la implicació en el servei ofert, sempre amb la voluntat de mantenir una relació de proximitat amb els usuaris i amb la màxima qualitat.

L'entitat presta assistència a 24.000 usuaris dels municipis de Vic, la Guixa, Muntanyola i Santa Eulàlia de Riuprimer. L'equip de professionals de l'EAP treballen principalment al CAP El Remei. L'EAP actua principalment com a proveïdor de la xarxa pública de salut i treballa en l'àmbit assistencial d'atenció primària sanitària de medicina general, infermeria, odontologia, atenció a la dona, programa d'atenció domiciliària, atenció a l'usuari, anàlisis clíniques i administració.

L'activitat de tractament objecte d'avaluació és posterior a l'entrada en aplicació del RGPD.

1.3 EQUIP D'AVALUACIÓ I PERSONES ENTREVISTADES

Els treballs de la present avaluació d'impacte s'han dut a terme per part de dos consultors de Faura-Casas experts en protecció de dades.

Per part de l'Entitat, es citen a continuació les persones entrevistades durant els treballs:

PERSONA ENTREVISTADA	CÀRREC/ÀREA DE TREBALL
José Antonio Carvajal	Delegat de Protecció de Dades, Servei de Pediatria, Responsable TIC i President del Consell d'Administració
Jordi Subirana	Responsable de Sistemes Informàtics
Marc Vila	Infermer

1.4 DATA DE REALITZACIÓ DE L'AVALUACIÓ D'IMPACTE

Dia	1 d'abril de 2019

1.5 VERSIÓ DE L'INFORME

- Primera versió de l'informe d'avaluació d'impacte de dades personals de l'activitat de prestació del servei assistencial en relació a l'ús de tecnologia de signatura electrònica per a la informació, recollida i gestió de consentiments dels interessats de data 23 de maig de 2019.

2. ANÀLISI DE LA NECESSITAT DE REALITZAR UNA AVALUACIÓ DE IMPACTE

La normativa estableix la necessitat legal de dur a terme una avaluació d'impacte en determinats casos, sense que això vulgui dir que en d'altres casos no sigui totalment necessària o recomanable com a eina habitual d'avaluació de riscos.

És fonamental realitzar una anàlisi prèvia per determinar de forma preliminar el nivell de risc a què pot estar exposat el tractament i prendre la decisió adequada d'acord amb el resultat.

Per determinar l'obligatorietat o necessitat de realitzar una AIPD, primer cal valorar si l'activitat de tractament s'inclou en algun dels supòsits inclosos als articles 35.1, 35.3, 35.4 i 35.5 RGPD. Seguidament, caldrà analitzar els nou criteris complementaris definits al document "Directrius sobre l'avaluació d'impacte relativa a la protecció de dades (EIPD) i per determinar si el tractament «comporta probablement un alt risc» a efectes del Reglament (UE) 2016/679" (també referit com a WP 248), del Grup de Treball de l'article 29, creat al seu torn per la Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, que poden evidenciar un elevat risc inherent a les operacions de tractament i que poden apuntar també a la necessitat de fer una AIPD.

D'altra banda, a data 6 de maig de 2019, tant l'Agència Espanyola de Protecció de Dades (AEPD) com l'Autoritat Catalana de Protecció de Dades (APDCAT) publiquen els llistats de tractaments de dades en què és obligatori fer una avaluació d'impacte, de conformitat amb l'article 35.4 RGPD. Segons aquestes autoritats de control, si un tractament de dades compleix dos o més criteris dels establerts als seus llistats, ja seria obligatòria la realització d'una avaluació d'impacte de forma prèvia a l'inici del tractament.

2.1. OBLIGACIÓ DE FER L'AIPD

Elements a analitzar	SI	NO
Avaluació sistemàtica i exhaustiva d'aspectes personals d'una persona; inclou l'elaboració de perfils.		x
Tractament a gran escala de dades sensibles.	x	
Observació sistemàtica a gran escala d'una zona pública.		x
Les Autoritat nacionals de protecció de dades proporcionaran llistes dels casos en què s'exigeix una AIPD.	x	

Implementació d'una nova tecnologia. Segons l'art. 35.1 del RGPD, s'identifica l'ús de noves tecnologies com a causa per realitzar una AIPD.		x

Elements complementaris: [1]	**SI**	**NO**
1. La iniciativa implica relacionar diferents fonts o orígens de dades personals (creuar informació) que, d'alguna manera, incrementen la capacitat d'anàlisi de la informació?		x
2. Avaluació o puntuació (inclosa l'elaboració de perfils)		x
3. Presa de decisions automatitzada amb efecte jurídic significatiu o similar		x
4. S'utilitzen tecnologies que poden ser especialment intrusives per a la privacitat? Observació sistemàtica o tecnologies invasives		x
5. Es tracten categories especials de dades o dades relatives a condemnes o infraccions penals?	x	
6. Es tracten dades de menors o col·lectius vulnerables?	x	
7. Es tracten dades a gran escala?	x	
8. El mateix tractament impedeix als interessats exercir un dret o utilitzar un servei o executar un contracte?		x
9. Ús innovador de noves tecnologies	x	
TOTAL RISC (4/9)	**44,44%**	

