Contingut del protocol de recerca

Quins elements ha de tenir un protocol de recerca des del punt de vista de protecció de dades ?

El protocol és el document on s'explica com és desenvoluparà el projecte de recerca, i des del punt de vista de protecció de dades, és el document que el membre expert el Comitè d'Ètica de la Investigació disposa per avaluar si el projecte de recerca compleix amb a normativa de protecció de dades. Per aquest motiu és important que l'apartat de protecció de dades dels protocols disposin d'una forma ordenada de la següent informació:

1) Identificació de les dades i els subjectes que les tracten.
2) Identificació dels tractaments i base legitimadora dels tractaments.
3) Eines utilitzades per a tractar les dades.
4) Transferències internacionals de dades.
5) Identificació de tractaments que poden suposar un alt risc pels drets i llibertats dels participants en el projecte de recerca.
6) Contingut del full d'informació i consentiment dels participants en el projecte de recerca.

1. Identificació dels subjectes i els tractaments de dades.

Quines dades és tracten i en quin format ?

- El primer que s'ha de determinar en un protocol són les dades que es tractaran i amb quina finalitat, fent una **descripció les tipologies de dades o variables que s'utilitzaran**. En aquest punt s'haurà d'indicar el format de les dades (**anònimes, identificades o pseudonimitzades**) i si es creuen amb altres bases de dades. Si les dades són anònimes o s'han pseudonimitzada s'ha de descriure com s'ha fet aquest procediment.

EXEMPLE

Les variables necessàries per a portar a terme l'estudi són el pes, l'edat, el nivell de glucèmia o colesterol i provindran del SAP de l'Hospital. Aquestes variables es creuaran amb informació del Registre Nacional de Difunts. La informació estarà codificada.

Les variables necessàries, descrites a l'apartat x del protocol, provenen del programa PADRIS, i estan anonimitzades pel propi sistema del programa PADRIS.

La **pseudonimització**, entesa com el tractament de dades personals de manera que ja no es puguin atribuir a un interessat 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, i s'ha de distingir de **l'anonimització**, on no és possible la reidentificació, ja que a diferència d'aquesta, a les dades pseudonimitzades els hi és plenament aplicable la normativa de protecció de dades. Així també s'ha de distingir de les **dades codificades** (habitualment utilitzades en recerca), on no existeix la separació tècnica i funcional establerta a l'article 17.2.d de la LOPD-GDD.

Qui tracta dades ?

- En segon lloc s'ha de descriure qui tracta dades en el projecte, que poden ser diversos actors i portar a terme diversos rols.
- En primer lloc s'ha d'identificar l'entitat que decideix en relació al tractament de les dades, és a dir, qui és el **responsable /responsables o coresponsables del tractament**.

EXEMPLE

L'Hospital X i el Promotor actuen com a responsables del tractament en el marc d'aquest estudi observacional.

- També s'han de descriure altres subjectes que accediran a les dades o que les rebran, encara que no tinguin la consideració de responsable del tractament. En aquest punt apareix la figura de **l'encarregat de tractament**, amb qui s'haurà de subscriure el corresponent contracte (aquest punt s'ha de gestionar amb serveis jurídics de la institució).

EXEMPLE

L'empresa X, al subministrar oxigen al domicili dels pacients haurà de disposar de les seves dades per a la prestació del servei, pel que actuarà com a encarregat de tractament.

La base de dades del projecte s'allotjarà als servidors de l'empresa X, pel que actuarà com a encarregat de tractament.

- **Responsable del tractament:** la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, sol o juntament amb d'altres, determina les finalitats i els mitjans del tractament; si el dret de la Unió o dels estats membres en determina les finalitats i els mitjans del tractament, el responsable del tractament o els criteris específics per al seu nomenament els pot establir el dret de la Unió o dels estats membres.
- Quan dos o més responsables determinen conjuntament els objectius i els mitjans del tractament, se'ls considera **corresponsables del tractament.**
- **Encarregat del tractament:** la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que tracta dades personals per compte del responsable del tractament.

2. Quina és la base de legitimació per a tractar les dades i l'origen de les dades

Quin és el motiu que ens habilita a tractar les dades i d'on provenen ?

- La normativa de protecció de dades, estableix que per tractar dades personals, és necessari disposar d'un motiu que ens habiliti a tractar-les, el que el RGPD anomena base de legitimació.
- Aquesta base de legitimació pot ser el consentiment o altres, que s'expliquen a la Fitxa 4. Per a utilitzar dades per recerca, o bé disposem del consentiment del titular de les dades, o són dades pseudonimitzades, pot ser un cas de reutilització de dades o un cas d'ús de dades per part d'una autoritat en matèria de salut pública en una situació d'emergència.
- S'ha d'indicar així mateix l'origen de les dades, si provenen directament del propi titular de les dades o si s'han obtingut d'una altra base de dades.

EXEMPLE

Les variables necessàries per a portar a terme l'estudi s'han obtingut directament del participants del projecte mitjançant el seu consentiment, d'acord amb l'establert als articles 6.1.a) i 9.2.a) del RGPD.

Les variables necessàries per a portar a terme l'estudi s'han obtingut del SAP, previ procés de pseudonimització per part de sistemes d'informació de la institució, d'acord amb l'establert a als articles 6. e), 9.2. j) + 89 RGPD, així com la disposició addicional 17.2.d de la LOPD-GDD.

