



Guia d'avaluació dels aspectes derivats de la normativa de protecció de dades en projectes de recerca



**Generalitat
de Catalunya**

Alguns drets reservats

© 2020, Generalitat de Catalunya. Departament de Salut.

Els continguts d'aquesta obra estan subjectes a una llicència de Reconeixement-No Comercial- Sense Obres Derivades 4.0 Internacional.

La llicència es pot consultar a la pàgina web de Creative Commons.

Editen:

Direcció General de Recerca i Innovació en Salut. Direcció General d'Ordenació i Regulació Sanitària. Oficina del DPD - Fundació TIC SALUT i SOCIAL.

1a edició:

Barcelona, juliol de 2020.

2a edició:

Revisió corporativa: desembre de 2025
Oficina de Comunicació.

Número de registre editorial:

82780



ÍNDEX

1.	Objectius del document	P. 4
2.	Introducció	P. 6
3.	Conceptes bàsics de protecció de dades i la seva interpretació en l'àmbit de recerca	P. 8
4.	Aspectes específics de protecció de dades en l'àmbit de la recerca	P. 22
5.	Metodologia per a la revisió dels aspectes de protecció de dades personals per part dels comitès d'ètica de recerca	P. 36

1.

Objectius del document

Han transcorregut cinc anys des de la publicació de la primera versió d'aquesta guia; per aquest motiu, es fa necessària una revisió, en la qual s'actualitzen continguts i s'incorporaran els nous criteris que s'han treballat al Grup de Recerca de l'Oficina del delegat de protecció de dades (d'ara endavant, DPD).

Aquest document és una guia informativa dels aspectes principals que s'han de tenir en compte en matèria de protecció de dades a l'hora d'avaluar projectes de recerca, tant pel membre expert en protecció de dades dels comitès d'ètica de la recerca (d'ara endavant, CER) o els comitès d'ètica de la recerca amb medicaments (d'ara endavant, CERm), com pel personal avaluador. Així mateix, també pretén ser una eina útil per a l'equip investigador i els gestors i gestores de projectes.

A fi de facilitar la tasca d'avaluació, s'inclouen enllaços a diversos documents que fixen els principals criteris interpretatius, i permeten ampliar informació de tots els temes per avaluar.

Aquesta guia disposa d'una primera part de conceptes bàsics de protecció de dades aplicats a l'àmbit de la recerca, una segona part que incorpora aspectes molt concrets de protecció de dades relacionats amb la recerca com l'ús de la IA en recerca, l'ús de mostres biològiques, els assaigs clínics i els estudis retrospectius.

Finalment, també s'incorporen uns materials de tipus pràctic, com una descripció dels elements que ha de contenir un protocol de recerca, els elements de protecció de dades que s'han d'incorporar en un full d'informació i consentiment, i una proposta de metodologia per avaluar els projectes de recerca.

2.

Introducció

La realització d'un projecte de recerca implica el tractament de categories especials de dades, i, per tant, s'han de tenir en compte les previsions que estableix l'article 9 del [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](#) (d'ara endavant, l'RGPD).

Així mateix, cal atènyer-se a la regulació que estableix la [Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals](#) (d'ara endavant, la LOPDGDD), en especial l'apartat 2 de la disposició addicional dissetena, en què es desenvolupen els criteris per al tractament de dades a la recerca.

Adicionalment a la normativa de protecció de dades, és necessari tenir en compte la normativa pròpia de l'àmbit de la recerca. En aquest sentit, és especialment rellevant tenir en compte les normatives reguladores següents de l'ús de mostres, assaigs clínics o estudis observacionals, ja que impacten directament en el règim de protecció de dades aplicable a aquest tipus de projectes. Així doncs, trobem com a normativa de referència:

- Llei 14/2007, de recerca biomèdica.
- Reial decret (RD) 1716/2011 que aprova el reglament de desenvolupament de la LIB.
- Reglament (UE) 536/2014, sobre els assaigs clínics de medicaments d'ús humà (RAC).
- Text refós de la Llei de garantia i ús racional dels medicaments i productes sanitaris, aprovat pel Reial decret legislatiu 1/2015, de 24 de juliol.
- Reial decret 1090/2015, de 4 de desembre, pel qual es regulen els assajos clínics amb medicaments, els comitès d'ètica de la recerca amb medicaments i el Registre espanyol d'estudis clínics.
- Reial decret 957/2020, de 3 de novembre, pel qual es regulen els estudis observacionals amb medicaments d'ús humà.
- Reial decret 192/2023, de 21 de març, pel qual es regulen els productes sanitaris.

Adicionalment, i amb el paquet normatiu aprovat en el marc de la Unió Europea dins l'estratègia de dades, destaquem dues normes que desplegaran els seus efectes al llarg dels propers anys: per una banda, trobem el **Reglament (UE) 2024/1689 del Parlament Europeu i del Consell, de 13 de juny de 2024, pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial**; i per l'altra, el **Reglament (UE) 2025/327 del Parlament Europeu i del Consell, d'11 de febrer del 2025, relatiu a l'Espai Europeu de Dades de Salut**.

Els criteris interpretatius de la normativa de protecció de dades en l'àmbit de la recerca s'han anat establint a través de diversos documents, tant d'àmbit estatal com europeu, entre els quals cal destacar els següents:

- EC - [Document Guidelines on FAIR Data Management in Horizon 2020](#), de la Comissió Europea de 26 de juliol de 2016.
- EC - [Document Ethics and data protection](#), de la Comissió Europea de 4 de febrer de 2019.
- EC - [Document Guidance How to complete your ethics self-assessment](#), de la Comissió Europea de 14 de novembre de 2018.
- APDCAT - [Dictamen 15/2019 en relació amb la consulta d'un centre sanitari sobre la necessitat del consentiment en el cas de la utilització de dades de salut pseudonimitzades en investigació biomèdica](#) de 14 de maig de 2019.
- APDCAT - [Dictamen 18/2019 en relació amb la consulta d'una associació de l'àmbit sanitari sobre diferents aspectes relacionats amb l'apartat 2 de la disposició addicional dissetena de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals](#), de 14 de maig de 2019.
- CEPD - [Dictamen 3/2019, sobre preguntes i respostes sobre la interrelació entre la regulació d'assajos clínics \(RAC\) i el Reglament general de protecció de dades \(RGPD\) \[article 70.1.b\)\]](#), adoptat el 23 de gener de 2019.
- CEPD - [Directrius 03/2020 sobre el processament de dades de salut amb finalitats de recerca científica en el context del brot de COVID-19](#), adoptades el 21 d'abril de 2020.
- APDCAT - [Dictamen 14/2020 en relació amb la consulta d'un hospital sobre l'accés a dades dels seus professionals en el marc d'un estudi científic desenvolupat en un altre hospital](#), de 27 d'abril de 2020.
- BIOÈTICA - [Informe del Comité de Bioética de España sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de covid-19](#), de 28 de abril de 2020.
- AEPD - [Informe jurídico AEPD relativo a la monitorización en ensayos clínicos](#).
- CEPD - [Documento del CEPD relativo a la respuesta a la solicitud de la Comisión Europea de aclaraciones sobre la aplicación coherente de l'RGPD, centrada en la investigación sanitaria](#).
- CEPD - Dictamen conjunto 3/2022 del CEPD y el SEPD sobre la propuesta de Reglamento del Espacio Europeo de Datos Sanitarios (EEDS).
- CEPD - Dictamen 28/2024 sobre determinats aspectes de protecció de dades relacionades amb el tractament de dades personals en el context dels models d'IA.

3.

Conceptes bàsics de protecció de dades i la seva interpretació en l'àmbit de recerca

3.1 Tipus de dades i aplicació de la normativa de protecció de dades

La normativa de protecció de dades s'aplica «al tractament totalment o parcialment automatitzat de dades personals, així com al tractament no automatitzat de dades personals contingudes en un fitxer o destinades a incloure-s'hi».

Per tant, el primer que hem de veure és què entenem per dada personal. En aquest sentit, podem categoritzar les dades com a dada identificada, anònima, pseudonimitzada i sintètica.

L'RGPD s'aplica a les dades personals, entenent com a tal la informació relativa a una persona física identificada o identificable.

Una persona física identificable és aquella que pot ser identificada, directament o indirectament, en particular mitjançant un identificador, com ara un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social de la persona física.

Exemples: nom, adreça, número d'identificació, pseudònim, ocupació, adreça electrònica, CV, dades de localització, adreça del protocol d'internet (IP), identificador de galetes, número de telèfon, imatge o CIP.

Les dades anònimes no queden sotmeses a la normativa de protecció de dades. En cas que el protocol indiqui que les dades estan anonimitzades, s'ha de descriure el sistema d'anonimització. En aquest sentit, l'Agència Espanyola de Protecció de Dades (d'ara endavant, AEPD) va emetre un document relatiu a l'anonimització en el qual podem trobar més informació: [Orientaciones y garantías en los procedimientos de anonimización de datos personales](#).

Cal distingir aquest concepte de les dades pseudonimitzades entenent que unes dades han estat pseudonimitzades quan ja no es poden identificar sense necessitat de disposar d'informació addicional, que estigui per separat, i que s'hagin aplicat una sèrie de mesures tècniques i organitzatives enfocades a evitar la reidentificació.

En el marc de la recerca, quan parlem de dades pseudonimitzades, cal que hi hagi una separació tècnica i funcional entre l'equip investigador i els encarregats de realitzar la pseudonimització i conservar la informació que permeti la reidentificació, si fos necessària.

En cas que no hi hagi aquesta separació tècnica i funcional, ens trobaríem davant del que comunament es coneix en l'àmbit de recerca com a codificació. En els dos casos, pseudonimització i codificació, s'aplica la normativa de protecció de dades. Podem trobar més informació en relació amb la pseudonimització a l'informe *Introducción al hash como técnica de seudonimización de datos personales* de l'AEPD i al document [Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions](#) d'ENISA.

Finalment, parlem d'una última categoria de dades, les dades sintètiques, que són dades artificials generades a partir de dades reals. Són dades que conserven els atributs de les dades reals, però no són dades identificables. amb la consulta d'un hospital sobre l'accés a dades dels seus professionals en el marc d'un estudi científic desenvolupat en un altre hospital, de 27 d'abril de 2020.

Per tant, quan parlem de tractament de dades personals, en el marc de la normativa de protecció de dades estarem pensant en dades pseudonimitzades o identificades.

L'altre element important de la definició és què considerem tractament. Entenem com a tal «qualsevol operació (o conjunt d'operacions) realitzada a les dades personals, de forma manual o automàtica».

Exemples: accés/consulta d'una base de dades que conté dades personals, gestió de la base de dades, publicar/posar una foto d'una persona en un lloc web, emmagatzemar adreces IP o adreces MAC, enregistrament de vídeo (CCTV), crear una llista de correu o una llista de participants.

El concepte de tractament de dades personals inclou qualsevol acció que utilitzi dades amb finalitats de recerca (fins i tot la revisió de registres a l'efecte d'identificar els participants en un projecte o l'accés a dades per anonimitzar-les). Les dades personals poden procedir de qualsevol tipus d'activitat investigadora (recerca en l'àmbit de les TIC, genètica, recollida de mostres, emmagatzematge de teixits), registres personals (educació, finances, penal, etc.), informació sobre l'estil de vida i la salut, històries familiars, característiques físiques, sexe i ètnia, informació sobre el seguiment de la localització i el domicili, etc.

Cal recordar que la normativa de protecció de dades, de conformitat amb el que estableix el considerant 27 de l'RGPD, no s'aplica a les dades de difunts. Tot i això, quan vulguem fer servir les dades de difunts per a un projecte de recerca, hem de tenir en compte que, si aquestes dades s'obtenen de la història clínica, s'han de considerar les previsions de la Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica. En aquesta norma es preveu que un dels usos de la història clínica (d'ara endavant, HC) és la recerca, i malgrat que no s'hi fa cap previsió específica, podem entendre que podem fer servir dades de difunts si no hi consta una oposició i el tractament de les dades es porta a terme de forma codificada; és a dir, mantenint separades les dades identificatives de les dades clíniques assistencials.

3.2 Principis de protecció de dades

L'article 5 de l'RGPD estableix els principis aplicables a la protecció de dades. Aquests principis són els que guien l'aplicació de la normativa de protecció de dades; per tant, a l'hora d'interpretar la normativa els hem de tenir molt presents. A continuació, veurem quins són els principis que impacten de forma més directa en l'àmbit de la recerca.

3.2.1 Principi de minimització de les dades

El tractament de les dades ha de ser **lícit, just i transparent**.

Només s'han d'incloure les dades que siguin **necessàries i proporcionades** per assolir la tasca o finalitat específica per a la qual van ser recollides (article 5.1 de l'RGPD).

Així, **només s'han de recollir les dades que siguin necessàries per assolir els objectius de la recerca**, per tant, el seu tractament ha de tenir un propòsit específic rellevant i limitat als objectius i a la metodologia del projecte.

La minimització de dades s'aplica no només a la quantitat de dades personals recollides, sinó també a la forma en què es podran accedir, processar i compartir, els motius pels quals s'utilitzen, així com el període de conservació.

Si no es pot identificar del tot el propòsit del tractament de dades en el moment de la recollida de dades o és necessari mantenir les dades més enllà de la durada del projecte, s'ha d'explicar i justificar.

Per exemple, en un projecte de recerca, si tenim prou recollint l'edat, no hem de demanar la data de naixement exacta.

3.2.2 Privacitat des del disseny i per defecte

L'article 25 de l'RGPD introdueix els conceptes de privacitat en el disseny i privacitat per defecte. La interpretació d'aquest concepte ha estat desenvolupada pel Comitè Europeu de Protecció de Dades (d'ara endavant, CEPD) a través de les [Directrius 4/2019 relatives a l'article 25: protecció de dades des del disseny i per defecte](#).

● Privacitat des del disseny

Això implica que el responsable ha d'aplicar, tant en el moment de determinar els mitjans de tractament com en el moment de la seva execució, les mesures tècniques i organitzatives adequades concebudes per aplicar de manera efectiva els principis de protecció de dades i integrar en el tractament les garanties necessàries per complir els requeriments del Reglament.

En aquest sentit, la Comissió Europea ha acordat que s'han d'establir mesures tècniques i organitzatives a les primeres fases del disseny de les operacions del tractament, de manera que es garanteixi la intimitat i els principis de protecció de dades des del primer moment («protecció de dades des del disseny»). L'ús de tècniques de pseudonimització i xifratge són exemples de privacitat des del disseny.

L'AEPD disposa de la [Guia de Privacitat des del Disseny](#), en la qual es detallen els principis que cal tenir en compte.

● Privacitat per defecte

Així mateix, el responsable ha d'aplicar les mesures tècniques i organitzatives adequades per garantir que, per defecte, només es tracten les dades personals necessàries per a cada finalitat específica del tractament. Aquesta obligació s'aplica a la quantitat de dades personals recollides, a l'abast del tractament, al termini de conservació i a l'accessibilitat de les dades.

En aquest sentit, la Comissió Europea ha establert que s'ha de garantir que les dades personals es tracten amb el màxim nivell de protecció de la intimitat (per exemple, només les dades necessàries, un termini de conservació curt i accessibilitat limitada), de manera que per defecte les dades personals no siguin accessibles a un nombre indefinit de persones («protecció de dades per defecte»). La principal manifestació d'aquest principi en els projectes de recerca seria recollir per defecte el mínim de dades possibles per dur a terme el projecte.

És especialment important garantir aquests principis en els projectes de recerca relacionats amb la creació de solucions tecnològiques. En aquest sentit, l'Autoritat Noruega de Protecció de Dades va elaborar el document **Software development with Data Protection by Design and by Default**, en què s'estableixen els criteris que s'han de tenir en compte des del punt de vista de la privacitat des del disseny i per defecte en el desenvolupament de solucions de programari.

3.2.3 Principi de transparència

L'article 5 de l'RGPD introdueix el principi de transparència, que significa que les dades personals es processen de manera justa i transparent en relació amb la persona afectada. Aquest principi està relacionat amb l'obligació d'informació, d'acord amb l'article 13 o 14 de l'RGPD.

Com a criteri general, s'ha d'informar individualment cada persona afectada sobre l'existència del tractament de dades amb finalitats de recerca, incloent-hi tots els punts de l'article 13 i 14 de l'RGPD.

El full d'informació del participant en el projecte de recerca ha de permetre informar adequadament del tractament de les dades personals del participant en l'assaig, ha de contenir la informació mínima que estableix l'article 13 de l'RGPD, a més d'una altra informació relativa al tractament d'aquestes dades, que ha d'incloure:

- La identitat del responsable o corresponsables del tractament de les dades i davant de qui i com poden exercir els vostres drets.
- La identificació de la forma de contacte amb el delegat de protecció de dades.
- La descripció de les finalitats del tractament de les dades, i comunicacions previstes, incloent-hi les transferències internacionals de dades.
- El tipus d'informació que es recull i el termini durant el qual es conserven les dades.
- Les mesures de seguretat per protegir la privacitat i els riscos per a la confidencialitat.
- El dret a conèixer perquè s'utilitzen les vostres dades, qui les té, a qui les pot cedir, a sol·licitar al responsable la cancel·lació de les dades i el dret a la rectificació de les dades quan siguin inexactes o estiguin incompletes.
- El dret a retirar el consentiment en qualsevol moment i la informació identificable de la base de dades de salut, així com el dret a sol·licitar i rebre informació sobre les vostres dades i el seu ús.
- El dret a presentar una reclamació davant l'autoritat competent.
- Una breu descripció de les mesures de seguretat per protegir la privacitat i els riscos per a la confidencialitat.

De vegades, els investigadors tracten dades de salut que no han obtingut directament de la persona titular de les dades, sinó que s'han obtingut de registres de pacients. D'acord amb l'article 89 de l'RGPD, en el cas de l'ús secundari de dades personals en l'àmbit de la recerca, s'ha de lliurar la informació a l'interessat en un termini raonable abans de la implementació del nou projecte de recerca.

Aquest deure d'informació només es pot exceptuar quan concorrin les situacions que indica l'article 14.5 de l'RGPD. Una d'aquestes situacions, per exemple, es pot donar quan es requereixen esforços desproporcionats, com seria si disposem d'un gran nombre d'informació sense dades de contacte, però els responsables han de prendre les mesures que garanteixin els drets dels titulars de les dades.

3.2.4 Principi de limitació de la finalitat

Les dades s'han de recollir amb finalitats determinades, explícites i legítimes i, posteriorment, no s'han de tractar de manera incompatible amb aquestes finalitats. D'acord amb l'apartat 1 de l'article 89, el tractament posterior de les dades personals amb finalitats d'arxiu en interès públic, amb finalitats de recerca científica i històrica o amb finalitats estadístiques, no es considera incompatible amb les finalitats inicials (limitació de la finalitat). Aquest principi és important, ja que introdueix el concepte d'ús secundari de les dades. En aquest sentit, hem de distingir l'ús primari de les dades de l'ús secundari.

- **Ús primari de les dades:** quan les dades són directament recollides per ser utilitzades per a una finalitat determinada. Per exemple, en l'àmbit de l'assistència, les dades es poden recollir d'acord amb l'interès públic per motius assistencials o, en l'àmbit de la recerca, es poden recollir dades directament dels participants en un estudi científic amb el seu consentiment.
- **Ús secundari de les dades:** quan les dades es fan servir amb una finalitat diferent per a la qual havien estat recollides inicialment. Per exemple, dades que inicialment es van recollir amb finalitats assistencials posteriorment es reutilitzen en un estudi observacional retrospectiu.

Quan parlem de les bases legitimadores en el proper apartat, tornarem a tractar els conceptes d'ús primari i secundari.

3.3 Bases legitimadores i supòsits de tractament de dades en la recerca

Per utilitzar categories especials de dades, com les dades de salut amb finalitats de recerca, hem de fer servir alguna de les bases legitimadores de l'article 6 de l'RGPD, així com aixecar la prohibició de tractament d'aquesta categoria especial de dades que estableix l'article 9.1 de l'RGPD, mitjançant algun dels supòsits de l'article 9.2 de l'RGPD, i en relació amb l'article 89 de l'RGPD. L'ús d'aquestes bases legitimadores es concreta en diversos supòsits que permeten l'ús de dades en la recerca i que es desenvolupen mitjançant la disposició addicional dissetena de la LOPDGDD.

Per interpretar aquest conjunt normatiu, s'ha de tenir en compte també el que estableixen els considerants 26, 28, 33, 34, 52, 53, 54 i 83. Així mateix, hem de tenir en compte diversos pronunciaments de les autoritats nacionals i europees en matèria de protecció de dades que han anat interpretant i concretant l'abast d'aquestes disposicions.

Aquests pronunciaments són:

- APDCAT - [Dictamen 15/2019 en relació amb la consulta d 'un centre sanitari sobre la necessitat del consentiment en el cas de la utilització de dades de salut pseudonimitzades en investigació biomèdica de 14 de maig de 2019.](#)
- APDCAT - [Dictamen 18/2019 en relació amb la consulta d 'una associació de l'àmbit sanitari sobre diferents aspectes relacionats amb l'apartat 2 de la disposició addicional dissetena de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, de 14 de maig de 2019.](#)
- CEPD - [Dictamen 3/2019, sobre preguntes i respostes sobre la interrelació entre la regulació d'assajos clínics \(RAC\) i el Reglament general de protecció de dades \(RGPD\) \[article 70.1.b\)\], adoptat el 23 de gener de 2019.](#)
- CEPD - [Directrius 03/2020 sobre el processament de dades de salut amb finalitats de recerca científica en el context del brot de COVID-19, adoptades el 21 d'abril de 2020.](#)
- APDCAT - [Dictamen 14/2020 en relació amb la consulta d 'un hospital sobre l'accés a dades dels seus professionals en el marc d'un estudi científic desenvolupat en un altre hospital, de 27 d'abril de 2020.](#)
- BIOÈTICA - Informe del Comitè de Bioètica d'Espanya sobre els requisits ètics i legals en recerca amb dades de salut de 8 d'abril de 2020.

Com a punt de partida, és rellevant indicar que la mateixa LOPDGDD, a través de la disposició final novena, ha modificat la Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica, que té la consideració de llei bàsica, i que regula, entre d'altres, l'accés a la història clínica i les finalitats amb les quals es pot dur a terme, incloent-hi la recerca. La modificació suposa una remissió a la disposició addicional dissetena de la LOPDGDD, on es regula el règim de l'ús de dades de salut. Per tant, en la interpretació de tot aquest conjunt normatiu, adquireix una rellevància especial la disposició addicional dissetena de la LOPDGDD, que permet inferir que els supòsits que permeten tractar dades de salut amb finalitats de recerca són molt amplis.

A fi d'exposar de la manera més entenedora possible en quins casos podem tractar dades amb finalitats de recerca, farem una explicació sistematitzada dels supòsits amb les bases legitimadores de l'article 6, els supòsits que permeten aixecar la prohibició de l'article 9 i les previsions de la disposició addicional dissetena de la LOPDGDD.

>> Marc normatiu en matèria de salut [art. 6.1.c.), d), e) i f) + 9.2.g), h), i) i j)]

En primer lloc, i a través de l'apartat primer de la disposició addicional dissetena, s'estableixen una sèrie de supòsits en què els tractaments de dades de salut per a finalitats de recerca, que recullen diverses normes estatals, poden trobar cobertura en diferents supòsits de l'RGPD (art. 9.2.g), h), i) i j) de l'RGPD), que aixequen la prohibició de tractar dades de categories especials, entre d'altres, les dades de salut, i n'habiliten el tractament. Aquest és la llista de normes que enumera l'apartat 1 de la disposició addicional dissetena:

- a) La Llei 14/1986, de 25 d'abril, general de sanitat.
- b) La Llei 31/1995, de 8 de novembre, de prevenció de riscos laborals.
- c) La Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica.
- d) La Llei 16/2003, de 28 de maig, de cohesió i qualitat del Sistema Nacional de Salut.
- e) La Llei 44/2003, de 21 de novembre, d'ordenació de les professions sanitàries.
- f) La Llei 14/2007, de 3 de juliol, de recerca biomèdica.
- g) La Llei 33/2011, de 4 d'octubre, general de salut pública.
- h) La Llei 20/2015, de 14 de juliol, d'ordenació, supervisió i solvència de les entitats asseguradores i reasseguradores.
- i) El text refós de la Llei de garanties i ús racional dels medicaments i productes sanitaris, aprovat pel Reial decret legislatiu 1/2015, de 24 de juliol.
- j) El text refós de la Llei general de drets de les persones amb discapacitat i de la seva inclusió social, aprovat pel Reial decret legislatiu 1/2013, de 29 de novembre.

Per tant, quan ens trobem en l'àmbit d'aquestes normes, hem d'analitzar si el text de la norma ens habilita prou per dur a terme el tractament de dades amb finalitats de recerca.

>> Consentiment [art. 6.1.a) + 9.2.a) de l'RGPD]

Aquest primer supòsit permet el tractament de dades de categories especials, com les de salut, basant-nos en l'existència del consentiment. Aquest consentiment ha de ser explícit i lliure. Només es pot utilitzar per aquesta via quan no hi hagi un desequilibri entre les parts.

En aquest sentit, el CEPD ha establert que, en determinats supòsits en el marc dels assaigs clínics, es pot produir aquest desequilibri entre les parts i, per tant, serà necessari recórrer a una altra base legitimadora, que s'haurà de determinar segons el cas concret. Vegeu [Dictamen 3/2019, sobre preguntes i respostes sobre la interrelació entre la regulació d'assaigs clínics \(RAC\) i el Reglament general de protecció de dades \(RGPD\) \[article 70.1.b\)\]](#).

Aquest consentiment es pot obtenir per tractar dades per a un projecte de recerca concret, o d'acord amb el que estableix la lletra a) de l'apartat 2 de la disposició addicional dissetena, es pot obtenir per tractar dades amb finalitats que abastin «categories relacionades amb àrees generals vinculades a una especialitat mèdica o investigadora». Aquesta previsió ens obre la porta a demanar dades per ser utilitzades en diversos projectes de recerca.

Així mateix, també haurem de garantir el compliment del que estableix la lletra f) de l'apartat 2 de la disposició addicional dissetena.

>> Ús amb finalitats de recerca en salut pública [art. 6.1.e) + 9.2.j) de l'RGPD]

La lletra b) de l'apartat 2 de la disposició addicional dissetena estableix la possibilitat de tractar dades de categories especials sense el consentiment dels afectats, sempre que es compleixin dos requisits. En primer lloc, que el tractament es dugui a terme per una autoritat sanitària o institució pública competent en vigilància de salut pública i, en segon lloc, que es donin unes circumstàncies d'excepcional rellevància i gravetat per a la salut pública.

- Per analitzar aquest supòsit, cal que tinguem en compte els criteris que indiquen les [Directrius 03/2020 sobre el processament de dades de salut amb finalitats de recerca científica en el context del brot de COVID-19](#) i el [Dictamen 14/2020 en relació amb la consulta d'un hospital sobre l'accés a dades dels seus professionals en el marc d'un estudi científic desenvolupat en un altre hospital, de 27 d'abril de 2020](#).

Així mateix, també hem de garantir el compliment del que estableix la lletra f) de l'apartat 2 de la disposició addicional dissetena.

>> Reutilització de dades [art. 6.1.e) + 9.2.j) + 89 de l'RGPD]

La reutilització de dades es regula a la lletra c) de l'apartat 2 de la disposició addicional dissetena i a la disposició transitòria sisena de la LOPDGDD (amb relació a les dades recollides abans de l'entrada en vigor de la LOPDGDD). Aquesta legitimació es basa amb el que disposa l'article 9.2.j), en relació amb l'article 89 de l'RGPD, i permet utilitzar les dades obtingudes amb un consentiment inicial per a un estudi de recerca, per a nous projectes d'àrees de recerca relacionades amb el projecte inicial. Seria un supòsit d'ús secundari de dades.

En aquest sentit, podem veure el document [*Informe del Comité de Bioética de España sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de covid-19*](#), on es reflexiona sobre l'ús secundari de dades per a la recerca.

Per poder basar-se en aquest supòsit, cal donar compliment al deure d'informació del titular de les dades (article 13 de l'RGPD) i disposar de l'informe favorable corresponent del CERm.

Així mateix, també hem de garantir el compliment del que estableix la lletra f) de l'apartat 2 de la disposició addicional dissetena.

>> Ús de dades en la recerca amb aplicació de les garanties que disposa la lletra d) de l'apartat 2 de la disposició addicional dissetena [art. 6.e) i f) + 9.2.j) + art. 89 de l'RGPD + lletra d) de l'apartat 2 de la disposició addicional dissetena]

Aquest supòsit ens permet tractar dades que inicialment es van recollir amb una finalitat assistencial per motius de recerca aplicant un seguiment de garanties com la pseudonimització. Es tracta d'un ús secundari de dades.

En primer lloc, s'ha de fer referència al fet que el concepte de pseudonimització vol dir «el tractament de dades personals de manera que ja no es puguin atribuir a una persona interessada sense utilitzar informació addicional, sempre que aquesta informació consti per separat i estigui subjecta a mesures tècniques i organitzatives destinades a garantir que les dades personals no s'atribueixen a una persona física identificada o identificable» (article 4.5 de l'RGPD).

La pseudonimització a l'RGPD es configura com una mesura tècnica, i s'ha de distingir de l'anonimització, ja que, a diferència d'aquesta, a les dades pseudonimitzades, els és plenament **aplicable la normativa de protecció de dades [article 6.4.e), 25.1 i 32.1.a) del RGPD, entre d'altres]**.

L'habilitació en la qual es basa la lletra d) de l'apartat 2 de la disposició addicional dissetena es fonamenta en l'article 9.2.j), en relació amb l'article 89.1, els dos de l'RGPD, sobre quan és necessari el tractament per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics del responsable del tractament (article 6.1.e) de l'RGPD), o també si és necessari per a la satisfacció d'interessos legítims del responsable o d'un tercer (article 6.1.f) de l'RGPD).

És a dir, podem fer servir dades pseudonimitzades per a finalitats de recerca, d'acord amb el que estableix la lletra d) de l'apartat 2 de la disposició addicional dissetena, per garantir:

- Una separació tècnica i funcional entre l'equip investigador i els que duguin a terme la pseudonimització i conservin la informació que possibiliti la reidentificació.
- Que les dades pseudonimitzades únicament siguin accessibles per a l'equip investigador quan:
 - i) Hi hagi un compromís exprés de confidencialitat i de no dur a terme cap activitat de reidentificació.
 - ii) S'adoptin mesures de seguretat específiques per evitar la reidentificació i l'accés de tercers no autoritzats.

Es pot procedir a la reidentificació de les dades en el seu origen quan, amb motiu d'una recerca que utilitzi dades pseudonimitzades, s'aprecii que hi ha un perill real i concret per a la seguretat o la salut d'una persona o un grup de persones, o una amenaça greu per als seus drets, o quan sigui necessària per garantir una assistència sanitària adequada.

No obstant això, en els darrers temps, i davant la dificultat d'alguns centres, han sorgit noves interpretacions respecte a aquesta necessitat de separació entre equip tècnic i funcional, com el que es va dur a terme al [Butlletí núm. 6 2024 de l'Associació Nacional de Comitès d'Ètica de la Investigació \(ANCEI\)](#). En aquest document es proposa una via interpretativa basada en el principi de limitació de la finalitat i els usos compatibles en el tractament de les dades sanitàries amb finalitats de recerca que estableix l'article 5.1.b) de l'RGPD.

3.4 Rols

D'acord amb la normativa de protecció de dades, les entitats que tracten dades personals poden assumir un d'aquests tres rols:

- **Responsable del tractament:** és qui determina la finalitat del tractament i, per tant, té la responsabilitat principal de garantir el compliment de la normativa. El responsable del tractament és el centre que fa la recerca o el promotor.
- **Encarregat de tractament:** és qui tracta les dades en nom del responsable i ha de seguir les seves instruccions; a més, està vinculat a les finalitats i als elements de tractament que el responsable hagi inclòs.
- **Corresponsables del tractament:** els corresponsables determinen les finalitats i els elements essencials del tractament de manera conjunta.

Per exemple, en un assaig clínic, el promotor i el centre sanitari es constitueixen com a responsables del tractament independents o com a corresponsables segons com es planteja l'estudi. Així, si determinen les finalitats del projecte de manera conjunta, estariem parlant de corresponsables.

Les entitats que participin en un projecte de recerca sempre han d'assumir un d'aquests tres rols. És bàsic determinar el rol en què actua una entitat per saber quines obligacions li corresponen i quines responsabilitats té.

En l'àmbit de la recerca, **normalment el responsable del tractament de les dades dels pacients és l'hospital o el centre assistencial**. Els professionals assistencials del centre que estan implicats en el diagnòstic o el tractament del malalt han de tenir accés a la història clínica. Cada centre ha d'establir el mecanisme que faci possible que, mentre es presta assistència a un pacient concret, els professionals que l'atenen puguin tenir accés en tot moment a la història clínica corresponent.

Aquestes dades, a més de l'ús assistencial, es poden fer servir amb finalitats de recerca per part del responsable del tractament; és a dir, el mateix hospital o centre assistencial, i per això es pot basar en qualsevol de les bases legitimadores que estableixen els articles 6 i 9 de l'RGPD. En el context de la recerca, les més habituals són l'interès públic en l'àmbit de la recerca o el consentiment dels titulars de les dades.

Per altra banda, pel que fa al **centre de recerca**, s'ha de verificar a través dels seus estatuts quin és l'abast de les seves atribucions, que poden anar des de la gestió i l'impuls de la recerca fins a la possibilitat de fer recerca.

Si el centre de recerca està habilitat per dur a terme recerca, es pot constituir com a responsable del tractament en projectes de recerca, sempre que disposi de base legitimadora suficient per accedir a les dades. En aquest sentit, cal remarcar que, en cas de voler accedir a dades de la història clínica del centre assistencial o hospital, s'haurà de legitimar la comunicació de les dades que li permeti actuar com a responsable del tractament.

En la relació entre el centre hospitalari i el centre de recerca, des del punt de vista de la protecció de dades, es poden donar diversos supòsits:

- a) Quan el centre de recerca actua simplement com a gestor de la recerca, si té accés a les dades, es constitueix com a encarregat de tractament.
- b) De vegades, però, el centre de recerca també es pot constituir com a responsable del tractament, sempre que els seus estatuts li atribueixin aquestes funcions. En aquest cas, però caldrà trobar una base legitimadora, com ara el consentiment, que li permeti constituir-se com a responsable del tractament d'unes dades de les quals no és el responsable inicial, com són les dades dels pacients de l'hospital.

En aquest sentit, el consentiment per participar en el projecte de recerca ha de preveure expressament la condició de responsables o corresponsables, tant del centre hospitalari com del centre de recerca, per fer un símil amb els assaigs clínics, en què el centre hospitalari i el promotor es constitueixen com a responsables o corresponsables del tractament.

Per exemple, en un estudi observacional que opta a una ajuda europea sol·licitada per la fundació que gestiona la recerca, tant el centre hospitalari com el de recerca es constitueixen com a responsables del tractament. En aquest cas, cal tenir en compte que tots dos tinguin una base legitimadora per al tractament de les dades, p. ex., el consentiment.

c) Finalment, hi ha supòsits en què les dades no provenen de la història clínica del centre, i el centre de recerca és l'únic responsable del tractament. Per exemple, els estudis amb voluntaris sans reclutats directament pel centre de recerca o estudis amb mostres d'un biobanc, sense que s'utilitzi informació addicional de la història clínica.

Cal recordar que l'accés a qualsevol informació relativa al pacient ha de ser estrictament professional. Qualsevol altre accés i/o comunicació de dades dels pacients està totalment prohibit i constitueix un accés indegut, el qual pot ser sancionat laboralment, administrativament i, fins i tot, penalment.

3.5 Relacions amb tercers, comunicacions i transferències internacionals

Un tercer, en l'àmbit de la recerca, l'hem d'entendre com aquella persona o entitat que no és ni el pacient ni el metge responsable i que obté les dades de salut per a l'estudi.

En el context d'un projecte de recerca, l'enviament de dades de salut al promotor (sigui comercial o acadèmic), o a un registre ubicat fora del servidor del centre en què estan allotjades, es considera una comunicació de dades a tercers, encara que estiguin codificades o pseudonimitzades, ja que en ambdós casos les dades (la informació) són identificables, amb més o menys dificultat.

La comunicació de dades és un tractament i, per tant, cal que disposi d'una base legítima, sigui el consentiment del titular o una de les altres que disposa l'article 6 de l'RGPD, i concorri en algun dels supòsits de l'article 9 de l'RGDP que permetin aixecar la prohibició de tractament de les categories especials de dades.

En relació amb les transferències internacionals de dades, s'entén com a tal l'enviament de dades fora de la zona econòmica europea (països de la UE + Liechtenstein, Islàndia i Noruega). En aquests casos, a més de disposar de la base legitimadora corresponent, cal garantir que la comunicació es duu a terme segons les condicions que estableixen els articles 44 a 50 de l'RGPD.

En aquest sentit, s'ha de comprovar, en primer lloc, si hi ha una [decisió d'adequació](#) per part de la Comissió Europea respecte a aquest tercer estat, és a dir, si ha estat declarat d'un nivell de protecció adequat. En cas que no hi hagi aquesta decisió d'adequació sobre el país concret, el responsable del tractament haurà d'haver adoptat alguna de les garanties complementàries següents:

- Normes corporatives vinculants.
- Clàusules sobre els tipus de protecció de dades adoptades per la Comissió Europea o per una autoritat de control i aprovades per la Comissió.
- Codis de conducta.
- Mecanismes de certificació.

Per tant, quan detectem que en un projecte s'ha de portar a terme una transferència internacional, cal consultar-ne l'adequació a l'expert en protecció de dades del CER/CERm.

En relació amb les transferències internacionals de dades, hem de fer referència al [Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions](#), que modifica diverses normes aplicables a les entitats del sector públic, entre les quals es troba la Llei 40/2015, de l'1 d'octubre, de règim jurídic del sector públic, a la qual s'afegeix el nou article 46 bis.

Article 46 bis. Ubicació dels sistemes d'informació i comunicacions per al registre de dades.

Els sistemes d'informació i comunicacions per a la recollida, l'emmagatzematge, el processament i la gestió del cens electoral, els padrons municipals d'habitants i altres registres de població, dades fiscals relacionades amb tributs propis o cedits i dades dels usuaris del sistema nacional de salut, així com els corresponents tractaments de dades personals, s'han d'ubicar i prestar dins del territori de la Unió Europea.

Les dades a què es refereix l'apartat anterior no poden ser objecte de transferència a un tercer país o organització internacional, amb excepció dels que hagin estat objecte d'una decisió d'adequació de la Comissió Europea o quan així ho exigeixi el compliment de les obligacions internacionals assumides per Espanya.

Per tant, en l'avaluació de projectes de recerca que impliquin transferències internacionals, i quan ens trobem en l'àmbit d'aplicació de l'article 46, hem de tenir en compte la limitació que estableix aquest article i valorar la seva aplicabilitat al projecte de recerca concret.

3.6 Avaluació d'impacte

L'article 35 de l'RGPD estableix que, en aquells casos en els quals sigui probable que el tractament comporti un alt risc per als drets i les llibertats de les persones físiques, el responsable del tractament ha de dur a terme una avaluació d'impacte relativa a la protecció de dades, que avaluï, en particular, l'origen, la naturalesa, la particularitat i la gravetat del risc.

D'altra banda, de conformitat amb la lletra f) de l'apartat 2 de la disposició addicional dissetena de la LOPDGDD, qualsevol projecte de recerca amb dades realitzat d'acord amb el que estableix l'article 89 de l'RGPD requereix la realització d'una avaluació d'impacte, sempre que es doni alguna de les situacions que disposa l'article 35 de l'RGPD o ens trobem en algun dels supòsits previstos per les autoritats de protecció de dades.

Es considera que el tractament de dades suposa un alt risc per als drets i les llibertats dels participants en la recerca quan es duen a terme perfilats, seguiment sistemàtic d'individus o processament a gran escala de categories especials de dades o s'utilitzen mètodes intrusius de processament de dades (com ara seguiment, vigilància, enregistrament d'àudio i vídeo, seguiment de geolocalització, etc.).

L'AEPD i l'Autoritat Catalana de Protecció de Dades (d'ara endavant, l'APDCAT) han publicat unes llistes dels tractaments que requereixen la realització d'una avaluació d'impacte, de conformitat amb el que estableix l'article 35.4 de l'RGPD, conjuntament amb unes guies i metodologies sobre com dur-les a terme.

A fi de determinar quan és necessari fer una avaluació d'impacte, també s'ha de tenir en compte el document de l'EDPB [Directrices sobre la evaluación de impacto relativa a la protección de datos \(EIPD\) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento \(UE\) 2016/679.](#)

En aquest sentit, les llistes de l'AEPD i l'APDCAT estableixen una sèrie de supòsits i indiquen que si es donen dues de les situacions enunciades o més és necessari fer una avaluació d'impacte.

Donades les característiques dels projectes de recerca, és altament probable que sigui necessari fer l'avaluació d'impacte corresponent, d'acord amb el que estableix l'article 35.3 de l'RGPD, ja que en l'àmbit de la recerca és molt habitual que es donin dos o més supòsits dels que s'indiquen a les llistes de l'AEPD i l'APDCAT.

El CERm no ha de dur a terme l'avaluació d'impacte, sinó que ha de verificar que existeix i que el seu resultat no evidencia cap incompliment de l'RGPD en el marc del projecte de recerca. El responsable del tractament, amb l'assessorament del delegat de protecció de dades, ha de dur a terme l'avaluació d'impacte.

Finalment, cal indicar que no és necessari fer una avaluació d'impacte per a cada projecte de recerca concret, sinó que és possible que determinats projectes de recerca comparteixin una mateixa avaluació d'impacte. S'ha d'avaluar en cada cas la necessitat de realitzar una avaluació d'impacte específica per al projecte, que vindrà determinada per l'existència d'elements únics i característics d'aquest projecte, com per exemple un alt component tecnològic (l'avaluació d'un algoritme, l'ús d'una app en el projecte de recerca o l'ús de tecnologies de dades massives).

3.7 Seguretat en el tractament de dades amb finalitats de recerca

La seguretat de les dades es regula a través de l'article 32 i, específicament en l'àmbit de la recerca, a través de l'article 89 de l'RGPD, i està estrictament lligada al principi d'integritat i confidencialitat que estableix l'article 5 de l'RGPD.

Així mateix, a través del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (i que, d'acord amb la disposició addicional primera de la LOPDGDD, és d'aplicació als tractaments de dades realitzats per les entitats del sector públic), es defineix la seguretat per defecte, que implica que els sistemes informàtics s'han de dissenyar de manera que garanteixin la seguretat per defecte, fet que suposa que:

- a)** El sistema ha de proporcionar la mínima funcionalitat requerida perquè l'organització assoleixi els seus objectius.
- b)** Les funcions d'operació, administració i registre d'activitat han de ser les mínimes necessàries, i s'ha d'assegurar que només siguin accessibles per a les persones, emplaçaments o equips autoritzats. Es poden establir, si escau, restriccions d'horari i punts d'accés habilitats.
- c)** En un sistema d'explotació s'han d'eliminar o desactivar, mitjançant el control de la configuració, les funcions que no siguin d'interès, siguin innecessàries i, fins i tot, aquelles que siguin inadequades a la finalitat que es persegueix.
- d)** L'ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi un acte conscient per part de l'usuari.

Cal que el sistema de tractament de les dades, com a mínim, garanteixi que:

- Disposa de les mesures tècniques i organitzatives necessàries per salvaguardar els drets dels participants en el projecte de recerca durant tot el cicle de tractament de les dades.
- El sistema de tractament de dades disposa de les mesures tècniques i organitzatives necessàries per evitar l'accés no autoritzat a dades personals.

Els criteris de seguretat que, de forma orientativa, s'han de tenir en compte en l'àmbit de la recerca són:

- a)** Pseudonimització, acords de confidencialitat, registres d'accés i distribució estricta de rols d'accés.
- b)** Realització d'una avaluació d'impacte de protecció de dades, d'acord amb l'article 35 de l'RGPD, quan aquest tractament pugui «comportar un risc elevat per als drets i les llibertats de les persones físiques», d'acord amb l'apartat 1 de l'article 35 de l'RGPD.
- c)** Consulta i assessorament del DPD quan sigui necessari. En aquest sentit, tots els CERm han de disposar d'una figura experta en protecció de dades que pot coincidir o no amb el DPD.
- d)** Les mesures adoptades per protegir les dades (incloses durant les transferències) han de ser adequades i estar documentades en el registre d'activitats de tractament.

Quan utilitzem recursos institucionals en els projectes de recerca, hem de seguir les directrius de seguretat indicades per la institució. Per aquest motiu, és important que la institució disposi d'una política de protecció de dades (article 24 de l'RGPD).

Quan s'utilitzin recursos externs en el marc del projecte de recerca, hem de poder verificar que les eines emprades compleixin els criteris de seguretat indicats en els paràgrafs anteriors.

Algunes indicacions pràctiques són les següents:

- Si les dades s'emmagatzemen en servidors externs, s'ha de garantir que aquests són segurs i s'han de detallar les mesures de seguretat aplicades a l'accés, incloent-hi una descripció de qui accedeix a les dades, quan, com i on s'emmagatzemen.
- S'ha d'evitar l'ús d'eines comercials no segures d'emmagatzemament al núvol que no garanteixin el compliment de l'RGPD.

- Si en el projecte es tracten dades amb un programari no institucional, cal que el codi desenvolupat per a les aplicacions utilitzi tècniques d'ofuscament de codi, sobretot en aplicacions mòbils, i que les aplicacions desenvolupades segueixin metodologies de desenvolupament segures.

L'aplicació del principi de privacitat des del disseny i per defecte, així com la realització d'una avaluació d'impacte, permeten garantir que aquestes mesures de seguretat són les adequades per al tractament de dades que es dugui a terme.

A continuació, i a fi d'oferir més claredat dels elements que hem de tenir en compte en matèria de seguretat, indiquem a tall de pregunta resposta els aspectes rellevants des del punt de vista de la seguretat.

3.7.1 Quins elements hem de tenir en compte quan utilitzem eines tecnològiques per tractar categories especials de dades?

Des del punt de vista de la normativa de protecció de dades, hem de tenir en compte diversos elements quan decidim desenvolupar o utilitzar una eina tecnològica per al tractament de categories especials de dades.

En primer lloc, en l'àmbit institucional és imprescindible disposar d'una política de protecció de dades (article 24 de l'RGPD), en què es prevegin les directrius de seguretat adoptades per la institució per garantir el compliment de la normativa de protecció de dades.

Així mateix, quan s'empren tecnologies innovadores en el tractament de categories especials de dades suposa un alt risc per als drets i les llibertats dels participants en la recerca. En aquest cas, d'acord amb l'article 35 de l'RGPD, cal fer una avaluació d'impacte. Per fer l'avaluació d'impacte en protecció de dades, disposeu de la plataforma AIPD, que posem a disposició de les entitats adherides a l'Oficina del DPD.

L'aplicació del principi de privacitat des del disseny i per defecte, així com la realització d'una avaluació d'impacte en protecció de dades, permeten garantir que aquestes mesures de seguretat són les adequades per al tractament de dades que es porta a terme.

3.7.2 Quins requeriments addicionals hem de tenir en compte quan utilitzem recursos externs?

a) Legitimació per al tractament de dades, accessos de tercers i usos secundaris. S'ha de garantir que, si un tercer té accés a dades (p. ex. mitjançant l'allotjament en servidors), es compti amb l'encarregat de tractament corresponent, d'acord amb l'article 28 de l'RGPD, i que no es duen a terme usos secundaris de dades.

b) Transferències internacionals de dades. Es considera transferència internacional de dades l'enviament de dades fora de la zona econòmica europea. En aquests casos, a més de disposar de la base legitimadora corresponent, cal garantir que la comunicació es du a terme segons les condicions que estableixen els articles 44 a 50 de l'RGPD. En aquest sentit, s'ha de destacar que el Privacy Shield (l'acord informal en l'àmbit de la legislació de protecció de dades entre els EUA i la UE) ha estat invalidat recentment. Aquesta eina era la que permetia fer transferències internacionals de dades als Estats Units.

Algunes indicacions pràctiques són les següents:

- Quan les dades s'emmagatzemen en servidors externs, cal garantir que aquests són segurs i detallar les mesures de seguretat aplicades a l'accés, incloent-hi una descripció de qui accedeix a les dades, quan, com i on s'emmagatzemen.
- S'ha d'evitar l'ús d'eines o plataformes comercials d'emmagatzemament en el núvol que no garanteixin el compliment de l'RGPD. En aquest sentit, destaquem que l'Agència de la Unió Europea per a la Ciberseguretat (ENISA) disposa d'un informe anomenat Cloud Security for Healthcare Service en què proporciona un conjunt de consells i bones pràctiques sobre seguretat i protecció de dades a l'hora d'utilitzar serveis al núvol en l'àmbit sanitari.

3.7.3 Quines eines col·laboratives podem utilitzar en el tractament de dades personals?

Hi ha múltiples eines i plataformes col·laboratives que serveixen per a l'emmagatzematge i la compartició de dades, algunes molt conegudes, com ara Google Drive, Microsoft OneDrive, Dropbox, WeTransfer, Mega, etc.

Aquestes eines, tot i la seva facilitat d'ús, no s'haurien d'utilitzar en el tractament de dades personals (emmagatzematge, publicació, compartició, etc.) per la manca de garanties de privacitat, seguretat de la informació i nivell de compliment normatiu.

Segons la Instrucció 8/2020, sobre l'ús de les TIC a l'Administració de la Generalitat de Catalunya, no es poden usar eines no corporatives quan hi hagi solucions a l'entorn professional i quan es tracti informació confidencial (dades personals). D'aquesta manera, desaconsellem la utilització d'aquestes eines o aplicacions en el tractament de dades personals (emmagatzematge, publicació, compartició, etc.), sempre que no hagin estat aprovades internament pel departament o entitat. Els motius principals són la manca de garanties pel que fa a la privacitat, la seguretat de la informació i de compliment normatiu que ofereixen aquestes eines en la versió comercial.

Com a exemples d'aquestes mancances tenim la pèrdua del control de les dades, la possible fuga o alteració de la informació, el risc d'accessos no autoritzats, la falta de còpies de seguretat que assegurin la disponibilitat de les dades o el potencial incompliment normatiu —transferències internacionals a països sense decisió d'adequació o garanties adequades, manca d'encàrrec de tractament quan un tercer accedeix a les dades en el marc d'una prestació de serveis (article 28 de l'RGPD) o el fet de no poder satisfer els drets dels titulars de les dades que estableix l'RGPD (dret a l'accés, la rectificació, la supressió, l'oposició, la limitació del tractament i la portabilitat d'aquestes dades).

Tot i això, l'Agència de Ciberseguretat de Catalunya recomana no fer ús del servei d'Office 365 de la Generalitat (Teams, OneDrive, SharePoint, Power BI, etc.) per al tractament de dades sensibles o confidencials, si no s'hi apliquen mesures de seguretat addicionals.

Per tant, a l'hora d'utilitzar serveis de Google, Microsoft, Dropbox o altres, us recomanem verificar que siguin eines corporatives i, en cas que ho siguin, accedir-hi mitjançant l'adreça de correu laboral. Si es fa servir alguna eina col·laborativa per al tractament de dades de caràcter personal, cal aplicar mesures de seguretat disponibles com el xifratge, l'autenticació de doble factor, la gestió adequada de permisos o el monitoratge de l'activitat per evitar accessos indeguts.

Eines per fer qüestionaris

Des del punt de vista de protecció de dades i de l'adequació a l'RGPD i la LOPDGDD, hem analitzat algunes de les plataformes tecnològiques utilitzades majoritàriament en projectes de recerca. A continuació, enumerem aquelles que considerem més adequades per al tractament de dades personals i/o de salut, per facilitar l'elecció de l'opció que s'adapti millor a les necessitats del projecte.

Plataformes per a enquestes

Per realitzar enquestes en què es tractin dades personals de categoria especial, recomanem fer servir plataformes que permetin instal·lar-se en els servidors locals de les institucions, com ara:

- REDCap
- LimeSurvey
- EUSurvey
- QuestionPro (també té disponible una versió al núvol que ofereix garanties en matèria de protecció de dades)

Per a enquestes amb un abast més ampli, que no tractin dades personals de categoria especial ni requereixin autenticació, recomanem Microsoft Forms (utilitzant l'eina corporativa mitjançant el compte institucional). Aquesta eina forma part del paquet d'Office 365 de Microsoft que proporciona el CTTI, amb un contracte d'encàrrec de tractament vigent. Aquesta suite d'aplicacions, en la versió corporativa, compta amb la certificació de l'Esquema Nacional de Seguretat (ENS) i de l'ISO 27001/27018.

Per a la recollida de dades clíniques, recomanem <https://www.clinicoverly.com/>

Desaconsellem la utilització d'eines comercials com Dropbox, SurveyMonkey, WeTransfer o GSuite (incloent-hi Google Analytics, Google Forms, Google Cloud, Google Drive, Google Docs, etc.), i Microsoft Office, tant en versions comercials gratuïtes com de pagament, per la pèrdua de control de les dades, la falta d'encàrrec de tractament o les possibles transferències internacionals que es puguin produir.

Plataformes per a l'anàlisi de dades biomèdiques i de recerca:

<https://www.datashield.org/> (instal·lat als servidors de les entitats)

Eines per compartir informació sensible:

- Mitjançant correu electrònic xifrat (enviant un codi de desxifrat per una altra via).
- Mitjançant sistemes de fitxers compartits de l'organització.
- Mitjançant OneDrive versió corporativa (accedint-hi amb un correu institucional).

Finalment, i en l'àmbit general, podem tenir en compte una sèrie de recomanacions en matèria de seguretat de la informació:

- Instal·lar REDCap o programaris de naturalesa similar en entorns on-premise, és a dir, en servidors allotjats al centre de processament de dades (CPD) de l'entitat de recerca.
- Identificar les bases de dades dels projectes i categoritzar les dades tractades en cadascuna.
- Incorporar únicament les dades necessàries i imprescindibles per dur a terme el projecte de recerca, i eliminar les dades innecessàries.
- Pseudonimitzar o anonimitzar les dades abans d'incorporar-les a REDCap.
- En cas de pseudonimització, cal separar adequadament les dades que permetin l'associació de dades personals de manera que l'equip investigador no hi tingui accés.
- Comunicar i emmagatzemar les dades personals emprant un xifratge segur.
- Establir un sistema de control d'accés sòlid i ben definit per a la base de dades de l'aplicació: política de contrasenya robusta, autenticació segura (2FA), assignació de rols i privilegis, i polítiques de mínim privilegi.
- Actualitzar el servidor i cercar si hi ha pedaços de seguretat.
- Protegir l'accés al servidor REDCap amb un tallafocs i establir polítiques d'accés per evitar les connexions remotes que provenguin de fora de l'entitat (filtratge IP). Podem personalitzar el servidor REDCap seguint la política de seguretat de l'entitat i les necessitats dels usuaris.
- Mantenir actualitzat el programari i les dependències, així com incorporar pedaços de seguretat disponibles tan aviat com sigui possible.
- Fer proves de seguretat (pentesting) per identificar possibles noves vulnerabilitats a la base de dades i al programari (REDCap).
- Tenir sistemes de monitoratge d'accessos i disposar de registre (log) de les accions realitzades sobre les dades.
- Disposar de sistemes de redundància i còpies de seguretat de les bases de dades.

4.

Aspectes específics de protecció de dades en l'àmbit de la recerca

En l'àmbit de la recerca, especialment amb els nous avenços en tecnologies de la informació, hi ha una sèrie d'aspectes que s'han de tenir en compte. Si bé són elements a analitzar en tots els àmbits, tenen un paper molt important en la recerca.

Per una banda, cal tenir en compte les implicacions que, en matèria de protecció de dades, té la participació de menors en els projectes de recerca, així com les especificitats que hem de considerar a l'hora de tractar les seves dades.

Per altra banda, trobem els projectes que incorporen elements d'intel·ligència artificial, en especial si es vol dur a terme anàlisis de perfils i decisions automatitzades.

També hi ha altres aspectes propis de l'àmbit de la recerca que, si bé no s'inclouen en el marc propi de la protecció de dades personals, resulten especialment rellevants a l'hora de posar-los en relació amb els requisits de protecció de dades, com els àmbits específics d'assaigs clínics o l'ús de mostres per a la recerca.

A continuació, es recullen els elements principals que cal tenir en compte en aquestes àrees concretes.

4.1 Menors a la recerca

Cada cop és més habitual que es tractin dades personals de menors d'edat en l'àmbit de la recerca. En aquest sentit, l'article 7.1 de la LOPDGDD estableix que els menors d'edat poden donar per ells mateixos el consentiment en matèria de protecció de dades a partir dels 14 anys. No obstant això, aquesta norma preveu una excepció per als supòsits en què la llei exigeixi l'assistència dels titulars de la pàtria potestat o de la tutela per dur a terme l'acte o el negoci jurídic en el context del qual se sol·licita el consentiment per al tractament. És a dir, hi haurà situacions en què l'edat mínima per al consentiment en protecció de dades no serà aquests 14 anys que estableix la norma, sinó que serà accessòria i estarà sotmesa a la de l'acte principal.

Ara bé, sovint es confon el consentiment com a base de legitimació per al tractament de les dades de menors (article 6.1.a) i/o 9.2.a) de l'RGPD) amb el consentiment informat propi de l'activitat biomèdica que es vol portar a terme, el qual es regeix per la normativa sectorial aplicable. Aquest consentiment informat presenta característiques pròpies i diferents respecte del consentiment com a base de legitimació del tractament de dades personals.

A continuació, s'adjunta una taula amb els diferents supòsits, depenent del context i el tipus d'estudi en què ens trobem.

Àmbit/finalitat	Supòsit	Edat mínima per prestar el consentiment en el tractament de dades personals quan aquest constitueixi la base de legitimitat [art. 6.1.a) + 9.2.a) de l'RGPD]	Edat mínima per prestar el consentiment informat per a l'actuació	Referències legals
RECERCA	Recerca amb caràcter general, quan no hi hagi cap intervenció.	<ul style="list-style-type: none"> ● 14 anys, excepte: >> No es consideri capaç intel·lectualment i emocionalment per comprendre l'abast de la intervenció. 	<ul style="list-style-type: none"> ● No es demana consentiment informat, ja que no es fa cap intervenció que afecti la seva salut. 	<ul style="list-style-type: none"> ● Llei 41/2002, de 14 de novembre ● Llei 21/2000, de 29 de desembre ● LOPDGDD ● RGPD
	Assaigs clínics	<ul style="list-style-type: none"> ● 18 anys*, excepte: >> Majors de 14 anys* que es considerin capaços intel·lectualment i emocionalment per comprendre l'abast de la intervenció. *Aquesta és la interpretació que aplica l'APDCAT al seu Dictamen CNS 41/2020, en què indica que és aplicable el règim general que disposa la normativa de l'autonomia del pacient, és a dir, el consentiment per al tractament de les seves dades depèn de la competència per comprendre l'abast de la intervenció sobre la seva salut, independentment que sigui menor o major de 16 anys. 	<ul style="list-style-type: none"> ● 18 anys*, excepte: >> Majors de 14 anys* que es considerin capaços intel·lectualment i emocionalment per comprendre l'abast de la intervenció. ● En cas de menors majors de 12 anys, també han de donar el seu consentiment, juntament amb els seus representants legals. ● En cas de menors de 12 anys, s'ha d'escollar la seva opinió. 	<ul style="list-style-type: none"> ● Reial decret 1090/2015, de 4 de desembre, pel qual es regulen els assajos clínics amb medicaments, els comitès d'ètica de la recerca amb medicament i del Registre espanyol d'estudis clínics ● Llei 41/2002, de 14 de novembre ● Llei 21/2000, de 29 de desembre ● LOPDGDD ● RGPD
	Recerca biomèdica	<ul style="list-style-type: none"> ● 18 anys 	<ul style="list-style-type: none"> ● 18 anys ● Els menors d'edat han de participar en la mesura de les seves possibilitats, segons les seves capacitats a la presa de decisions al llarg del procés de recerca. 	<ul style="list-style-type: none"> ● Llei 14/2007, de 3 de juliol, de recerca biomèdica ● LOPDGDD ● RGPD
	Estudis observacionals amb medicaments	<ul style="list-style-type: none"> ● 18 anys 	<ul style="list-style-type: none"> ● 18 anys 	<ul style="list-style-type: none"> ● Reial decret 957/2020, de 3 de novembre, pel qual es regulen els estudis observacionals amb medicaments d'ús humà ● LOPDGDD ● RGPD

4.2 Estudis amb dades que incorporen elements d'intel·ligència artificial. Anàlisi de perfils i decisions automatitzades

En els estudis en què s'incorporen elements d'intel·ligència artificial, a més de la normativa de protecció de dades personals, s'han de tenir en compte les normatives següents:

- Reglament (UE) 2024/1689 del Parlament Europeu i del Consell, de 13 de juny, pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial (RIA)
- Reglament (UE) 2025/327 del Parlament Europeu i del Consell, d'11 de febrer, relatiu a l'Espai Europeu de Dades de Salut (EEDS)

Si bé el RIA exclou, a priori, la recerca, és indispensable tenir en compte la normativa esmentada un cop es vulguin portar a terme accions relacionades amb l'ús d'IA a la pràctica clínica. En aquest sentit, si no es tenen en compte les indicacions del RIA des d'un inici (des del disseny), difícilment es podran incorporar, per exemple, algoritmes d'IA que s'hagin utilitzat en la recerca que no compleixin amb el que es disposa al Reglament.