2.2. RESULTAT DE L'ANÀLISI

L'activitat de tractament de la prestació assistencial sí que respon, d'entrada, a supòsits de realització obligada d'una avaluació d'impacte, de conformitat amb l'article 35 del RGPD, ja que

[1] Conforme als nou criteris definits a les "*Directrices sobre Evaluación de Impacto en materia de protección de datos del Grupo artículo 29 WP 248*".

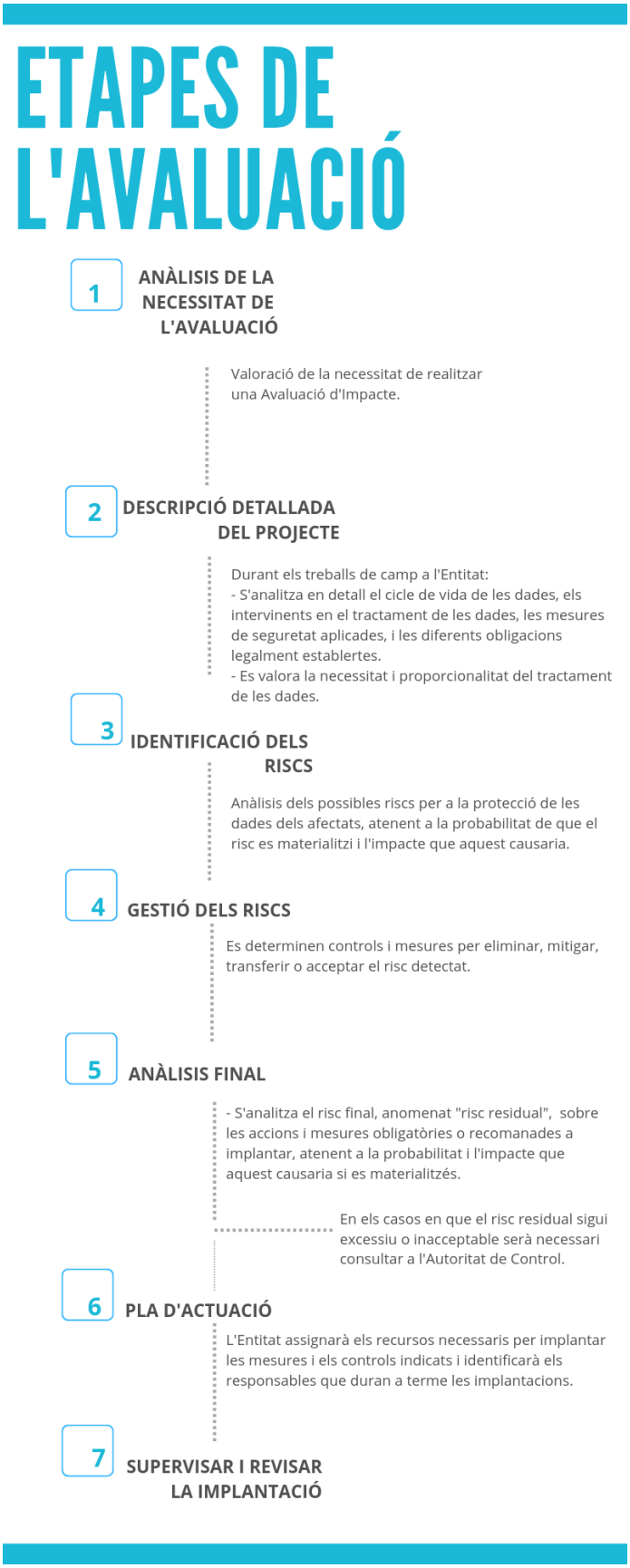
preveu el tractament de dades sensibles a gran escala. No obstant, dins d'aquesta activitat de tractament, les tasques corresponents a la informació, obtenció i gestió dels consentiments dels interessats no impliquen tractament de dades sensibles. Per tant, és convenient fer també l'anàlisi complementària, d'acord amb els criteris definits al document precitat WP 248 del Grup de Treball de l'article 29. Segons aquesta anàlisi, el tractament, restringit a la gestió de la informació i els consentiments, presenta un risc de 44,44%, ja que compleix quatre criteris. D'acord amb el document WP 248, n'hi ha prou amb què es compleixin dos criteris perquè, en la majoria dels casos, el responsable requereixi la realització d'una avaluació d'impacte. Per tant, en complir-ne quatre, l'activitat específica objecte d'avaluació requereix la realització d'una avaluació d'impacte.

D'altra banda, d'acord amb els llistats de tractaments de dades en què és obligatòria la realització d'una avaluació d'impacte, segons han publicat les autoritats de control el dia 6 de maig de 2019, el tractament que és objecte d'anàlisi compliria dos o més dels criteris i, per tant, també segons aquest criteri, l'avaluació d'impacte seria obligatòria. En concret, es compliria el requisit de tractar dades a gran escala i el requisit d'implicar una nova tecnologia que pot posar en risc els drets i llibertats de les persones.

Pels motius expressats i a requeriment de l'entitat, procedim a identificar, analitzar i valorar detalladament els riscos que pugui presentar el tractament de dades objecte d'avaluació.

3. RESUM EXECUTIU

3.1 DESCRIPCIÓ EXECUTIVA DEL PROJECTE I DEL MÈTODE D'AVALUACIÓ



3.2 PRINCIPALS AMENACES QUE S'HAN IDENTIFICAT

Les principals amenaces que s'han identificat en realitzar l'anàlisi detallada del tractament de dades, són les que s'exposen a continuació:

- Possibilitat que hi hagi accés no autoritzat per part d'un proveïdor que accedeixi a les dades.
- Risc que la informació que es proporciona sobre el tractament no s'avingui amb les previsions de l'art. 13 RGPD.
- No consta procediment de modificació de contrasenyes ni de limitació d'intents d'accessos fallits, ni en l'aplicació de signatura electrònica ni en els altres programes.
- L'aplicació de signatura electrònica no té implementada mesura de bloqueig per inactivitat. Possibilitat d'accés no autoritzat a l'aplicació a través de tauletes o PCs.
- Pèrdua de la unitat de memòria -encriptada- que conté la còpia de seguretat en el seu trasllat.
- Falta de diligència o mala fe en l'ús de l'aplicació i de la informació confidencial sobre els pacients per part del personal autoritzat.
- Risc de tall en el subministrament elèctric.
- Error tècnic: Possibilitat de caiguda de servidor o de mal funcionament en general dels dispositius (pistoles o tauletes) a l'hora de recollir consentiments.
- Possibilitat que es desatengui un consentiment rebutjat o que no es tinguin en compte els consentiments realment prestats pel consentiment.

3.3 RESUM DE LES MESURES MÉS RELLEVANTS QUE S'HAN PROPOSAT PER MITIGAR ELS RISCOS

- Fer signar i/o actualitzar un acord de confidencialitat amb empreses que puguin tenir un accés accidental a les dades, especialment amb l'empresa Dadà Comunicació. De la mateixa manera, mantenir contracte d'encarregat de tractament amb els proveïdors que tractin dades, com ara Validated ID, S.L.
- Millorar la informació que es proporciona perquè sigui conforme a l'art. 13 RGPD i informi correctament sobre la finalitat de la recollida, la base jurídica, el procediment d'exercici dels drets dels interessats, els destinataris i la prestació dels consentiments, sobre els quals cal informar sempre sobre la possibilitat de revocar-los.

- Implementar procediments de renovació obligada de contrasenyes, segons els quals totes les contrasenyes hagin de ser modificades anualment. Aplicar mesures de limitació d'intents d'accés fallits en tots els programes utilitzats per al tractament de les dades.

- Aplicar mesura de bloqueig per inactivitat al programa de gestió de consentiments i signatura electrònica, ja que aquesta mesura no es troba implementada en tots els suports i dispositius amb què es treballa habitualment. Sí que està implementada en les tauletes per defecte, però no en els ordinadors. Així, per exemple, no es pot controlar que els que treballen des de casa tinguin aquesta mesura implementada. Per tant, el més adequat és implementar una mesura de bloqueig per inactivitat al programa.

- Assegurar la seguretat mitjançant la correcta realització de procediments d'identificació, d'assignació, de registre d'entrades i sortides en relació a les unitats de memòria que es fan servir habitualment per a la conservació de la còpia de seguretat mensual, i mantenir el procediment d'encriptació.

- Proporcionar formació i informació al personal actualitzada sobre protecció de dades, especialment relativa al DPD i al procediment de notificació i comunicació d'una violació de seguretat, però també sobre el deure de confidencialitat i les mesures de seguretat aplicables.

- A part de mantenir l'ús del SAI com a solució general, per al cas d'impossibilitat de prestar el servei, caldria preveure procediment alternatiu a través de documentació en paper.

- Preveure procediment alternatiu per al cas eventual de no disposar temporalment dels recursos tècnics necessaris, de manera que, en aquests casos, es pugui continuar prestant servei i registrant els consentiments mitjançant l'ús de documentació en paper.

- Millorar el procediment pel qual l'aplicació avisa el treballador de l'entitat sobre els consentiments rebutjats dels pacients. Assegurar que tots els treballadors autoritzats coneixen la importància de basar-se en els consentiments efectivament prestats per l'interessat abans d'iniciar qualsevol nou tractament de de les dades.

3.4 MESURES QUE AFECTEN ALS ENCARREGATS DE TRACTAMENT

- Signar un contracte d'encàrrec de tractament amb Validated ID, S.L.

- Definir procediments per garantir signar els contractes d'encàrrec de tractament de dades que corresponguin.

3.5 NECESSITAT DE FER UNA CONSULTA PRÈVIA

Conforme a l'article 36 del RGPD, el responsable del tractament consultarà l'Autoritat de control competent abans d'iniciar el tractament, quan una avaluació d'impacte relativa a protecció de dades en virtut de l'article 35 del RGPD mostri que el tractament suposa un alt risc per als drets i llibertats dels interessats, si el responsable del tractament no aplica les mesures oportunes per mitigar-lo.

Es conclou que el tractament avaluat no requereix una consulta prèvia a l'Autoritat de control competent, per diferents motius, però sobretot perquè, com es pot comprovar, l'entitat compta amb mesures de seguretat necessàries per mitigar els riscos identificats de forma suficient i substancial. Això no treu, d'altra banda, que aquests riscos no puguin reduir-se ni minimitzar-se, tal com correspon actuar a un responsable del tractament.

4. DESCRIPCIÓ DETALLADA DEL PROJECTE

4.1 DESCRIPCIÓ DEL/S TIPUS DE DADES I DEL/S TRACTAMENT/S

L'Entitat sol·licita dur a terme una avaluació d'impacte en relació a la implantació d'una nova tecnologia de signatura electrònica en el procediment d'informació i recollida de consentiments dels usuaris dels seus serveis. Les dades tractades són dades de pacients de la societat EAP VIC, que gestiona, entre d'altres, el CAP El Remei, de Vic.

4.2 DESCRIPCIÓ DETALLADA I FUNCIONAL. ELEMENTS RELLEVANTS

	Obtenció de les dades	Classificació	Ús	Cessió / Transferència	Destrucció
Procés	En general, obtenció dels propis pacients i introducció en entorn informàtic OMI.	No aplica un procés de classificació com a tal.	Programa de gestió d'informació, consentiments i signatura electrònica. D'altra banda, programa OMI per a la gestió general de pacients i històries clíniques.	Es fa a través dels propis programes de l'HC3, el SI-SISO i el SISCAT, per complir el contínuum assistencial.	No consten procediments ni terminis definits de destrucció de documentació en paper.
Dades tractades	Dades d'identitat (nom, adreça i DNI) i de contacte, però també dades sobre la seva salut i històries clíniques.	No aplica un procés de classificació com a tal.	Dades d'identificació i contacte, però també dades sobre la seva salut i històries clíniques.	Dades d'identificació i contacte, però també dades sobre la seva salut i històries clíniques.	Dades d'identificació i contacte, però també dades sobre la seva salut i històries clíniques.
Intervinents	Persones autoritzades a realitzar la recollida, generalment de la Unitat d'Atenció a l'Usuari.	No aplica un procés de classificació com a tal.	Les dades són tractades només pel personal autoritzat de l'Entitat. Hi poden accedir, amb diferents perfils, personal administratiu i sanitari.	Diferents perfils autoritzats poden participar dels processos de comunicació, però sobretot són els mateixos professionals sanitaris.	No hi ha actualment un perfil autoritzat específicament a la destrucció.

Tecnologies utilitzades	Programa de gestió d'informació, consentiments i signatura electrònica. D'altra banda, programa OMI per a la gestió general de pacients i històries clíniques.	No aplica un procés de classificació com a tal.	Programa de gestió d'informació, consentiments i signatura electrònica. D'altra banda, programa OMI per a la gestió general de pacients i històries clíniques.	HC3 (història clínica compartida de Catalunya). Plataformes SI-SISO (història clínica compartida a Osona) i SISCAT (proveïdors d'atenció especialitzada)	No s'apliquen programes de destrucció específics.

Interessats	Pacients dels centres de salut gestionats per EAP VIC, especialment el CAP El Remei, de Vic.
Responsable del tractament	EQUIP D'ASSITÈNCIA PRIMÀRIA VIC, S.L.P.
Encarregat del tractament	Validated ID, S.L.
Terceres parts involucrades	Els tercers disposen d'un compromís de confidencialitat signat, segons informacions proporcionades. En aquest cas, Dadà Comunicació.
Cessions de dades	Es comuniquen dades a CatSalut i a l'HC3 (història clínica compartida de Catalunya), al SI-SISO (història clínica compartida d'Osona) i al SISCAT (proveïdors d'atenció especialitzada).
Mesures de seguretat	Tots els programes que es fan servir per a l'obtenció i tractament de les dades preveuen mesures de control d'accés per usuari i contrasenya individuals (contrasenya de mida mínima i alfanumèrica). No es preveu bloqueig per inactivitat a l'OMI. No es preveu una política de modificació de contrasenyes. Sí que hi ha un procediment implementat de revisió i control d'accessos indeguts.
Còpies de seguretat	Les còpies de seguretat de l'Entitat es realitzen a través de tres procediments: es realitza una còpia granular diària per a fitxers de dades, una còpia completa setmanal i una còpia també completa mensual, que es guarda encriptada en una unitat de memòria, desada en una cabina i lluny del servidor del centre de replicat, que és l'ABS Centelles "El Congost". Tant la còpia granular diària com la còpia setmanal es repliquen en el servidor de l'ABS de Centelles "El Congost"