ATENCIÓ! Cal fer esment que no existeix una exempció d'obtenir el consentiment en matèria de protecció de dades, el que existeixen són bases legitimadores diferents al consentiment.

ATENCIÓ! Així mateix també cal tenir en compte que el tractament de dades anònimes no requereix de base de legitimació ja que no aplica la normativa de protecció de dades.

ATENCIÓ! El simple accés a la història clínica per a realitzar la selecció de pacients que participaran a un projecte de recerca és considera tractament de dades (segmentació). L'accés a la història clínica per a realitzar aquesta segmentació es considerarà lícita sempre i quan es porti a terme per l'equip mèdic que atén al pacient. Una vegada realitzada la selecció dels candidats a participar en un projecte de recerca els membres de l'equip mèdic podran iniciar el reclutament de pacients per les vies i amb les eines que aprovades pel CEIm.

3. Descripció de les eïnes utilitzades per a tractar les dades

Amb quines eines informàtiques tractem les dades ?

- El protocol cal que indiqui com és tractaran les dades, és a dir, on s'emmagatzemaran i els recursos informàtics que s'utilitzaran.
- En relació a on s'emmagatzemaran s'haurà d'indicar si es fan servir servidors propis o d'un tercer, així mateix, com si es fan servir eines d'emmagatzemament al núvol o plataformes de gestió de dades per tercers (per exemple REDCAP), i les característiques de les mateixes.
- Caldrà fer una breu descripció de les mesures de seguretat que garanteixen que les dades sols siguin accessibles a l'equip investigador, tal i com clau d'accés i passwords.
- Les eines d'emmagatzematge i intercanvi d'informació que s'utilitzin sempre han de ser les institucionals o bé verificar a través del Departament de Sistemes d'Informació que es tracten d'eines segures.

EXEMPLE

Les dades del projecte s'emmagatzemaran en servidors a la institució. Es transmetran les dades pseudonimitzades al promotor del projecte mitjançant una VPN.

Per a portar a terme el projecte s'utilitzarà la plataforma REDCAP, allotjada en els servidors de la institució, i que disposa de les mesures de seguretat determinades per la institució. Les dades s'emmagatzemen en el servidor web local on l'organització ha instal·lat el programari i, per tant, només accessible en equips que hi tinguin una connexió de confiança mitjançant VPN i credencials segures (certificats, claus RSA o contrasenyes complexes). S'ha incorporat un sistema per tal que únicament el servei de l'aplicació pugui enviar les dades al backoffice, mitjançant un firewall que únicament permeti les peticions des de les adreces IP de l'aplicació. El servidor web té habilitada la configuració de capçalera HTTP X-Frame-Options amb el valor «same-origin» per prevenir atacs de clickjacking.

ATENCIÓ! No és poden utilitzar eines d'emmagatzemament i intercanvi de dades al núvol comercials no segures com Googledrive, wetransfer, google forms, drop box, Survey Monkey,...

ATENCIÓ! Si utilitzem un servidor d'una empresa per allotjar dades del projecte, encara que estiguin codificades o pseudonimitzades, haurem de signar el corresponent contracte d'encarregat de tractament previst a l'article 28 del RGPD.

Disposem d'eines d'emmagatzematge i plataformes que es consideren segures:

- **REDCAP**. Es considera segur l'ús del REDCAP sempre que no s'utilitzi la versió en *cloud*, sinó l'allotjada en els servidors de la institució, sempre i quan disposi de les mesures de seguretat determinades per la institució. Les dades s'emmagatzemin en el servidor web local on l'organització ha instal·lat el programari i, per tant, només accessible en equips que hi tinguin una connexió de confiança mitjançant VPN i credencials segures.
- **TIXEO.** Es tracta d'una plataforma segura per a realitzar videoconferències.

4. Transferencies internacionals de dades

Quan és produeix una transferència internacional de dades ?

- Es considera transferència internacional de dades l'enviament d'aquestes fora de la zona Econòmica Europea quan no hi ha un acord que garanteixi que el país o l'entitat de destí de les dades compleixen amb els requisits mínims que la normativa europea exigeix. Podeu trobar més informació a https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales.
- S'ha de determinar l'existència de transferències internacionals de dades, així com la seva adequació a la normativa de protecció de dades. Aquesta informació s'haurà de reflectir en el full d'informació del participant al projecte de recerca.

EXEMPLE

Les dades s'enviaran a Canadà, país amb el que existeix una decisió d'adequació d'acord amb l'article 45 del RGPD.

ATENCIÓ! El Tribunal de Justícia de la Unió Europea ha invalidat el Privacy Shield, pel que les transferències realitzades a USA bastant-se en aquest instrument ja no són vàlides.

5. Identificació de tractaments que suposen un alt risc pels drets i llibertats dels titulars de les dades

Quines situacions suposen un alt risc ?

- Des del punt de vista de la normativa de protecció de dades determinades situacions és considera que suposen un alt risc pels drets i llibertats dels titulars de les dades.

  Aquestes situacions són:

  - Realització de perfilat de dades o presa de decisions automatitzades respecte participants individuals.
  - