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

Informe d'avaluació d'impacte de dades personals per implementació d'una aplicació, en versió aplicació per a terminal smartphone/dispositiu mòbil i en versió web, per a la comunicació entre professionals de l'Entitat i amb els pacients, d'acord amb el Reglament (UE) 2016/679 general de protecció de dades.

Protocol número: C-11.632

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 una aplicació anomenada "Medxat" que es pot utilitzar en la versió web i, prèvia descàrrega, en un smartphone/dispositiu mòbil. La finalitat de l'aplicació és la comunicació entre professionals de l'Entitat, així com la comunicació d'aquests amb els pacients, i la possibilitat de crear grups d'usuaris i compartir arxius, documents i imatges. En aquest sentit, s'ha avaluat de forma específica la implementació de l'aplicació 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'aplicació denominada "Medxat" 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 proporcionen llistes dels casos en què s'exigeix una AIPD.	x	

Implementació d'una nova tecnologia. Segons l'article 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 (6/9)	**66,66%**	

[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*".

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 preveu el tractament de dades sensibles a gran escala.

L'activitat de tractament de l'aplicació, tant en la seva versió web com en la seva versió mòbil per smartphone i tauleta, es troba subjecta a la realització d'avaluació d'impacte, de conformitat amb l'article 35 del RGPD, perquè és un ús innovador de noves tecnologies aplicat a un tractament de dades sensibles a gran escala.

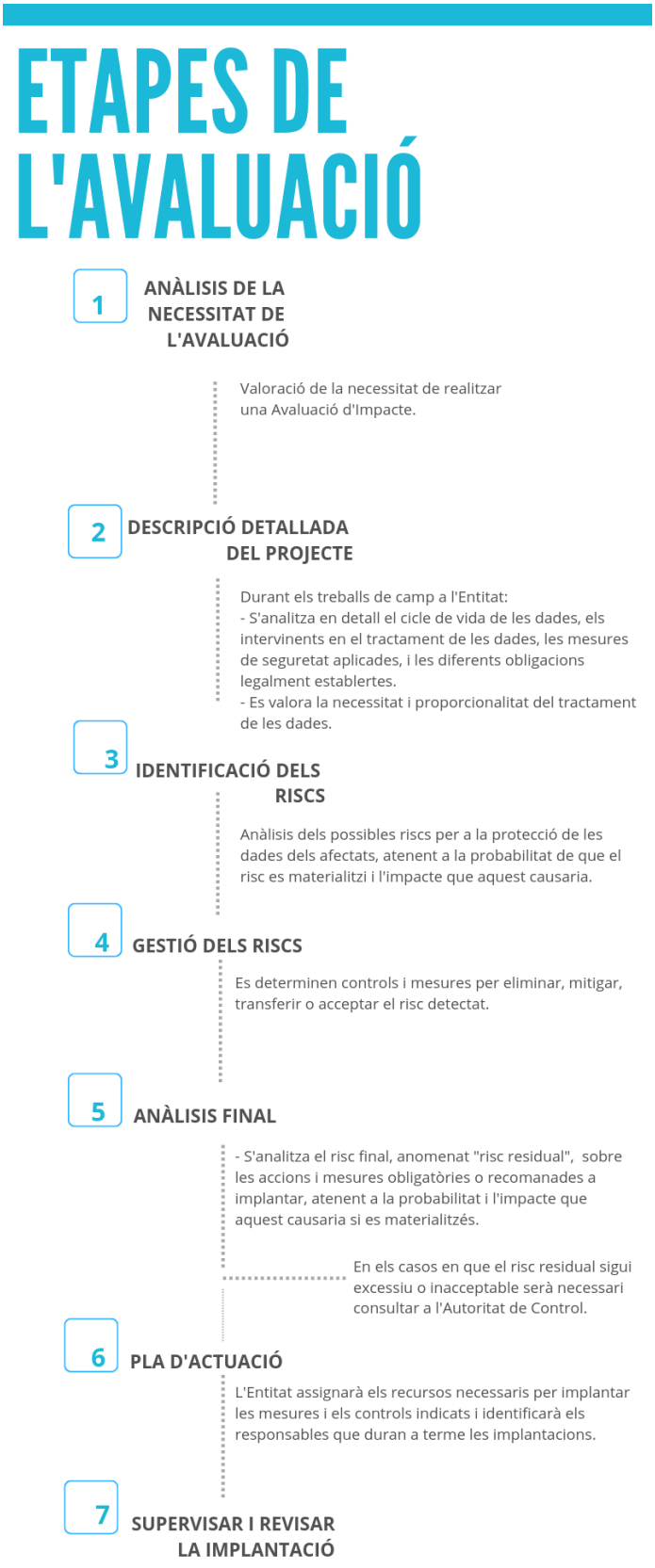
Segons els criteris definits a les Directrius sobre Avaluació d'Impacte en matèria de protecció de dades del Grup de l'article 29 WP 248, el tractament, restringit a la gestió de la informació i els consentiments, presenta un risc de 66,66%. Per tant, l'activitat específica objecte d'avaluació requereix 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:

- Sistema deficient d'identificació i autentificació.
- Falta de recollida de consentiment de l'usuari pacient de l'Entitat.
- No consta correctament proporcionada la informació de l'article 13 del RGPD als diferents interessats.
- L'usuari professional pot escollir el seu nom, càrrec i departament. Tanmateix, la introducció de la seva fotografia no es modera, ni revisa.
- No hi ha previst un sistema de baixa de l'usuari, ni de bloqueig del mateix.
- No es modera la introducció de les fotografies, arxius i documents en els grups.
- Falta de registre d'accessos.
- Descàrrega de fitxers temporals.
- Falta d'acceptació dels usuaris als grups de comunicació i falta de previsió d'usuaris màxims als grups de comunicació.
- No hi ha termini de supressió de les comunicacions.
- Probabilitat que les dades i informacions rellevants que els usuaris introdueixen a l'aplicació no s'introdueixin a la història clínica del pacient.
- No es troba correctament definit el procediment per pèrdua o robatori de l'smartphone amb l'aplicació descarregada.
- Manca de contracte d'encarregat de tractament amb Athenea Solutions & Tech, S.L.

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

- Modificar i adaptar el sistema d'identificació i autentificació.
- Preveure la recollida del consentiment de l'usuari pacient de l'Entitat.

- Proporcionar la informació de l'article 13 del RGPD a través de l'aplicació en la versió navegador web i la versió per al seu ús a smartphone i tauletes.

- Impossibilitat que els usuaris professionals puguin modificar el seu nom, càrrec i departament i es revisi la introducció de la seva fotografia.

- Preveure els sistemes de baixa i bloqueig de l'usuari.

- Moderar la introducció de les fotografies, arxius i documents en els grups.

- Implementar el registre d'accessos.

- Preveure procediments d'eliminació dels fitxers temporals.

- Moderar i limitar els usuaris màxims als grups de comunicació.

- Preveure el termini de supressió de les dades.

- Preveure que les dades i informacions que s'introdueixin passin a la història clínica del pacient.

- Definició del procediment per pèrdua o robatori.

- Signar el contracte d'encàrrec de tractament amb Athenea Solutions & Tech, S.L.

3.4 MESURES QUE AFECTEN ALS ENCARREGATS DE TRACTAMENT

- Signar un contracte d'encàrrec de tractament amb Athenea Solutions & Tech, 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 si implanta les mesures per evitar les amenaces.

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 aplicació per a la comunicació entre els professionals de l'Entitat, així com d'aquests amb els pacients, compartir grups de comunicació i arxius, documents i imatges.