Procediment per complir amb el deure d'informació	Es proporciona un document d'informació als pacients, que, en general, és conforme a la normativa en matèria de protecció de dades i al RGPD. Amb el nou procediment, es preveu que aquest document es continuï proporcionant en paper, però que es signi en una tauleta per part de l'interessat.
Procediment d'obtenció del consentiment (quan sigui necessari)	S'obtenen diferents consentiments sobre protecció de dades, especialment per a habilitar formes de comunicació i comunicacions. També s'obtenen consentiments sanitaris. La nova aplicació ha de facilitar que aquests consentiments es puguin obtenir de forma electrònica, fent servir una taula que contingui l'aplicació, la signatura electrònica i la marcació de les opcions desitjables per part de l'interessat.
Procediment per a l'exercici dels drets per part dels interessats	Segons la informació legal que dona l'entitat sobre el tractament a través de diferents documents, ja es proporciona una informació sobre procediment d'exercici de drets, que passa per enviar un correu electrònic al Delegat de Protecció de Dades.
S'identifiquen les obligacions i mesures de seguretat dels encarregats del tractament al contracte	En general, ja es disposa de contractes d'encàrrec de tractament que ja estiguin actualitzats i adaptats al RGPD.
Procediment per donar compliment a la notificació d'incidències de seguretat	Ja hi ha un procediment definit de notificació de violacions de seguretat que passa pel Delegat de Protecció de Dades, tal com s'identifica en la informació legal que es proporciona.
En cas d'existència de transferències internacionals fora de la UE, son adequades?	No consten.

4.3 OBJECTIUS I FINALITATS DEL TRACTAMENT

4.3.1. BASE DE LA LEGITIMACIÓ

LEGITIMACIÓ	
Legitimació	Article 9.2.h RGPD: el tractament és necessari per a finalitats de prestació d'assistència sanitària i social.
Justificació	La base jurídica que legitima la prestació d'assistència i tractament de tipus sanitari legitima alhora l'obtenció dels consentiments sobre protecció de dades i sanitaris que siguin necessaris d'acord amb la normativa aplicable.

4.3.2. NECESSITAT I PROPORCIONALITAT DE LES OPERACIONS DEL TRACTAMENT

NECESSITAT I PROPORCIONALITAT		
	(SI/NO)	*Comentaris:*
Les dades recollides seran utilitzades exclusivament per a la finalitat declarada i no per a cap altra no informada ni incompatible amb la legitimació d'ús (principi delimitació a finalitat).	Sí	
La finalitat perseguida requereix de totes les dades recollides i de totes les persones afectades (principi de minimització)	SI	
Les tecnologies utilitzades per al tractament són escaients i adients a la finalitat, també des del punt de vista dels drets fonamentals	SI	
Les dades no es conserven durant més temps del necessari per a l'acompliment de la finalitat (principi de limitació del termini de conservació)	SÍ	

4.3.3. CODIS DE CONDUCTA

L'article 40 del RGPD estableix que els estats membres, les autoritats de control, el Comitè i la Comissió promouran l'elaboració de codis de conducta destinats a contribuir a la correcta aplicació de la normativa en matèria de protecció de dades, tenint en compte les característiques específiques dels diferents sectors de tractament i les necessitats específiques de les microempreses i las petites i mitjanes empreses.

Els codis de conducta s'elaboraran per part d'associacions i d'altres organismes representatius de categories de responsables i encarregats, per als quals seran vinculants, un cop adherit al codi de conducta. Els codis de conducta preveuran l'aplicació del RGPD a las característiques i necessitats dels diferents sectors d'activitat pel que fa als següents punts:

- El tractament lleial i transparent
- Els interessos legítims perseguits pels responsables del tractament en contextos específics
- La recollida de dades personals
- La seudonimització de les dades personals

- La informació proporcionada al públic i als interessats
- L'exercici dels drets dels interessats
- La informació proporcionada al públic i als interessats
- L'exercici dels drets dels interessats
- La informació proporcionada als infants i la seva protecció, com també la forma d'obtenir el consentiment dels titulars de la pàtria potestat o tutela.
- Les mesures i procediments per garantir la seguretat del tractament i la protecció de les dades des del disseny i per defecte.
- La notificació de violacions de seguretat de les dades personals a les autoritats de control i la comunicació de les violacions als interessats
- La transferència de dades personals a tercers països i organitzacions internacionals
- Els procediments extrajudicials i d'altres procediments de resolució de conflictes.