Adicionalment, cal tenir en compte que, pel que fa al seu àmbit d'aplicació, el punt 2.3 de les directrius de la Comissió sobre les pràctiques d'intel·ligència artificial prohibides, que es van publicar el 4 de febrer de 2025, estableix:

(30) De conformitat amb l'article 2(8) de la Llei d'IA, aquesta no s'aplica «a cap activitat de recerca, prova o desenvolupament relativa a sistemes o models d'IA abans de la comercialització o la posada en servei». Aquesta exclusió està d'acord amb la lògica basada en el mercat de la Llei d'IA, que s'aplica als sistemes d'IA un cop es comercialitzen o es posen en servei.

Per exemple, durant la fase de recerca i desenvolupament (R+D), els desenvolupadors d'IA tenen la llibertat d'experimentar i provar noves funcionalitats que podrien implicar tècniques que es podrien considerar manipuladores i estar recollides a l'article 5(1)(a) de la Llei d'IA, si s'utilitzen en aplicacions orientades al consumidor. La Llei d'IA permet aquesta experimentació en reconèixer que l'R+D a la fase inicial és essencial per refinar les tecnologies d'IA i garantir que compleixin els estàndards ètics i de seguretat abans de la seva comercialització.

(31) Tal com s'aclareix al considerant 25 de la Llei d'IA, aquesta té per objecte donar suport a la innovació i reconeix la importància de la recerca científica per fer avançar les tecnologies d'IA i contribuir al progrés científic i a la innovació. Per tant, l'article 2, apartat 6, de la Llei d'IA estableix una exclusió per als sistemes o models d'IA, inclosos els seus resultats, desenvolupats específicament i posats en servei amb l'única finalitat de fer recerca i desenvolupament científics.

Per exemple, la recerca sobre les respostes cognitives i conductuals davant estímuls subliminals o enganyosos impulsats per la IA pot proporcionar informació valuosa sobre les interaccions entre humans i IA, cosa que servirà de base per a aplicacions d'IA més segures i eficaces en el futur. Malgrat la prohibició que estableix l'article 5, apartat 1, lletra a) de la Llei d'IA, es permeten aquestes investigacions, ja que estan excloses de l'àmbit d'aplicació d'aquesta Llei.

(32) No obstant això, l'exclusió de l'article 2(8) de la Llei d'IA s'entén sense perjudici de l'obligació de complir amb el que disposa aquesta Llei quan un sistema d'IA es comercialitza o es posa en servei com a resultat d'aquesta activitat de recerca i desenvolupament. Les proves en condicions reals en el sentit de la Llei d'IA tampoc no estan cobertes per aquesta exclusió. Per exemple, un municipi que vulgui provar un programari de reconeixement facial utilitzant un sistema RBI als carrers durant el carnaval pot reclutar voluntaris perquè el sistema els identifiqui en condicions reals. Atès que les proves al món real no entren dins l'exclusió de l'article 2(8) de la Llei d'IA, les proves planificades han de complir plenament els requisits establerts per als sistemes RBI a la Llei d'IA, llevat que el sistema es provi en un entorn de proves regulatiu d'IA o de conformitat amb el règim especial per a proves en condicions reals fora d'aquest entorn, tal com estableixen els articles 60 i 61 de la Llei d'IA.

(33) En qualsevol cas, qualsevol activitat de recerca i desenvolupament (fins i tot quan estigui exclosa de l'àmbit d'aplicació de la Llei d'IA) s'ha de dur a terme de conformitat amb les normes ètiques i professionals reconegudes per a la recerca científica, així com la legislació de la Unió aplicable (per exemple, la legislació sobre protecció de dades, que continua sent aplicable).

És a dir, es considera que les proves amb dades reals, encara que formin part d'una recerca, els és d'aplicació el RIA. L'aspecte interessant d'aquest punt és que reconeix la possibilitat que les proves fetes amb dades reals tinguin la consideració de recerca.

En aquest sentit, una de les novetats que ha generat més debat la trobem a l'article 27 del RIA, que és la necessitat de portar a terme una avaluació d'impacte de drets fonamentals (AIDF), que no s'ha de confondre amb l'AIPD, tot i que puguin coincidir en alguns punts. En aquest context, l'Autoritat Catalana de Protecció de Dades (APDCAT) ha publicat la seva [Metodologia aplicada de l'avaluació d'impacte sobre els drets fonamentals en el disseny i desenvolupament de la IA](#) per portar a terme aquest tipus d'avaluacions.

No obstant això, en l'àmbit de la salut, aquest requeriment només s'ha de complir en casos molt concrets de sistemes d'IA d'alt risc, inclosos en l'annex III del RIA, que comprenen:

- Sistemes d'IA destinats a ser utilitzats per les autoritats públiques, o en nom seu, per avaluar l'admissibilitat de les persones físiques a l'hora de beneficiar-se de serveis d'assistència sanitària, o per modificar o retirar aquests serveis.
- Serveis d'IA destinats a ser utilitzats per a l'avaluació i la classificació de les trucades d'emergència realitzades per persones físiques en serveis d'assistència mèdica, així com en sistemes de triatge de pacients en serveis d'urgències.

Per tant, la repercussió que té aquesta obligació en els projectes de recerca en la salut és probablement de baix impacte.

Aquesta obligació, tot i que pugui tenir punts en comú, és independent de la necessitat de realitzar l'AIPD corresponent, que, en els projectes que utilitzin dades personals i tecnologies basades en IA, és una obligació que estableix l'RGPD.

Bases de legitimació:

El disseny d'algoritmes passa per diverses fases de maduresa durant la seva etapa de desenvolupament, que va des de la creació del codi, la recopilació de les dades personals per a l'entrenament, l'entrenament de les dades i la validació.

Quant al cicle de vida i la classificació, una primera referència la trobem en l'escala TRL, que mesura la maduresa de la tecnologia. Aquesta escala va del TRL 1 al TRL 9, i abasta des dels principis bàsics de la tecnologia (TRL1) fins a les proves portades amb èxit en entorns reals (TRL9). Aquesta escala s'utilitza en les diferents convocatòries europees de projectes de recerca.

Recentment, però, el Dictamen 28/2024 sobre determinats aspectes de protecció de dades relacionats amb el tractament de dades personals en el context dels models d'IA, emès pel CEPD, proposa una classificació en dues fases: la fase de desenvolupament i la fase de desplegament.

El desenvolupament d'un model d'IA cobreix totes les etapes prèvies a qualsevol desplegament del model d'IA i inclou, entre altres coses, el desenvolupament de codi, la recollida de dades personals de formació, el preprocessament de les dades personals per l'entrenament i l'entrenament. El desplegament d'un model d'IA cobreix totes les etapes relacionades amb l'ús d'un model d'IA i pot incloure qualsevol operació realitzada després de la fase de desenvolupament.

És determinant veure si el tractament de dades que fem amb l'algoritme d'IA es pot considerar recerca o pot classificar-se d'una altra forma. Com a norma general, es considera que l'entrenament, la validació i la prova, incloent-hi les proves amb dades reals, dels algoritmes d'IA s'emmarquen en el camp de la recerca.

Com en tot projecte de recerca, en aquestes fases es poden tractar dades personals i, en aquest cas, caldrà determinar quina és la base legitimadora del tractament de dades que es pot utilitzar en cada fase, la qual estarà directament relacionada amb la finalitat del tractament. Per tal que aquest tractament de les dades sigui lícit, cal comptar amb una de les bases de legitimació que disposa l'article 6 de l'RGPD. Així mateix, en tractar-se de dades de categoria especial, com les dades de salut, addicionalment, cal comptar amb alguna de les excepcions que estableix l'article 9 de l'RGPD que en permetin el tractament.

En l'àmbit de la salut, aquest es configura com a recerca, sigui perquè es troba en la fase de desenvolupament d'un algoritme que acabarà sent producte sanitari o perquè les dades s'utilitzen per fer estudis comparatius d'eficàcia respecte d'altres eines de diagnòstic habituals. En aquest cas, el fonament que solem utilitzar al sector públic per tractar les dades es basa en l'interès públic amb finalitats de recerca (art. 6.1.e) + art. 9.2.j) de l'RGPD), d'acord amb el que estableix l'article 89 i l'apartat 2 de la disposició addicional dissetena de la LOPDGDD. No obstant això, tal com s'ha esmentat a l'apartat de bases de legitimació, aquest tractament també es pot basar en altres supòsits, com el consentiment del participant

IA en la normativa de protecció de dades:

L'RGPD introdueix dos conceptes: el perfilatge o profiling i la presa de decisions automatitzades, que de vegades són complexos d'identificar, però es donen sovint en el marc de projectes de recerca, i tenen una especial rellevància pel que fa a l'aplicació de la normativa de protecció de dades, especialment l'article 22 de l'RGPD.

Hi ha una **elaboració de perfils** quan es donen els elements següents: hi ha una forma automatitzada de tractament, en relació amb les dades personals, i l'objectiu és avaluar aspectes personals en relació amb una determinada persona física (art. 4.4 de l'RGPD).

Cal distingir l'elaboració de perfils de la simple classificació de persones, ja que la definició inclou l'element avaluar, que implica analitzar o fer prediccions sobre persones.

Aquesta elaboració de perfils pot implicar que:

- i) es prengui una decisió a partir únicament d'una decisió automatitzada,
- ii) pot ser que l'elaboració del perfil no impliqui cap presa de decisions basades únicament en una decisió automatitzada o,
- iii) que directament no impliqui la presa de cap decisió.

L'article 22 de l'RGPD només s'aplica al primer cas, quan s'estableix el **dret a no ser objecte d'una decisió basada únicament en un tractament automatitzat**.

Per tant, la clau està en el concepte de decisió automatitzada, és a dir, la capacitat de presa de decisions basades únicament en mitjans tecnològics **sense una participació humana** que permet descartar l'aplicació de l'article 22 de l'RGPD.

Per determinar si hi ha participació humana, aquesta **supervisió humana** s'ha de dur a terme de manera que sigui **significativa** per a la presa de la decisió, no únicament simbòlica. L'ha de dur a terme una **persona autoritzada i competent** amb **capacitat suficient per modificar la decisió**, i capaç d'entendre totes les dades per tenir-les en compte a l'hora de realitzar l'anàlisi corresponent. En aquestes situacions, quan es duu a terme **l'avaluació d'impacte** per justificar la no aplicació de l'article 22, **s'ha d'identificar el grau de participació humana en el procediment de presa de decisions**.

Aquest concepte l'hauríem d'incloure com un element a valorar en la metodologia d'avaluació d'impacte que fem. Cal determinar com afecta la participació humana en el procediment de presa de decisions i si aquesta descarta l'aplicació de l'article 22 de l'RGPD.

Per tant, els conceptes de decisió automatitzada i elaboració de perfils s'encavalquen, però es poden donar de manera independent. És a dir, les decisions automatitzades es poden donar sense elaboració de perfils, i l'elaboració de perfils es pot donar sense que hi hagi decisions automatitzades.

Podem concloure que l'article 22 de l'RGPD només és aplicable quan hi ha una decisió automatitzada que afecta els drets dels interessats i que l'elaboració de perfils no sempre entra dins l'àmbit d'aquest article, únicament serà així quan es pren una decisió automatitzada a partir d'aquesta elaboració de perfils.

Tant en el cas de decisions automatitzades com en el d'elaboració de perfils, al marge de l'article 22 de l'RGPD, s'ha de considerar el fet d'aplicar els principis de l'article 5 de l'RGPD i les bases legitimadores. A fi de garantir que s'apliquen correctament els principis de la normativa en aquestes situacions, el document [Directrius sobre decisions individualitzades automatitzades i elaboracions de perfils del Grup de Treball de l'article 29](#), inclou un annex de bones pràctiques per garantir el compliment dels principis de l'article 5 de l'RGPD.

4.3 Assaigs clínics

Quan analitzem el règim jurídic dels assaigs clínics, cal tenir en compte tant la normativa pròpia dels assaigs clínics com la normativa de protecció de dades (RGPD i LOPDGDD). Des del punt de vista de la normativa específica per la matèria hem de tenir en compte:

- Reglament UE 536/2014, sobre assaigs clínics de medicaments d'ús humà (CTR per les seves sigles en anglès).
- Text refós de la Llei de garantia i ús racional dels medicaments i productes sanitaris, aprovat pel Reial decret legislatiu 1/2015, de 24 de juliol.
- Reial decret 1090/2015, de 4 de desembre, pel qual es regulen els assajos clínics amb medicaments, els comitès d'ètica de la recerca amb medicaments i el Registre espanyol d'estudis clínics.

Adicionalment, i donada la complexitat en la interpretació de la normativa, també haurem de tenir en compte l'Informe [038/2021](#) elaborat per l'Agència Espanyola de Protecció de Dades relatiu al tractament de dades en el marc dels assaigs clínics, així com el [Dictamen 3/2019](#) sobre les preguntes i respostes sobre la relació entre el Reglament sobre assaigs clínics (REC) i el Reglament general de protecció de dades (RGPD) del Comitè Europeu de Protecció de Dades.

Bases de legitimació:

Com en tot projecte de recerca, els responsables del tractament (promotor i centre) han de disposar d'una base jurídica que habiliti els diferents tractaments que es porten a terme en el marc d'un assaig, d'acord amb el que estableix **l'article 6 de l'RGPD**. A més, en tractar-se de dades de salut, han de comptar amb un dels supòsits que disposa **l'article 9.2 de l'RGPD, que permetin aixecar la prohibició de tractament de dades de salut que estableix l'article 9.1 de l'RGPD**.

Seguint el criteri del Comitè Europeu de Protecció de Dades, podem distingir dos tipus de tractaments de dades en el transcurs de dades:

1. Operacions relacionades directament amb l'activitat de recerca: són les activitats de tractament dutes a terme per l'equip d'investigació del centre i el promotor en els seus respectius rols de responsables, respecte a la recollida i el tractament de dades relacionades amb el fitxer de dades mestres de l'assaig. Tal com apunta el CEPD, en el context dels assaigs, la recerca científica s'ha d'entendre d'acord amb els estàndards i les normes metodològiques i ètiques del sector, de conformitat amb les normes de bona pràctica clínica.

El CEPD assenyala que en aquest cas es poden utilitzar les bases jurídiques següents:

- a) Consentiment explícit de l'interessat: art. 6.1.a) + 9.2.a) de l'RGPD
- b) Missió d'interès públic: art. 6.1.e) + art. 9.2.i) o 9.2.j) de l'RGPD
- c) Interès legítim del responsable: art. 6.1.f) + art. 9.2.i) o 9.2.j) de l'RGPD

Des de la posició que ocupen els centres de recerca del sector públic, s'aplicarien les opcions a) i b) atès que l'opció c) en tot cas seria aplicable a la indústria farmacèutica, promotora de l'assaig.

2. Operacions relacionades amb la finalitat de protecció de la salut, la qualitat i seguretat dels medicaments mitjançant la generació de dades fiables i sòlides (finalitats relacionades amb la fiabilitat i la seguretat): el CEPD entén que la base jurídica adequada és el compliment d'una obligació legal per part del responsable del tractament (art. 6.1.c) de l'RGPD). Aquesta base operaria en relació amb el compliment d'obligacions formals i procedimentals, entre les quals s'inclouen:

- la notificació de l'investigador d'esdeveniments adversos al promotor;
- la conservació de l'arxiu mestre de l'assaig i dels expedients mèdics dels subjectes que ve determinat per la normativa nacional;
- i la comunicació de dades dels assaigs clínics a les autoritats competents en el curs d'una inspecció.

Distribució de rols:

Respecte als rols dels diferents actors en els assaigs clínics, actualment no hi ha cap posició unànime en l'àmbit europeu. Tant la corresponsabilitat entre el promotor i el centre hospitalari com el fet de considerar el promotor i el centre de recerca com a responsables independents, cadascú amb les seves funcions i obligacions, són possibles.