4.2 DESCRIPCIÓ DETALLADA I FUNCIONAL. ELEMENTS RELLEVANTS

	Obtenció de les dades	Classificació	Ús	Cessió / Transferència	Destrucció
Procés	Obtenció dels propis pacients, ja sigui per l'aplicació o directament per part dels professionals de l'entorn informàtic OMI.	No aplica un procés de classificació com a tal.	Comunicació entre els professionals de l'Entitat, així com d'aquests amb els pacients, compartir grups de comunicació i arxius, documents i imatges.	En el seu cas, es fa a través dels propis programes de l'HC3, el SI-SISO i el SISCAT, per complir el contínuum assistencial.	En el seu cas, no consten procediments ni terminis definits de l'eliminació de les comunicacions.
Dades tractades	Dades d'identitat (nom, adreça i DNI) i de contacte dels professionals de l'Entitat i els pacients. Dades de salut i històries clíniques dels pacients.	No aplica un procés de classificació com a tal.	Les dades d'identificació dels professionals de l'Entitat i els pacients serveixen per identificar les parts intervinents. Les dades de salut i històries clíniques dels pacients serveixen per tal que el professional de l'Entitat pugui donar resposta a les peticions comunicatives del pacient.	En el seu cas, es fa a través dels propis programes de l'HC3, el SI-SISO i el SISCAT, per complir el contínuum assistencial.	En el seu cas, no consten procediments ni terminis definits de l'eliminació de les comunicacions.
Intervinents	Professionals i pacients de l'Entitat.	No aplica un procés de classificació com a tal.	Comunicació entre els professionals de l'Entitat, així com d'aquests amb els pacients, compartir grups de	En el seu cas, es fa a través dels propis programes de l'HC3, el SI-SISO i el SISCAT, per complir el	No hi ha actualment un perfil autoritzat específicament a l'eliminació

			comunicació i arxius, documents i imatges.	contínuum assistencial.	de les comunicacions.
Tecnologies utilitzades	Aplicació en la seva versió web i, prèvia descàrrega, en la versió mòbil per ús a smartphone i/o tauleta.	No aplica un procés de classificació com a tal.	Programa OMI, de gestió general de pacients i històries clíniques, i el programa de gestió consentiments i signatura electrònica.	HC3 (història clínica compartida de Catalunya). Plataformes SI-SISO (història clínica compartida a Osona) i SISCAT (proveïdors d'atenció especialitzada)	No s'apliquen programes d'eliminació de les comunicacions.

Interessats	Treballadors i pacients dels centres de salut gestionats per EAP VIC, especialment el CAP El Remei, de Vic.
Responsable del tractament	EAP VIC
Encarregat del tractament	Athenea Solutions & Tech, S.L. és el proveïdor de l'aplicació denominada "Medxat". Jordi Subirana com a proveïdor extern pels serveis d'informàtica.
Terceres parts involucrades	No consten.
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	L'accés dels usuaris a l'aplicació, ja sigui versió web o smartphone i tauleta, es realitza amb l'estàndard OAuth 2.0 del SDK de Firebase. L'accés de l'usuari es basa en correu electrònic i contrasenya de longitud mínima de 6 caràcters, sense requisits de composició. El sistema no preveu el bloqueig per error de la contrasenya. No hi ha previst un bloqueig per inactivitat de la sessió. No hi ha prevista la caducitat de la contrasenya. Pel primer accés, en el cas dels usuaris professionals de l'Entitat, hauran de baixar l'aplicació per a la versió smartphone o utilitzar la versió web. En ambdós casos, l'usuari professional de l'Entitat introdueix el seu correu electrònic professional per donar-se d'alta com a usuari, i el

	sistema li envia un correu electrònic de benvinguda. També ha d'introduir la contrasenya que vulgui amb l'únic requisit que sigui d'una longitud mínima de 6 caràcters. Per al primer accés, en el cas dels usuaris pacients de l'Entitat, l'Entitat procedeix a realitzar l'alta del pacient, sense que aquest prèviament hagi consentit, introduint les dades dels camps obligatoris del seu nom, número de DNI i correu electrònic. En el procés d'alta, l'Entitat pot introduir el número d'història clínica, el sexe i data de naixement del pacient. L'Entitat pot vincular a professionals a l'usuari pacient mitjançat l'opció "Vincular sanitario". Un cop emplenats els camps, l'Entitat clica a la casella "Crear Paciente"; si l'usuari s'ha creat correctament apareix un avís a la part superior dreta assenyalant "OK Paciente creado correctamente". A partir d'aquest moment, l'usuari rep un correu electrònic de benvinguda. L'usuari professional de l'aplicació, ja sigui versió web o smartphone, pot configurar el seu nom, càrrec i departament. L'únic camp que el sistema no permet modificar a l'usuari professional de l'Entitat és el correu electrònic. L'usuari pot introduir una fotografia seva al camp habilitat a tal efecte; no consta la revisió o control de les fotografies per part de l'Entitat. No hi ha previst un procediment de baixa de l'usuari, i tampoc de bloqueig. L'inici de comunicacions entre els usuaris no requereix de cap permís, així com tampoc l'opció de compartir arxius, documents i fotografies. Les comunicacions es realitzen sobre canals de comunicació destinada a la transferència de dades d'Hipertext amb el protocol "*https*". El protocol "*https*" utilitza el xifrat basat en la seguretat de text SSL/TLS. Les dades dels missatges es transmeten i emmagatzemen al servidor encriptades mitjançant el protocol AES ("*Advanced Encryption Standard*"). El sistema permet l'intercanvi d'arxius, documents i fotografies entre usuaris. En el cas de la versió de l'aplicació pel seu ús per smartphone, les fotografies es visualitzen al dispositiu sense necessitat de descàrrega, no obstant, es poden descarregar a la carpeta de l'aplicació instal·lada al smartphone. En el cas de la versió de l'aplicació pel seu ús al navegador, les fotografies es poden descarregar a la carpeta de descàrregues. El sistema permet la creació de grups d'usuaris sense requisits d'acceptació per part dels usuaris, ni restricció dels usuaris màxims. No hi ha previst la realització de la revisió dels accessos. Es guarda l'últim accés de cada usuari i les dades referents als missatges. Quan s'envia un missatge, s'enregistra qui ha enviat el missatge i la data i l'hora d'enviament i recepció al servidor. Quan es rep un missatge, s'enregistra la data i l'hora de recepció i lectura del receptor.

	Inicialment es preveia l'eliminació de les comunicacions als 30 dies, però amb posterioritat no consta temps d'eliminació de les comunicacions, romanent indefinidament emmagatzemades. El sistema preveu que l'usuari professional de l'Entitat pot remetre el contingut d'una comunicació al seu correu electrònic professional. No obstant, no consta cap previsió tècnica, ni obligació formalitzada per l'usuari professional de traslladar la informació a la base de dades de l'historial clínic. En cas de pèrdua de l'smartphone o dispositiu, l'administrador del sistema pot bloquejar l'usuari després que ell mateix hagi notificat la pèrdua. No consta la forma de notificació per part de l'usuari a l'administrador del sistema. No consta la disponibilitat de l'administrador del sistema les 24 hores els 7 dies de la setmana.
Còpies de seguretat	Les còpies de seguretat es realitzen de forma automàtica un cop al dia a les 23 hores. El servidor és un servidor cloud Firestore de Google situat a Frankfurt, Europa, segons informacions del proveïdor Athenea Solutions & Tech, S.L.
Procediment per complir amb el deure d'informació	Segons informacions proporcionades, l'usuari de l'aplicació, bé sigui un usuari treballador o un usuari pacient, ha d'acceptar els textos legals del proveïdor Athenea Solutions & Tech, S.L. i l'Avís legal i política de privacitat de l'Entitat per tal de poder utilitzar l'aplicació. En revisar els textos legals del proveïdor pel que fa a protecció de dades, s'hi indica que el responsable del tractament de les dades dels usuaris és el centre mèdic, sense identificar-lo específicament. Es revisa l'Avís legal i política de privacitat de l'Entitat, però no inclou de forma expressa la informació del tractament objecte de la present Avaluació d'Impacte. Posteriorment l'Entitat informa que substituirà el seu Avís legal i política de privacitat per una Política de Privacitat i Xarxes Socials. Es revisa aquesta Política de Privacitat i Xarxes Socials, que ja inclou de forma expressa el tractament objecte de la present avaluació d'impacte. D'altra banda, en aquest text s'assenyala que el termini de conservació de les converses és de 30 dies, si bé el proveïdor Athenea Solutions & Tech, S.L. informa que no hi ha un termini definit de conservació. El text no inclou la referència al termini de conservació dels arxius, documents i imatges. A data de la present Avaluació d'Impacte no consta a la versió web cap text legal de Protecció de Dades d'EAP Remei Vic. El text legal que consta és el del proveïdor Athenea Solutions & Tech, S.L., però no inclou la Política de Privacitat d'EAP Remei Vic. Pel que fa a la versió del seu ús a smartphone tampoc consta, a data de la present Avaluació d'Impacte, cap text legal de Protecció de Dades d'EAP Remei Vic i el text legal que