L'Entitat no està adherida actualment a cap codi de conducta inscrit en una autoritat de control.

5. IDENTIFICACIÓ I GESTIÓ DE RISCOS

En els punts següents s'exposen els riscos detectats, s'identifiquen les amenaces i les possibles conseqüències, atenent l'impacte i la probabilitat de materialització d'acord amb els criteris següents:

Impacte (I)

Nivell	Classificació	Descripció
1	**Menyspreable**: Els interessats no es veuran pràcticament afectats o trobaran alguna petita inconveniència	• Molèsties o irritació a persones físiques. • S'incompleixen obligacions materials sense perjudicis rellevants. • No es priva dels drets i llibertats.
2	**Limitat**: Els interessats podran trobar inconveniències no significatives	• Estrès o patiment físic menor de persones físiques. • Costos extra, denegació d'accés a alguns serveis o incompliment d'obligacions materials amb perjudicis econòmics. • Es priva dels drets i llibertats dels interessats, per exemple, per difamació d'un interessat per divulgació de dades personals.
3	**Significatiu**: Els interessats trobaran conseqüències significatives, que haurien de poder superar sense dificultats serioses.	• Empitjorament de l'estat de salut o agressions físiques. • Apropiació indeguda de fons, pèrdua de la feina o incompliment d'obligacions materials amb perjudicis econòmics rellevants. • S'agredeixen els drets i llibertats dels interessats, com en els exemples següents: una citació judicial, la inclusió en una llista de morositat o la divulgació de dades personals amb impacte significatiu en la reputació de l'interessat.
4	**Màxim**: Els interessats trobaran conseqüències significatives o fins i tot irreversibles, que podran no arribar a superar-se.	• Agressions físiques amb conseqüències irreparables. • Assumpció d'un deute inassolible, impossibilitat de tornar a treballar o incompliment d'obligacions materials amb perjudicis econòmics irreparables. • S'agredeixen significativament els drets i llibertats dels interessats, com, per exemple, en els següents casos: sofriment psicològic amb conseqüències a llarg termini o irreparables per la divulgació de dades sensibles.

Probabilitat (P)

Nivell	Classificació	Descripció
1	**Menyspreable:** La possibilitat de materialització és molt baixa (per exemple, un fet que pot passar de forma fortuïta).	No ha passat mai i es preveuen mesures per evitar que passi.
2	**Limitada:** La possibilitat d'ocurrència és baixa (per exemple, un esdeveniment que pot passar de forma ocasional).	No ha passat mai i hi ha mesures per evitar que passi, però no en tots els casos.
3	**Significativa:** La possibilitat de materialització és alta.	Hi ha mesures, però, si una mesura falla, no podrà impedir el fet no desitjat.
4	**Màxima:** Ens trobem en un potencial escenari de risc	No s'han previst mesures per reduir-ne i mitigar-ne el risc de materialització

Resultats del risc:

	MOLT ALT	Valor 8
	ALT	Valor 7
	MITJÀ	Valor de 3 a 6
	BAIX	Valor entre 1 i 2

5.1. IDENTIFICACIÓ, ANÀLISI I VALORACIÓ DETALLADA DELS RISCOS, DELS SEU IMPACTE I PROBABILITAT

El resultat de la identificació, anàlisis i valoració detallada dels riscos es mostra en quadre següent:

Núm. risc	Descripció de l'amenaça	Conseqüència	(P)	(I)	Risc inherent
1	Possibilitat que hi hagi accés no autoritzat per part d'un proveïdor que accedeixi a les dades.	- Incompliment normatiu. - Sancions de l'autoritat de control. - Accés de persona no autoritzada. - Ús il·lícit de les dades. - Fuita d'informació confidencial.	2	2	4
2	Risc que la informació que es proporciona sobre el tractament no s'avingui amb les previsions de l'art. 13 RGPD.	- Possible incompliment normatiu. - Vulneració dels drets dels interessats. - Sancions.	2	1	3
3	No consta procediment de modificació de contrasenyes ni de limitació d'intents d'accessos fallits, ni en l'aplicació de signatura electrònica ni en els altres programes.	- Risc d'accés no autoritzat a les dades i violació de seguretat. - Risc de difusió de les dades.	2	2	4
4	L'aplicació de signatura electrònica no té implementada mesura de bloqueig per inactivitat. Possibilitat d'accés no autoritzat a l'aplicació	- Risc d'accés no autoritzat a les dades i violació de seguretat. - Risc de difusió de les dades.	1	2	3