Escollir una opció o una altra dependrà del context i la configuració de l'assaig clínic. En aquest sentit, cal fer esment del fet que el Codi Tipus de Farmaïndústria aposta per la configuració de l'assaig com a dos responsables independents.

Cal tenir en compte que en cas de decantar-se per l'acord de corresponsabilitat, s'haurà de signar l'acord de conformitat corresponent que estableix l'article 28 de l'RGPD.

Especial consideració de la figura dels monitors:

En primer lloc, s'ha de tenir en compte que els **monitors es consideren encarregats de tractament del promotor**, d'acord amb l'Informe 0038/2021 emès per l'Agència Espanyola de Protecció de Dades.

No obstant això, el monitor o monitora ha d'accedir a la història clínica del centre en l'exercici de les funcions que legalment té atribuïdes. En aquest sentit, **el responsable de la informació personal de la història clínica dels pacients són els centres de salut** i, per tant, el que s'ha de fonamentar és la legitimació per permetre l'accés d'una persona externa al centre a les dades necessàries per a la verificació pròpia del monitoratge. Això s'aplica amb independència que aquest accés es faci al centre o en remot. Valorar i decidir si existeix aquesta legitimació és una tasca del responsable del tractament de la història clínica, és a dir, del centre on es porta a terme l'assaig.

Així, pel que fa a la relació entre monitor i centre, l'informe esmentat sosté que el monitor no actua com a encarregat de tractament del centre i que la base jurídica que habilita aquest accés del monitor a les dades de la història clínica **esdevé pel compliment d'una obligació legal del responsable (art. 6.1.c) de l'RGPD**.

Per tant, la signatura de documentació relativa a la confidencialitat i bones pràctiques que fan signar els centres esdevé part de la relació entre el centre responsable de la HC, que ha de prendre les mesures de seguretat que cregui necessàries, i el monitor, i no com a part de la relació d'encarregat del tractament del monitor respecte al promotor. **Per tant, no esdevé un element que el promotor hagi de valorar i/o oposar-se a la seva signatura.**

Tercers contractats pel promotor:

En cas que una tercera entitat (proveïdor contractat pel promotor) accedeixi a dades personals per prestar el seu servei, encara que sigui contractada pel promotor, resulta necessari valorar cas per cas qui és el responsable del tractament de les dades a les quals aquesta tercera entitat accediria. Aquest responsable de tractament és qui haurà de formalitzar un contracte d'encarregat del tractament amb la tercera entitat. A diferència del cas del monitoratge, aquesta actuació no està emparada per una norma de rang legal.

Dret d'informació al participant:

D'altra banda, com en tots els projectes de recerca, és essencial informar els participants del projecte amb la informació que estableix l'article 13 de l'RGPD, amb la particularitat que la normativa d'assaigs clínics també incorpora certa informació addicional a transmetre. Aquesta informació s'ha de proporcionar de manera que sigui completa, succinta, clara, pertinent i comprensible.

Des del punt de vista de la normativa específica dels assaigs clínics, s'ha d'informar de:

- La naturalesa, els objectius, els beneficis, les implicacions, els riscos i els inconvenients de l'assaig clínic.

- Els drets i les garanties del subjecte d'assaig pel que fa a la seva protecció i, en particular, el seu dret a negar-se a participar-hi i a abandonar l'assaig clínic en qualsevol moment sense haver de proporcionar cap justificació i sense sofrir cap perjudici per aquest motiu.
- Les condicions en les quals es durà a terme l'assaig clínic, inclosa la durada prevista de la participació dels subjectes.
- Les possibles alternatives de tractament, incloses les mesures de seguiment en cas que el subjecte d'assaig decideixi interrompre la seva participació.

Així mateix, des del punt de vista de la normativa de protecció de dades, d'acord amb l'article 13 de l'RGPD, s'ha d'informar del següent:

- Nom del tractament.
- Responsable del tractament. En aquest cas, s'ha d'identificar el centre on es porta a terme l'assaig com a titular de les dades identificades i el promotor com a titular de les dades pseudonimitzades.
- Dades de contacte del delegat de protecció de dades. S'han d'identificar tant al DPD del promotor com del centre, ja que ambdós són responsables del tractament.
- Finalitats del tractament.
- Base jurídica o legitimació per al tractament. En aquest punt, cal tenir en compte que la base jurídica més adequada per als diversos tractaments de les dades en el marc d'un assaig clínic no sempre és el consentiment. Sovint es pot utilitzar l'interès públic o el compliment d'una obligació legal, segons les circumstàncies en què es porti a terme l'assaig.
- Altres destinataris a qui es comuniquen les dades.
- Conservació de les dades. L'arxiu mestre de l'assaig clínic s'ha de conservar com a mínim durant 25 anys després. Per tant, és el temps mínim de conservació de les dades que s'ha d'indicar.
- Exercici de drets i dret a presentar una reclamació davant l'autoritat competent (AEPD/APDCAT).

Tota aquesta informació, tot i que s'haurà de facilitar en una entrevista prèvia amb un membre de l'equip investigador, també ha de constar per escrit i estar a disposició del subjecte.

En aquest sentit, us fem referència a l'[Informe 040931/2019 de l'AEPD](#), que analitza el contingut de la guia de l'AEMPS — *Guía para la correcta elaboración de un modelo de hoja de información al paciente y consentimiento informado (HIP(CI))* —, en què s'analitzen els elements que ha de tenir el full d'informació i consentiment des del punt de vista del tractament de dades en el marc dels assaigs clínics.

Ús de les dades dels investigadors més enllà de la recerca:

El tractament de les dades dels investigadors amb finalitats que no són necessàries per a la consecució de l'assaig clínic, com pot ser l'emmagatzematge per part dels promotors per contactar-hi per a futurs projectes, no es pot basar en l'interès legítim com a base de legitimació, sinó que resultaria necessari el consentiment de l'investigador.

En aquest sentit, la responsabilitat d'informar els investigadors del tractament de les seves dades personals no pot transferir-se a l'investigador principal, ja que la situació no constitueix una de les excepcions que recull la normativa. Per tant, el responsable del tractament, en aquest cas la promotora, té l'obligació d'informar els interessats de tots els aspectes de l'article 13 de l'RGPD.

Conservació de l'arxiu mestre:

El contingut de l'arxiu mestre de l'assaig es compon dels documents essencials relacionats amb aquest, de tal manera que permetin verificar la seva realització i la qualitat de les dades obtingudes tenint en compte totes les característiques d'aquest assaig. Aquest arxiu s'haurà de conservar durant 25 anys.

4.4 Ús de mostres per a la recerca

Com s'ha posat de manifest, aquest apartat no analitza únicament el règim del tractament de dades aplicable a les dades obtingudes de les mostres biològiques, sinó que també estudia el règim aplicable a la gestió de les mostres biològiques, que no es considera en si dada personal, sinó una font de les quals es poden obtenir dades personals.

La regulació de l'ús de mostres per a la recerca la podem trobar e la normativa següent:

- Llei 14/2007 de recerca biomèdica (d'ara endavant, LIB, per les seves sigles en castellà).
- Reial decret 1716/2011 que aprova el reglament de desenvolupament de la LIB (d'ara endavant, RDLIB).
- Recomanació (2016)6 del Comitè de Ministres als estats membres sobre investigacions sobre materials biològics d'origen humà (d'ara endavant, RecCM).

Així mateix, donada la naturalesa de les mostres biològiques com a dada personal, també és d'aplicació la normativa de protecció de dades:

- 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.
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

A continuació, es tracten els aspectes relacionats amb la forma de legitimar l'ús de les mostres per a la recerca (consentiment i excepcions al consentiment), els diferents règims d'emmagatzematge de la mostra, la forma com s'han de transferir les mostres entre centres i una anàlisi de la incidència de la normativa de protecció de dades en l'àmbit de la recerca amb mostres.

Ús de mostres per a la recerca:

La normativa estableix com a criteri general que totes les mostres que s'utilitzin amb finalitats de recerca han de disposar del consentiment informat corresponent del subjecte font, amb el contingut que estableix l'article 59 de la LIB i l'article 23 del RDLIB.

Així, com a principi general, l'ús de mostres per a la recerca sempre ha de disposar del consentiment del subjecte font de la mostra i obtenir el vistiplau del Comitè d'Ètica de la Recerca.

En determinades situacions, el CER pot autoritzar de forma excepcional l'ús de mostres que no disposen de consentiment, sempre que concorrin uns determinats requeriments. Aquest règim d'excepcionalitat s'estableix en diversos preceptes de la LIB i el RDLIB:

CONSENTIMENT EN L'ÚS DE MOSTRES BIOLÒGIQUES

	Requeriments	Normativa
RÈGIM GENERAL	<p>Totes les mostres que s'utilitzin amb finalitats de recerca han de disposar del consentiment informat corresponent del subjecte font, amb el contingut següent:</p> <ul style="list-style-type: none"> ● Règim d'ús i emmagatzematge de les mostres (projecte, col·lecció o biobanc). Finalitat de la investigació, identificació del responsable i lloc de realització de les anàlisis. ● Riscos i beneficis esperats de la recerca i possibilitat de tornar a contactar amb el subjecte font. ● Dret de revocació, dret a la confidencialitat i dret a conèixer les dades genètiques rellevants obtingudes a través de la recerca. ● Advertir de la possibilitat d'obtenir informació que afecti la salut del subjecte font i el seu dret a rebre o no rebre aquesta informació, així com l'advertència que aquesta informació pot afectar també els seus familiars i la conveniència d'informar-los. ● Destinació de la mostra una vegada finalitzat el projecte. 	<p>Articles 4, 13, 58 i 59 de la LIB Article 23 de l'RDLIB</p>
ALTRES RÈGIMS DEL CONSENTIMENT	<p>Els subjectes que no poden escriure poden atorgar el consentiment per qualsevol mitjà admes en dret que permeti deixar constància de la seva voluntat.</p> <hr/> <p>Les persones incapacitades legalment o menors d'edat han d'atorgar el consentiment per substitució, tot i que han de participar durant el procés de recerca en la mesura del possible i, segons la seva edat o capacitats, en la presa de decisions.</p>	<p>Articles 4.1, 4.2 i 20 de la LIB</p>
EXCEPCIONS AL RÈGIM DEL CONSENTIMENT	<p>Realització de recerca en situacions clíniques d'emergència en persones que no puguin prestar el seu consentiment, a causa de la seva situació clínica quan concorren les condicions següents:</p> <ul style="list-style-type: none"> ● Que no sigui possible realitzar investigacions d'eficàcia comparable en persones que no es trobin en aquesta situació d'emergència. ● Que en cas que no sigui previsible que la recerca produeixi resultats beneficiosos per a la salut del pacient, tingui el propòsit de contribuir a millorar de forma significativa la comprensió de la malaltia o la condició del pacient, amb l'objectiu de beneficiar altres persones amb la mateixa malaltia o condició, sempre que comporti el mínim risc i incomoditat. <p>Aquests són casos excepcionals i justificats, i quan la persona torna a estar en condicions de fer recerca n'ha de donar el consentiment.</p> <hr/> <p>Autorització de l'ús de les mostres per part del CER quan l'obtenció del consentiment no sigui possible o representi un esforç no raonable, sempre que es donin els requeriments següents:</p> <ul style="list-style-type: none"> ● No es disposi d'una alternativa viable per a la realització del projecte amb un altre grup de mostres per les quals es disposi del consentiment. ● Que es tracti d'una recerca d'interès general. ● Que la recerca, degudament autoritzada, es porti a terme per la mateixa institució que va sol·licitar el consentiment per a l'obtenció de mostres, en cas que aquest fos necessari. ● En cas que es tracti de mostres de subjectes identificats o identificables, que la recerca sigui menys efectiva o no sigui possible sense les dades identificatives del subjecte font. ● Que no consti una objecció expressa del subjecte font o la seva representació legal. ● Que es garanteixi la confidencialitat de les dades de caràcter personal. ● Que s'ha valorat l'esforç, el temps i els mitjans humans, materials i econòmics necessaris per obtenir el consentiment. <hr/> <p>En cas de donants morts, amb un dictamen previ favorable del CER, les mostres es poden utilitzar sempre que no consti l'objecció expressa del subjecte font, consultant les seves últimes voluntats. Si no es tingués constància d'aquestes, se n'ha de consultar els familiars i professionals sanitaris que van atendre la persona, a fi d'esbrinar si es dona l'oposició. A més, s'ha de tenir present que, en cas que el projecte tingui alguna implicació clínica directa per als familiars, se'ls ha de preguntar addicionalment si volen que se'ls informi dels resultats clínicament rellevants per a ells.</p>	<p>Article 21 de la LIB</p> <hr/> <p>Article 58 de la LIB i 24 de l'RDLIB</p> <hr/> <p>Article 26 del RDLIB</p>
MOSTRES RECOLLIDES ABANS DE L'ENTRADA EN VIGOR DE LA LIB	<p>Mostra anònima: la mostra es pot utilitzar prèvia autorització del CER.</p> <p>Mostra identificada: la mostra es pot utilitzar amb l'autorització prèvia del CER valorant que concorren els requisits següents:</p> <ul style="list-style-type: none"> ● Es tracta d'una recerca d'interès general. ● La recerca sigui menys efectiva o no sigui possible sense les dades identificatives del subjecte font. ● No hi consta una objecció expressa. 	<p>Disposició transitòria segona de la LIB</p>

Règim d'emmagatzematge de mostres:

D'acord amb l'article 22 de l'RDLIB, les mostres biològiques es poden recollir i utilitzar per a un projecte de recerca concret, passar a formar part d'una col·lecció o bé passar a formar part d'un biobanc:

- **Projecte de recerca concret:** les mostres conservades per a la seva utilització en un projecte de recerca concret només es poden fer servir en aquest projecte de recerca, tret que el subjecte font doni un nou consentiment exprés perquè la mostra pugui ser utilitzada en altres projectes o per tal que s'incorpori en una col·lecció o biobanc.
- **Col·lecció:** conjunt ordenat i amb vocació de permanència de mostres biològiques d'origen humà, conservades fora de l'àmbit organitzatiu d'un biobanc, destinades a la recerca biomèdica. Aquestes mostres només es poden fer servir per a una línia de recerca i per les entitats o persones que constin en el document de consentiment, tret que concorri un nou consentiment exprés del subjecte font per a una altra finalitat o per cedir la mostra a un tercer. En aquest punt, es pot arribar a admetre que es comparteixin mostres en projectes col·laboratius en què participa l'investigador titular de la col·lecció si al document de consentiment informat se'n fa referència.
- **Biobanc:** establiment sense ànim de lucre que acull una o diverses col·leccions de mostres biològiques d'origen humà amb finalitats de recerca biomèdica. Les mostres emmagatzemades en un biobanc es poden fer servir en qualsevol recerca en les condicions que estableix la LIB, sempre que el subjecte font o, si escau, els seus representants legals hagin prestat consentiment per tal que la mostra es guardi en el biobanc.

Acords de transferència de mostres:

Cal fer esment que les mostres de vegades s'han d'utilitzar fora del centre on es van obtenir. Per poder enviar aquestes mostres fora dels centres, el règim d'ús de la mostra ho ha de permetre i s'ha de disposar del consentiment del pacient, però també s'ha de signar un MTA (Material Transfer Agreement).

Hem de distingir els MTA que la normativa estableix com a obligatoris (articles 33 i 34 de l'RDLIB) i aquells que, encara que no estiguin establerts com a obligatoris per la norma, considerem necessaris per garantir l'ús que es farà de la mostra. En aquest sentit, també s'ha de tenir en compte el que estableix l'article 17 de la Recomanació CM, en relació amb els principis que han de guiar la transferència de mostres, i interpretar la legislació espanyola a la llum del que estableix aquest text.

- **MTA obligatoris:** articles 33 i 34 de l'RDLIB.
 - La mostra es troba al biobanc, col·lecció o en projecte i s'incorpora en un biobanc o col·lecció.
 - La mostra es troba al biobanc o col·lecció i s'incorpora en un projecte.
- **MTA no obligatoris: article 31 de l'RDLIB.**
 - Utilització de mostres biològiques procedents d'altres països. La normativa estableix que la responsabilitat de garantir que les mostres recollides a l'estranger compleixen amb la LIB és del CERm. Per tant, és l'única forma de garantir aquest extrem.
 - Enviament de mostres a repositoris internacionals que no són biobancs o col·lecció en el sentit de la LIB. No es preveu aquest cas per norma, per tant, és l'única manera que tenim de garantir que la mostra es tractarà amb els requisits mínims que estableix la normativa.
 - Estudis multicèntrics en què la mostra recollida en el marc d'un projecte o col·lecció s'utilitzarà per a diverses situacions, sempre que estigui previst en el consentiment.

Respecte al contingut mínim d'aquests MTA, s'ha d'incorporar:

- Identificació del cedent i el cessionari, i el règim jurídic aplicable a les mostres.
- Delimitació de l'ús que es pot fer de les mostres i destinació una vegada finalitzat el projecte.
- Règim de dades personals associades a les mostres.
- En cas que les mostres estiguin codificades, obligació de comunicar les troballes rellevants.
- Costos associats a l'obtenció de les mostres que es repercuteixen, en absència d'ànim de lucre.
- Aspectes relacionats amb la propietat intel·lectual del projecte.

Malgrat aquest contingut mínim, caldrà ampliar-ne el contingut per tal d'ajustar-lo a les especificitats del projecte concret.

Protecció de dades en l'ús de mostres per a recerca:

Com en tots els casos, des del punt de vista estrictament de la normativa de protecció de dades, cal veure quina és la base legal que ens permet fer servir les dades associades a la mostra amb finalitats de recerca.

Tanmateix, abans d'entrar a revisar aquest punt, cal destacar que, quan parlem d'ús de mostres en el marc d'un biobanc, sovint la titularitat del biobanc recau en la fundació o entitat que gestiona o porta a terme la recerca, mentre que la història clínica d'on extreuen les dades per fer recerca és titularitat de l'hospital.

Per tant, a l'hora de sol·licitar el consentiment per al tractament de les dades, cal tenir en compte que el consentiment relatiu a l'ús de mostres i les dades associades en el marc del biobanc no inclou el consentiment per accedir a dades de la història clínica amb finalitats de recerca, fins i tot si aquestes dades es vinculen a la mostra.

Així mateix, cal fer esment que, quan demanem consentiment per emmagatzemar les mostres al biobanc, es demanen unes dades personals bàsiques associades a la mostra, ja que sense aquestes la mostra no tindria cap utilitat.

Finalment, cal aclarir que, en termes normatius, és important diferenciar entre el consentiment informat que hem detallat en apartats anteriors, que resulta indispensable per al tractament de la mostra, del consentiment en l'àmbit de la protecció de dades personals, que constitueix una base de legitimació per poder tractar les dades. Així, ens podem trobar casos en què hi hagi un consentiment informat per a l'ús de la mostra, però la base de legitimació no sigui el consentiment, sinó algun dels altres supòsits que estableix la normativa.

BASES DE LIGITIMACIÓ PER A L'ÚS DE LES MOESTRES A LA RECERCA

	Requeriments	Normativa
CONSENTIMENT	<p>Règim general: permet el tractament de categories especials de dades, com les de salut, basant-nos en l'existència del consentiment. Sols el podem utilitzar quan aquest realment sigui lliure i no es consideri que hi ha un desequilibri entre les parts.</p> <p>És important ressaltar que, d'acord amb l'RGPD, l'àmbit del consentiment pot ser ampli, sense haver-se de lligar a un projecte concret, si bé, d'acord amb la interpretació del GT29, no pot donarse com un «consentiment en blanc» sense cap concreció o limitació.</p>	Articles 6.1.a) + 9.2.a) de l'RGPD, considerant 33 de l'RGPD + lletra a) de l'apartat 2 de la disposició addicional dissetena de la LOPDGDD
	<p>Consentiment anterior a l'RGPD: no hi ha cap obligació legal de tornar a recollir el consentiment sempre que les dades personals s'utilitzin per a la finalitat concreta per la qual es va prestar el consentiment o bé quan es destinin a àrees de recerca relacionades amb l'especialitat en què s'integrava el projecte inicial.</p>	Disposició transitòria sisena de la LOPDGDD
	<p>Menors d'edat: el consentiment prestat per majors de 14 anys es considera vàlid. No obstant això, si el tractament de dades pot generar alguna afectació greu en el menor d'edat, s'ha de demanar el consentiment als seus representants.</p> <p>En tot cas, si és menor de 14 anys, és necessari el consentiment dels representants, tot i que si és major de 12 anys, també s'ha de comptar amb el seu assentiment.</p>	Article 7 de la LOPDGDD
SALUT PÚBLICA	Permet el tractament de categories especials de dades, com les de salut, basant-nos en l'existència d'un interès públic en l'àmbit de la salut pública. Aquesta legitimitació s'aplica sempre que la recerca s'efectuï per autoritats sanitàries i institucions públiques competents en salut pública, i només en situacions extraordinàries, d'especial rellevància i gravetat.	Articles 6.1.e) + 9.2.i) o 9.2.j) de l'RGPD + lletra b) de l'apartat 2 de la disposició addicional dissetena de la LOPDGDD
REUTILITZACIÓ DE DADES	Es considera lícita i compatible la reutilització de dades personals amb finalitats de recerca en matèria de salut i biomèdica quan, havent-se obtingut el consentiment per a una finalitat concreta, s'utilitzin les dades per a finalitats o àrees de recerca relacionades amb l'àrea en què s'integrava científicament l'estudi inicial. Aquesta legitimitació requereix un informe previ favorable del CER.	Articles 6.1.e) + 9.2.j) de l'RGPD + lletra c) de l'apartat 2 de la disposició addicional dissetena de la LOPDGDD
PSEUDONIMITZACIÓ DE DADES	<p>A diferència del cas anterior, en què les dades no cal que estiguin necessàriament pseudonimitzades, en aquest cas podem utilitzar dades pseudonimitzades per a finalitats de recerca si es compleixen una sèrie de requisits:</p> <ul style="list-style-type: none"> ● Separació tècnica i funcional entre l'equip investigador i l'equip que pseudonimitza les dades i guarda la informació que possibilita la reidentificació del subjecte font. ● Accés a les dades pseudonimitzades per part de l'equip investigador quan es compleixin les condicions següents: <ul style="list-style-type: none"> ○ Compromís de confidencialitat i no reidentificació. ○ Mesures de seguretat específiques per evitar la reidentificació i l'accés de tercers no autoritzats. <p>No obstant això, es poden reidentificar les dades quan s'apreciï que hi ha un perill real i concret per a la seguretat o la salut d'una persona o grup de persones, o una amenaça greu per als seus drets o sigui necessària per garantir una assistència sanitària adequada.</p>	Articles 6.1.e) o 6.1.f) + 9.2.j) + 89 de l'RGPD + lletra d) de l'apartat 2 de la disposició addicional dissetena de la LOPDGDD

5.

Metodologia per a la revisió dels aspectes de protecció de dades personals per part dels comitès d'ètica de recerca

5.1. Àmbit d'aplicació i necessitat

5.1.1 Justificació de la necessitat

L'avaluació de projectes per part dels CER i CERm implica la verificació que el projecte compleix amb la normativa de protecció de dades i, més concretament, amb l'apartat h) de la disposició addicional dissetena de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals. Concretament, aquest precepte estableix el següent:

h) En el termini màxim d'un any des de l'entrada en vigor d'aquesta llei, els comitès d'ètica de la recerca, en l'àmbit de la salut, biomèdic o del medicament, han d'integrar entre els seus membres un delegat de protecció de dades o, si no n'hi ha, un expert amb coneixements suficients del Reglament (UE) 2016/679 quan s'ocupin d'activitats de recerca que comportin el tractament de dades personals o de dades pseudonimitzades o anonimitzades.

Els projectes de recerca, en compliment del principi de privacitat des del disseny i per defecte del que disposa l'article 25 del Reglament (UE) 2016/679, del 27 d'abril del 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, implica que el responsable del tractament ha de dissenyar el tractament de manera que garanteixi la privacitat de les dades i aplicar les mesures de seguretat i garanties adients.

Tanmateix, al Reial decret 1090/2015, de 4 de desembre, pel qual es regulen els assaigs clínics amb medicaments, els comitès d'ètica de la recerca amb medicaments i el Registre espanyol d'estudis clínics, estableix en el seu article 3.1 el següent:

Només es pot iniciar un assaig clínic objecte d'aquesta regulació quan el CERm i l'Agència Espanyola de Medicaments i Productes Sanitaris hagin considerat que es compleixen totes les condicions següents:

[...] d) Es respecten els drets del subjecte a la seva integritat física i mental, i a la seva intimitat, i es protegeixen les dades de caràcter personal que el concerneixen, d'acord amb la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, i la seva normativa de desenvolupament, així com amb la normativa europea vigent en la matèria.

Conseqüentment, quan els projectes arriben al CER/CERm, ja haurien de disposar des de l'inici d'una revisió que acrediti el compliment dels requeriments en matèria de protecció de dades, incloent-hi l'AIPD corresponent. No obstant això, a la pràctica és habitual que l'equip investigador ometi aquesta primera revisió i que, per tant, sigui en el moment de l'avaluació per part del CER/CERm quan s'entri a valorar el compliment del projecte pel que fa als requisits en matèria de protecció de dades.

Convé ressaltar que a Catalunya hi ha més d'una vintena de CERm, i que, en el cas de projectes multicèntrics, aquests intervenen en l'avaluació d'un mateix projecte, de manera que aquest fet suposa l'aplicació d'una diversitat de criteris d'avaluació dels aspectes de protecció de dades dels projectes. Cal insistir en el fet que el volum de projectes d'aquests CERm és variable depenent del centre, però supera amb escreix els 200 projectes anuals, comptant els projectes avaluats pels CER.

En conclusió, els recursos destinats a l'avaluació dels projectes des del punt de vista de protecció de dades no són suficients donada la complexitat que suposa la seva aplicació en l'àmbit de la recerca i el volum de projectes.

D'aquesta situació neix la necessitat de crear un **procediment àgil i que garanteixi la revisió harmonitzada del compliment de la normativa de protecció de dades en els projectes que es presentin als diferents CER/CERm**, que inclou la revisió dels aspectes derivats de l'article 35 de l'RGDP, que s'estructuren en:

- una descripció sistemàtica de les activitats de tractament previstes;
- una avaluació de la necessitat i la proporcionalitat del tractament respecte de la seva finalitat;
- i una avaluació dels riscos i les mesures previstes per afrontar-los, incloses les mesures de seguretat i mecanismes que garanteixin la protecció de les dades personals.

La tipologia de dades que es tracten en projectes de recerca en l'àmbit de la salut fa que de forma habitual concorrin elements que suposen un risc elevat per als drets i les llibertats dels titulars de les dades. Per aquest motiu, es fa necessari garantir l'aplicació d'una metodologia que permeti la revisió dels aspectes principals derivats de la normativa de protecció de dades. Així mateix, quan el **responsable del tractament ho consideri oportú**, s'ha d'aplicar la metodologia de l'Oficina del DPD de Salut per a la realització d'avaluacions d'impacte.

5.1.2 Àmbit d'aplicació

L'aplicació d'aquesta metodologia està dirigida a **recercaries, membres dels CER i CERm, coordinadors de protecció de dades i responsables del tractament**.

Per tal que la metodologia sigui efectiva, és primordial la implicació del **responsable del tractament, com a garant del compliment de la normativa de protecció de dades** en relació amb el tractament que troben dins el seu àmbit de responsabilitat, així com la implicació dels instituts de recerca, en la seva funció de gestors de la recerca.

Cada institució pot decidir a quins projectes de recerca aplica aquesta metodologia i quins projectes en queden exclosos.

L'aplicació d'aquesta metodologia s'entén sens perjudici de l'aplicació d'altres eines que les institucions considerin convenients per garantir el compliment de la normativa de protecció de dades.

5.2. Circuit i estructura de la metodologia

A continuació, es descriuen les fases del circuit.

I. Elaboració del protocol i presentació del projecte al CER/CERm

El circuit s'inicia en el moment en què un equip investigador prepara els documents per presentar-los al CER/CERm corresponent. En aquest moment, el CER/CERm, de forma addicional al protocol, ha de demanar a l'equip que empleni el document que conté la informació necessària perquè el projecte sigui avaluat des del punt de vista de protecció de dades. El document que ha de completar l'equip investigador s'adjunta com a annex 1.

Es recomana penjar l'annex 1 a la intranet del CER/CERm, així com fer una difusió inicial per facilitar-ne l'ús als equips investigadors. Addicionalment, es recomana habilitar un punt de contacte per ajudar els investigadors a resoldre els dubtes relacionats amb el projecte.

II. Avaluació del projecte per part del CER/CERm

Els avaluadors del projecte han de revisar l'annex 1 completat per l'equip investigador, i determinar els elements del projecte que consideren que suposen un risc, amb l'objectiu de demanar els aclariments pertinents. En cas de dubte, poden consultar amb l'expert de protecció de dades del CER/CERm.

III. Emissió del dictamen i coordinació amb altres CER/CERm

Una vegada el CER/CERm consideri que s'han respost correctament tots els aspectes de protecció de dades, podrà emetre'n un dictamen favorable. A continuació, es proporcionen uns criteris de consens entre els diferents CER/CERm en relació amb l'avaluació dels projectes relacionats amb la protecció de dades:

1. Tipus de dictamen. Es recomana no emetre dictàmens condicionats al compliment dels aspectes que indica l'**annex 1**, ja que la dificultat per verificar que els requeriments assenyalats s'han complert efectivament pot fer que es portin a

terme projectes sense el compliment efectiu d'aquests requeriments. Quan es detecti la necessitat de signar qualsevol tipus d'instrument jurídic, com ara un contracte d'encarregat de tractament o unes clàusules contractuals tipus, i aquests no estiguin disponibles en el moment d'emetre el dictamen, s'ha de comunicar als investigadors perquè traslladi aquesta informació als serveis jurídics corresponents. La responsabilitat del CER/CERm finalitza amb la comunicació a l'equip investigador de la necessitat de signar aquestes eines jurídiques, ja que és responsabilitat de l'equip garantir la tramitació i formalització dels requeriments jurídics del projecte.

2. Aportació d'AIPD per part del promotor. El CER/CERm ha d'analitzar els diferents tractaments de dades que es porten a terme en l'àmbit del projecte, per la qual cosa l'aplicació d'aquesta metodologia s'ha d'entendre sens perjudici de les AIPD que aportin els promotors o RT del projecte, i que determini i analitzi el tractament de dades portat a terme en l'àmbit del promotor. Quan el promotor o RT del projecte aportin una AIPD relativa al tractament que porta a terme, podrà ser acceptada pel CEI/CEIm amb independència de la metodologia utilitzada, sempre que el nivell de risc detectat sigui baix.