	consta és el del proveïdor Athenea Solutions & Tech, S.L., però no la Política de Privacitat d'EAP Remei Vic.
Procediment d'obtenció del consentiment (quan sigui necessari)	No consta cap procediment de recollida de consentiment per part dels usuaris pacients.
Procediment per a l'exercici dels drets per part dels interessats	Segons la Política de Privacitat i xarxes socials que els usuaris acceptaran i es troba pendent d'incorporar, el procediment per a l'exercici dels drets per part dels interessats és dirigir-se per escrit al Delegat de Protecció de Dades a una adreça física o una adreça electrònica. Al lloc web de l'Entitat www.eapvic.org es poden trobar els impresos per exercir els drets. Per a la revocació del consentiment es preveu que es pugui realitzar fent un escrit a l'adreça física o l'adreça electrònica del Delegat de Protecció de Dades.
S'identifiquen les obligacions i mesures de seguretat dels encarregats del tractament al contracte	No consta signat el contracte d'encarregat de tractament amb el proveïdor Athenea Solutions & Tech, S.L. El contracte amb el proveïdor informàtic Jordi Subirana està signat.
Procediment per donar compliment a la notificació d'incidències de seguretat	A l'Entitat 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 relació a l'aplicació objecte de la present avaluació d'impacte hi ha un procediment de comunicació de l'usuari a l'administrador per comunicar la pèrdua del mòbil; no obstant, aquest procediment no es troba definit i no consta la forma de realització de la comunicació. No consta un procediment per notificar altes incidències de seguretat de l'aplicació.
En cas d'existència de transferències internacionals fora de la UE, son adequades?	No consten transferències internacionals de dades.

4.3 OBJECTIUS I FINALITATS DEL TRACTAMENT

4.3.1. BASE DE LA LEGITIMACIÓ

LEGITIMACIÓ	
Legitimació	Respecte a l'usuari professional de l'Entitat: execució d'un contracte; article 61.c) RGPD. Respecte a l'usuari pacient de l'Entitat: el seu consentiment; article 9.2.a RGPD,

Justificació	Respecte a l'usuari professional de l'Entitat la base jurídica que legitima l'ús de l'aplicació és l'execució del contracte laboral del professional amb l'Entitat. Respecte a l'usuari pacient de l'Entitat la base jurídica que legitima l'ús de l'aplicació és el consentiment de l'usuari interessat.

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)	NO	

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 les 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	Sistema deficient d'identificació i autentificació: • Contrasenya d'accés de 6 caràcters sense requisits. • No hi ha previsió de caducitat de la contrasenya. • No hi ha bloqueig per error de la contrasenya. • No hi ha previst bloqueig per inactivitat de la sessió. • No s'ha aconseguit determinar si és obligatori el canvi de contrasenya a la primera connexió.	- Risc de l'atac denominat "força bruta". - Risc de violació de seguretat. - Risc d'accés de persona no autoritzada. - Risc d'ús il·lícit de les dades. - Risc de fuita d'informació confidencial.	3	4	7
2	Falta de recollida de consentiment de l'usuari pacient.	- Incompliment normatiu. - Sancions.	4	4	8

3	No consta correctament proporcionada la informació de l'article 13 del RGPD als diferents interessats.	-	Incompliment normatiu. Sancions.	3	3	6
4	L'usuari professional pot escollir el seu nom, càrrec i departament. Tanmateix, la introducció de la seva fotografia no es modera, ni revisa.	- -	Risc de suplantació d'identitat. Risc d'accés de persona no autoritzada.	3	4	7
5	No hi ha previst un sistema de baixa de l'usuari, ni de bloqueig del mateix.	- - -	Risc de pèrdua d'informació confidencial. Risc de difusió o accés il·lícit per part de tercer. Risc de violació de seguretat.	4	4	8
6	No es modera la introducció de les fotografies, arxius i documents en els grups.	- - -	Risc d'àtacs de virus mitjançant les fotografies, arxius i documents. Risc de violació de seguretat. Risc d'accés il·lícit per part de tercer.	3	3	6
7	Falta de Registre d'Accessos.	-	Impossibilitat de controlar els accessos.	2	2	4
8	Descàrrega de fitxers temporals.	-	Accés per part d'usuari no autoritzat.	2	2	4