	a través de tauletes o PCs.				
5	Pèrdua de la unitat de memòria -encriptada- que conté la còpia de seguretat en el seu trasllat.	- Risc de pèrdua d'informació confidencial. - Risc de de difusió o accés il·lícit per part de tercer.	1	2	3
6	Falta de diligència o mala fe en l'ús de l'aplicació i de la informació confidencial sobre els pacients per part del personal autoritzat.	- Possibilitat de difusió d'informació confidencial. - Accés no autoritzat a tercer.	3	2	5
7	Risc de tall en el subministrament elèctric.	- No quedar registrat correctament l'estat de l'interessat sobre si ha rebut la informació sobre el tractament els consentiments. - Vulneració de drets de l'interessat. - Possibles sancions	2	2	4
8	Error tècnic: Possibilitat de caiguda de servidor o de mal funcionament en general dels dispositius (pistoles o tauletes) a l'hora de recollir consentiments.	- Impossibilitat de poder complir el deure d'informació o recollir els consentiments necessaris. - Vulneració de drets	1	2	3
9	Possibilitat que es desatengui un consentiment rebutjat o que no es tinguin en compte els consentiments realment prestats pel consentiment.	- Tractament il·lícit de dades sense la corresponent autorització expressa i inequívoca. - Incompliment del deure d'informació.	2	2	4

6. GESTIÓ DELS RISCOS

En funció al risc inherent avaluat en el quadre anterior es proposen les següents mesures a implementar per mitigar el risc:

6.1 RESUM DE MESURES A IMPLANTAR SEGONS RISC

Núm. risc	Mesura a implementar	(P)	(I)	Risc residual
1	Fer signar i/o actualitzar un acord de confidencialitat amb empreses que puguin tenir un accés accidental a les dades, especialment amb l'empresa Dadà Comunicació. De la mateixa manera, mantenir contracte d'encarregat de tractament amb els proveïdors que tractin dades, com ara Validated ID, S.L.	0	1	1
2	Millorar la informació que es proporciona perquè sigui conforme a l'art. 13 RGPD i informi correctament sobre la finalitat de la recollida, la base jurídica, el procediment d'exercici dels drets dels interessats, els destinataris i la prestació dels consentiments, sobre els quals cal informar sempre sobre la possibilitat de revocar-los.	1	0	1
3	Implementar procediments de renovació obligada de contrasenyes, segons els quals totes les contrasenyes hagin de ser modificades anualment. Aplicar mesures de limitació d'intents d'accés fallits en tots els programes utilitzats per al tractament de les dades.	1	1	2
4	Aplicar mesura de bloqueig per inactivitat al programa de gestió de consentiments i signatura electrònica, ja que aquesta mesura no es troba implementada en tots els suports i dispositius amb què es treballa habitualment. Sí que està implementada en les tauletes per defecte, però no en els ordinadors. Així, per exemple, no es pot controlar que els que treballen des de casa tinguin aquesta mesura implementada. Per tant, el més adequat és implementar una mesura de bloqueig per inactivitat al programa.	1	1	2
5	Assegurar la seguretat mitjançant la correcta implementació de procediments d'identificació, d'assignació, de registre d'entrades i sortides en relació a les unitats de memòria que es fan servir habitualment per a la conservació de la còpia de seguretat mensual, i mantenir el procediment d'encriptació.	0	1	1

6	Proporcionar formació i informació al personal actualitzada sobre protecció de dades, especialment relativa al DPD i al procediment de notificació i comunicació d'una violació de seguretat, però també sobre el deure de confidencialitat i les mesures de seguretat aplicables.	1	1	2
7	A part de mantenir l'ús del SAI com a solució general, per al cas d'impossibilitat de prestar el servei, caldria preveure procediment alternatiu a través de documentació en paper.	0	1	1
8	Preveure procediment alternatiu per al cas eventual de no disposar temporalment dels recursos tècnics necessaris, de manera que, en aquests casos, es pugui continuar prestant servei i registrant els consentiments mitjançant l'ús de documentació en paper.	0	1	1
9	Millorar el procediment pel qual l'aplicació avisa el treballador de l'entitat sobre els consentiments rebutjats dels pacients. Assegurar que tots els treballadors autoritzats coneixen la importància de basar-se en els consentiments efectivament prestats per l'interessat abans d'iniciar qualsevol nou tractament de les dades.	1	1	2

7. CONCLUSIONS

7.1 VALORACIÓ FINAL

Un cop implementades les mesures proposades per minimitzar els riscos detectats en el tractament de les dades que és objecte d'avaluació, els nivells de risc restants serien de nivell baix, raonables i acceptables, i ja no s'identificaria un risc manifest per als drets i llibertats de les persones físiques.

7.2 PLA D'ACTUACIÓ

Com a mesura inicial, cal que el delegat o delegada de protecció de dades informi a la direcció executiva de l'entitat i als òrgans corresponents de direcció jeràrquica sobre el resultat d'aquesta avaluació d'impacte.

Cal que, amb la intervenció del delegat de protecció de dades, l'Entitat prevegi les mesures necessàries de difusió i publicació del resultat d'aquesta avaluació d'impacte que consideri adequades tant a nivell intern com, si és el cas, també a través de la web de l'Entitat.