3. Coordinació amb altres CERm. A fi de facilitar-ne l'avaluació, quan un projecte de recerca hagi estat avaluat per un CER/CERm que hagi seguit aquesta metodologia i completat l'**annex 1**, s'ha de presumir que l'avaluació del projecte des del punt de vista de la protecció de dades és correcta, sens perjudici de la potestat del responsable del tractament de decidir sobre els seus tractaments. L'annex 1 s'ha de compartir amb els altres CER/CERm que avaluïn el projecte.

4. Convivència amb altres eines. L'aplicació d'aquesta metodologia implica la revisió dels aspectes bàsics que estableix l'article 35 de l'RGPD, però en determinats projectes — per motius de volum, projecció internacional o complexitat— el responsable del tractament, o el mateix CERm, pot considerar necessària la realització d'una AIPD, d'acord amb la metodologia d'AIPD de l'Oficina del DPD o qualsevol altra metodologia que el responsable del tractament consideri adient.

Els criteris que poden ajudar al responsable del tractament o al CERm a decidir si s'ha d'optar per fer una AIPD segons la metodologia d'AIPD de l'Oficina del DPD són els següents:

- Es tracta d'un projecte multicèntric europeu en què el centre que avalua és el centre coordinador.
- El projecte consisteix en la validació d'una eina d'intel·ligència artificial o de tecnologies biomètriques.
- El projecte consisteix en la utilització de grans volumetries de dades.

5. Reclutament. En la fase prèvia d'un projecte de recerca, l'investigador ha de revisar les històries clíniques dels malalts per decidir quins pacients són candidats i oferir-los de participar en el projecte.

Aquest procediment, que és imprescindible per reclutar els participants en el projecte de recerca, implica un accés i una segmentació de les dades de la història clínica amb finalitats no assistencials.

Qualsevol persona externa a l'assistència del pacient no hi pot accedir. Han de ser usuaris autoritzats pel centre (responsable del tractament), com ara persones de l'equip mèdic que atenen el pacient o personal de sistemes d'informació.

Aquest punt no exclou la responsabilitat del CERm d'avaluar quina forma de contacte és la menys invasiva amb la intimitat del pacient, és a dir, si el reclutament s'ha de fer durant una visita mèdica o s'admet fer una trucada per oferir participar en el projecte de recerca.

En cap cas, la metodologia substitueix l'elaboració d'una AIPD quan aquesta sigui obligatòria d'acord amb la normativa.



Annex I: Formulari a completar en matèria de protecció de dades

Identificació del projecte

Investigador principal

Data

Annex I: formulari a completar en matèria de protecció de dades

En aquest apartat, es reproduïx la proposta de formulari que han de completar els investigadors quan dissenyin el projecte per a la seva presentació al CER, juntament amb una breu explicació i exemples que faciliten la seva formalització i posterior revisió.

1. Descripció sistemàtica del tractament de les dades

Cal fer una descripció exhaustiva del tractament, ja que aquesta serà la base per avaluar la necessitat, la proporcionalitat i els riscos del tractament. Tractament de dades significa l'ús que es dona a les dades.

Descripció de les dades i motius pels quals es tracten.

En aquest apartat, s'ha de fer una breu explicació de quines dades s'utilitzen per al projecte, com es tracten, d'on provenen i cap a on van.

Exemple: en aquest projecte s'utilitzen les dades provinents del SAP per incorporar-se a una base de dades titularitat del Consorci Europeu. Aquestes dades inclouran les variables relacionades amb les cardiopaties dels participants, dades relatives als seus hàbits de vida i la zona de residència.

Aquestes dades es creuaran amb dades provinents d'altres hospitals participants en el projecte. Les dades s'anonimitzaran i seran accessibles per a tots els membres del Consorci Europeu. L'anonimització es realitzarà per part de l'empresa XXX.

Format de les dades.

En aquest apartat, s'ha d'indicar com són les dades: codificades, pseudonimitzades o anònimes. Cal explicar breument com es fa el procediment de codificació, pseudonimització o anonimització. Una dada pseudonimitzada és una dada personal a la qual se li ha substituït un atribut per un pseudònim, per la qual cosa no es pot identificar sense informació addicional. A diferència de la codificació, l'equip investigador no té accés a aquesta informació addicional. La diferència entre la pseudonimització i la codificació és que la pseudonimització la fa un tercer extern a l'equip investigador. Les dades anònimes o anonimitzades són aquelles dades que ja no poden reidentificar el titular original de les dades.

Descripció dels subjectes que intervenen en el tractament de les dades.

En aquest apartat, s'ha d'indicar quines institucions utilitzen dades en el transcurs del projecte.

En l'àmbit de protecció de dades, bàsicament distingim:

- 1.** Responsable del tractament: és qui determina la finalitat del tractament i, per tant, té la responsabilitat principal de garantir el compliment de la normativa. El responsable del tractament és el centre que realitza la recerca i/o el promotor.
- 2.** Encarregat de tractament: és qui tracta les dades en nom del responsable i ha de seguir les instruccions del responsable, i està vinculat a les finalitats i els elements de tractament que el responsable hagi inclòs. Exemple: en un assaig clínic, el promotor i el centre sanitari es constitueixen com a responsables del tractament.

Es produeixen comunicacions de dades?

Considerem que hi ha una comunicació de dades quan les dades es tracten per part d'un tercer que no té la consideració d'encarregat de tractament. Hem d'indicar si les dades surten de l'àmbit del responsable del tractament. Exemple: les dades es comunicaran a un laboratori.

- Sí
 NO

En cas afirmatiu, cal indicar on i el motiu:

Es produeixen transferències internacionals?

Es considera transferència internacional l'enviament d'aquestes dades fora de la zona econòmica europea (països de la UE + Liechtenstein, Islàndia i Noruega).

- Sí
- NO

Comentaris (si escau):

Durant quant de temps es conserven les dades?

S'ha d'indicar el nombre d'anys o un criteri que permeti determinar-ne el temps. Exemple: una vegada finalitzat el projecte de recerca, les dades es conservaran el temps necessari per respondre a les reclamacions dels participants en l'assaig.

Decisions automatitzades i intel·ligència artificial.

El tractament avalua de manera sistemàtica o exhaustiva aspectes personals de persones físiques (situació econòmica, salut, etc.) basant-se en un tractament automatitzat, com l'elaboració de perfils?

- Sí
- NO

Descripció

El tractament inclou sistemes d'intel·ligència artificial (IA)?

- Sí
- NO

Descripció

2. Necessitat i proporcionalitat

Anàlisi de la base legitimadora.

Una base legitimadora és el supòsit que ens permet utilitzar una dada personal. Per ser lícits, l'ús de dades personals ha d'estar emparat per alguna base legitimadora que recull l'article 6 de l'RGPD. Quant a les dades de salut o les dades genètiques, que són especialment sensibles, l'RGPD prohibeix la seva utilització amb caràcter general, però estableix una sèrie d'excepcions (recollides en l'article 9.2 de l'RGPD), que són, entre altres, 1. Consentiment explícit, 2. Interès públic en l'àmbit de la salut pública, i 3. Finalitats de recerca (amb el compliment de determinats requisits).

Exemple: un oncòleg decideix demanar un consentiment a tots els pacients que atén per utilitzar les seves dades amb la finalitat d'investigar en l'àmbit de les malalties oncològiques.

Trieu el motiu que justifica el tractament de les dades:

- a) La persona interessada —o la seva representació legal— ha donat el seu consentiment per al tractament de les seves dades personals, per a una o diverses finalitats específiques.
- b) El tractament és necessari per complir una missió feta en interès públic o en l'exercici de poders públics conferits al responsable del tractament en el marc de la salut pública.
- c) Les dades són recollides inicialment per a una altra finalitat i es reutilitzen per a la recerca de manera pseudonimitzada.
- d) Altres (cal descriure'ls).

Es compleix el principi de minimització i exactitud de les dades.

S'ha de verificar que únicament es tracten les dades que són necessàries per al projecte. Les dades utilitzades en un projecte de recerca han de ser sempre les mínimes adequades, pertinents i limitades. Així, només s'han de tractar les dades necessàries per aconseguir els objectius de la recerca. Les dades recaptades han de respondre a un propòsit específic, rellevant i limitat als objectius i la metodologia del projecte. La minimització de dades s'aplica a la quantitat i el tipus de dades personals recollides, però també a la manera en què es podran accedir, qui hi podrà accedir, com es podran processar i compartir, els motius pels quals s'utilitzen, així com el període de conservació.

Exemple: en un projecte de recerca podem optar entre sol·licitar l'edat del subjecte, sol·licitar un interval d'edat (per exemple, entre 30 i 40) o sol·licitar la data concreta de naixement del subjecte. En aquest sentit, per complir amb el principi de minimització de dades, hauriem d'analitzar quina informació realment necessitem.

- Sí
- NO

Comentaris (si escau):

Heu definit una estratègia o un conjunt de procediments per evitar la creació o el reforç d'un biaix injust en el sistema d'IA, tant en relació amb l'ús de dades d'entrada com en el disseny de l'algorisme?

- Sí
- NO

Heu previst la intervenció humana per avaluar el sistema d'IA, tant en la fase d'entrenament com en la fase d'aplicació?

- Sí
- NO

Heu tingut en compte la diversitat i la representativitat dels usuaris en les dades? Heu realitzat proves per a poblacions concretes o casos d'ús problemàtics?

- Sí
- NO

Heu establert processos per verificar i realitzar un seguiment dels biaixos potencials durant el desenvolupament, desplegament i ús del sistema?

- Sí
- NO

Heu assegurat que el disseny dels sistemes d'IA sigui equitatiu?

- Sí
- NO

Descripció:

Justificació:

3. Controls per garantir els drets de les persones

Deure d'informació.

En aquest punt, hem d'indicar quan es dona la informació de l'ús que fem de les dades, en el moment de recollir el consentiment o, si el projecte no requereix cap consentiment, la informació és la que es va donar en el moment inicial de recollida de les dades. En tots dos casos, hem d'informar dels aspectes que estableixen els articles 13 i 14 de l'RGPD.

Això significa que, en un projecte de recerca, cal informar cada participant de:

- 1.** La identitat del responsable del tractament de les dades.
- 2.** L'ús que es farà de les dades i el temps de conservació.
- 3.** L'exercici de drets dels participants. Cal informar sobre com podran exercir els drets de protecció de dades personals (*ARSO-POL), també el seu dret a presentar una reclamació davant l'autoritat de control si consideren que s'han vulnerat els seus drets.
- 4.** La identitat del delegat o delegada de protecció de dades. És aquella persona física encarregada de vetllar pel dret fonamental a la protecció de dades personals i supervisar el compliment de la normativa reguladora.

La recollida de dades personals inclou l'obtenció directa de la persona interessada?

- Sí
 NO

Es facilita la informació de tots els aspectes de l'article 13 de l'RGPD?

- Sí
 NO

Comentaris (si escau):

Informació a la persona interessada quan les dades procedeixen d'altres fonts

La recollida de dades personals inclou l'obtenció d'altres fonts? (no directament de la persona interessada)

- Sí
- NO

Es facilita la informació de tots els aspectes de l'article 14 de l'RGPD?

- Sí
- NO

Comentaris:

Exercici de drets.

En aquest apartat, s'ha d'explicar com s'articula l'exercici dels drets que estableix l'RGPD. L'RGPD estableix que els titulars de les dades poden exercir els drets que es detallen a continuació davant el responsable del tractament: dret d'accés, dret de rectificació, dret de supressió (dret a l'oblit), dret d'oposició, dret de limitació del tractament de dades i dret de portabilitat de les dades. Quan es redacti el full d'informació i consentiment per als participants de l'estudi, cal indicar una adreça de correu electrònic que permeti gestionar ràpidament aquest exercici de drets. Es desaconsellen adreces genèriques, per la qual cosa una bona opció pot ser posar l'adreça de l'investigador responsable (i que aquest conegui com procedir).

S'ha establert un procediment o protocol estàndard per a la gestió de sol·licituds d'exercici de drets?

- Sí
- NO

El temps de resposta és inferior a trenta dies?

- Sí
- NO

Comentaris

Dret a no ser objecte de decisions individuals automatitzades (incloent-hi l'elaboració de perfils)

Es realitza un tractament automatitzat que té efectes jurídics o altres efectes significatius per a les persones?

- Sí
- NO

Quina base legal ho permet?

- És necessari per a l'execució d'un contracte entre la persona interessada i el responsable.
- Està autoritzat pel dret de la Unió o d'un estat membre.
- La persona interessada ha donat el seu consentiment explícit

Comentaris:

Hi ha un procediment perquè les persones puguin demanar intervenció humana, expressar el seu punt de vista i impugnar la decisió?

- Sí
 NO

Comentaris

Es fa ús de categories especials de dades en el tractament automàtic?

SÍ / NO

Hi ha personal en l'organització amb la capacitat de revisar les decisions i canviar-les?

- Sí
 NO

Comentaris

En cas que se'n faci ús, quina base legal ho permet? *Marqueu amb una X.*

- La persona interessada ha donat el seu consentiment explícit.
 El tractament es fa per protegir els interessos vitals de la persona interessada o d'una altra persona.

Comentaris:

4. Riscos en la seguretat de les dades

Entorn tecnològic de tractament de les dades

On s'allotgen les dades del projecte? La base de dades està situada en els servidors de la institució (Sí) o en els servidors del promotor (No)?

En cas que les dades únicament es tractin en l'entorn del centre, si la base de dades s'allotja en els servidors de la institució es considera que s'apliquen les mesures de seguretat que el responsable del tractament ha determinat en la seva política de seguretat institucional.

- Sí
 NO

S'han establert controls d'accés apropiats per garantir que només les persones autoritzades puguin accedir a la informació del projecte?

- Sí
 NO

El desenvolupament del projecte implica algun tipus d'integració amb el sistema de gestió de pacients?

En aquest cas, es pregunta si per exemple el SAP es connecta a alguna mena d'aplicació que extreu dades.

- Sí
 NO

Els membres de l'equip investigador són conscients de les seves responsabilitats en matèria de seguretat de la informació en el tractament d'aquestes dades?

- Sí
 NO

El sistema de tractament està certificat amb l'Esquema Nacional de Seguretat (RD 311/2022) o amb l'estàndard ISO 27001 sobre seguretat de la informació?

Aquesta pregunta s'ha de consultar amb una persona experta de protecció de dades o amb sistemes d'informació.

- Sí
 NO

Es faran còpies de seguretat regulars de les dades del projecte?

Aquesta pregunta s'ha de consultar amb una persona experta de protecció de dades o amb sistemes d'informació.

- Sí
- NO

Justificació

Ús de dispositius o aplicacions

Per al desenvolupament del projecte s'utilitzen aplicacions o dispositius externs al centre i al promotor?

En aquest apartat, s'han d'indicar tots aquells tractaments que es porten a terme fora dels servidors de la institució i les mesures de seguretat que s'hi apliquen.

Exemple: les dades s'allotgen en un servidor extern del promotor.

- Sí
- NO

Per al desenvolupament del projecte s'utilitzen aplicacions o dispositius externs al centre i al promotor?

En aquest apartat, s'han d'indicar tots aquells tractaments que es porten a terme fora dels servidors de la institució i les mesures de seguretat que s'hi apliquen.

Exemple: les dades s'allotgen en un servidor extern del promotor.

- Sí
- NO

L'ús d'aquestes aplicacions o dispositius externs estan aprovats per l'àrea TIC?

En cas que hi hagi una aplicació corporativa que pugui dur a terme la mateixa funcionalitat, s'ha de fer servir segons les indicacions de la política interna d'ús de dispositius i aplicacions.

- Sí
- NO

Annex I: formulari a completar en matèria de protecció de dades

Indiqueu quins són aquests dispositius o aplicacions, així com la seva finalitat en el context del projecte.