9	Falta d'acceptació dels usuaris als grups de comunicació i falta de previsió d'usuaris màxims als grups de comunicació.	-	Risc de difusió de dades personals. - Risc d'accés a dades no autoritzat. - Risc de violació de seguretat.	2	2	4
10	No hi ha termini de supressió de les comunicacions.	-	Risc d'accés a dades no autoritzat. - Risc de violació de seguretat.	2	2	4
11	Probabilitat que les dades i informacions rellevants que els usuaris introdueixen a l'aplicació no s'introdueixin a la història clínica del pacient.	-	Risc d'integritat de les dades. - Risc per a la prestació de l'assistència sanitària.	4	4	8
12	No es troba correctament definit el procediment per pèrdua o robatori del smartphone amb l'aplicació descarregada.	-	Risc de violació de seguretat. - Risc d'accés de persona no autoritzada. - Risc d'ús il·lícit de les dades. - Risc de fuita d'informació confidencial.	4	4	8
13	Manca de contracte d'encarregat de tractament signat amb Athenea Solutions & Tech, S.L.	-	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

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	Modificar i adaptar el sistema d'identificació i autentificació.	1	1	2
2	Preveure la recollida del consentiment de l'usuari pacient.	1	0	1
3	Proporcionar la informació de l'article 13 del RGPD a través de l'aplicació en la versió navegador web i la versió per al seu ús a smartphone i tauletes.	0	1	1
4	Impossibilitat que els usuaris professionals puguin modificar el seu nom, càrrec i departament i es revisi la introducció de la seva fotografia.	0	1	1
5	Preveure els sistemes de baixa i bloqueig de l'usuari.	1	1	2
6	Moderar la introducció de les fotografies, arxius i documents en els grups.	1	1	2
7	Implementar el Registre d'Accessos.	1	1	2
8	Preveure procediments d'eliminació dels fitxers temporals.	1	1	2
9	Moderar i limitar els usuaris màxims als grups de comunicació.	1	1	2
10	Preveure el termini de supressió de les dades.	1	1	2

11	Assegurar-se que tots els usuaris de l'aplicació coneixen l'obligació i necessitat d'introduir les informacions rellevats de l'aplicació a la història clínica.	1	1	2
12	Definició del procediment per pèrdua o robatori.	1	1	2
13	Signar el contracte d'encàrrec de tractament amb Athenea Solutions & Tech, S.L.	0	1	1

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 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, 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	Modificar i adaptar el sistema d'identificació i autentificació.		
2	Preveure la recollida del consentiment de l'usuari pacient.		
3	Proporcionar la informació de l'article 13 del RGPD a través de l'aplicació en la versió navegador web i la versió per al seu ús a smartphone i tauletes.		
4	Impossibilitat que els usuaris professionals puguin modificar el seu nom, càrrec i departament i es revisi la introducció de la seva fotografia.		
5	Preveure els sistemes de baixa i bloqueig de l'usuari.		
6	Moderar la introducció de les fotografies, arxius i documents en els grups.		
7	Implementar el registre d'accessos.		
8	Preveure procediments d'eliminació dels fitxers temporals.		
9	Moderar i limitar els usuaris màxims als grups de comunicació.		
10	Preveure el termini de supressió de les dades.		

11	Assegurar-se que tots els usuaris de l'aplicació coneixen l'obligació i necessitat d'introduir les informacions rellevats de l'aplicació a la història clínica.	
12	Definició del procediment per pèrdua o robatori.	
13	Signar el contracte d'encàrrec de tractament amb Athenea Solutions & Tech, S.L.	

Barcelona, a 23 de maig de 2019.

Pere Ruiz Espinós

- Soci -

Caterina Bartrons Pou

- Gerent -