Amb la supervisió i el consell del delegat o delegada de protecció de dades, el responsable del tractament, en atenció als resultats d'aquesta avaluació d'impacte i abans de començar el tractament, ha de definir els recursos, procediments, persones encarregades i terminis necessaris per dur a terme d'adopció de les mesures proposades de mitigació del risc o, si és el cas, les mesures alternatives que consideri més adients.

D'altra banda, cal tenir present que l'activitat de tractament de les dades que ha estat objecte d'avaluació pot patir modificacions en alguna de les seves operacions de processament amb el pas del temps. Aquests canvis en relació a la situació inicial de tractaments poden afectar els riscos o les mesures previstes per mitigar-ne els riscos i, per això, cal preveure mecanismes de revisió de les avaluacions realitzades. Es recomana revisar l'anàlisi de riscos realitzat davant qualsevol canvi significatiu en les activitats de tractament que puguin derivar en l'aparició de nous riscos o en la variació dels riscos ja detectats.

Finalment, tot i que no és obligatori, el responsable del tractament pot optar per publicar totalment o parcialment l'AIPD. Això pot generar més confiança en el projecte i serveix al principi de "responsabilitat proactiva" i al de transparència del tractament; òbviament, aquesta publicació no ha de generar riscos per al tractament, de manera que, per exemple, no s'ha de publicar informació relacionada amb la seguretat de les dades.

Publicar l'AIPD resulta d'especial rellevància quan l'interès del tractament pot tenir un cert impacte social, o pot generar un estat d'opinió en les persones de les quals es poden arribar a tractar les dades. Els tractaments responsabilitat de les administracions públiques sovint poden generar aquest interès. En el cas que el tractament avaluat pugui afectar només persones de la mateixa organització, per exemple els empleats, també pot ser convenient consultar-los com a parts afectades. Resulta recomanable portar un registre de les avaluacions d'impacte fetes, que pot ser particular o pot ser una informació a incorporar en el registre d'activitats de tractament de l'article 30 de l'RGPD.

Núm. risc	Mesura a implementar	Recursos	Persona responsable
1	Fer signar i/o actualitzar un acord de confidencialitat amb empreses que puguin tenir un accés accidental a les dades, especialment amb l'empresa Dadà Comunicació. De la mateixa manera, mantenir contracte d'encarregat de tractament amb els proveïdors que tractin dades, com ara Validated ID, S.L.		
2	Millorar la informació que es proporciona perquè sigui conforme a l'art. 13 RGPD i informi correctament sobre la finalitat de la recollida, la base jurídica, el procediment d'exercici dels drets dels interessats, els destinataris i la prestació dels consentiments, sobre els quals cal informar sempre sobre la possibilitat de revocar-los.		
3	Implementar procediments de renovació obligada de contrasenyes, segons els quals totes les contrasenyes hagin de ser modificades anualment. Aplicar mesures de limitació d'intents d'accés fallits en tots els programes utilitzats per al tractament de les dades.		
4	Aplicar mesura de bloqueig per inactivitat al programa de gestió de consentiments i signatura electrònica, atès que aquesta mesura no es troba implementada en tots els suports i dispositius amb què es treballa habitualment. Sí que està implementada en les tauletes per defecte, però no en els ordinadors. Així, per exemple, no es pot controlar que els que treballen des de casa tinguin aquesta mesura implementada.		
5	Assegurar la seguretat mitjançant la correcta realització de procediments d'identificació, d'assignació, de registre d'entrades i sortides en relació a les unitats de memòria que es fan servir habitualment per a la conservació de la còpia de		

	seguretat mensual, i mantenir el procediment d'encriptació.	
6	Proporcionar formació i informació al personal actualitzada sobre protecció de dades, especialment relativa al DPD i al procediment de notificació i comunicació d'una violació de seguretat, però també sobre el deure de confidencialitat i les mesures de seguretat aplicables.	
7	A part de mantenir l'ús del SAI com a solució general, per al cas d'impossibilitat de prestar el servei, caldria preveure procediment alternatiu a través de documentació en paper.	
8	Preveure procediment alternatiu per al cas eventual de no disposar temporalment dels recursos tècnics necessaris, de manera que, en aquests casos, es pugui continuar prestant servei i registrant els consentiments mitjançant l'ús de documentació en paper.	
9	Millorar el procediment pel qual l'aplicació avisa el treballador de l'entitat sobre els consentiments rebutjats dels pacients. Assegurar que tots els treballadors autoritzats coneixen la importància de basar-se en els consentiments efectivament prestats per l'interessat abans d'iniciar qualsevol nou tractament de de les dades.	

Barcelona, a 23 maig de 2019.

Pere Ruiz Espinós

- Soci -

Caterina Bartrons Pou

- Gerent -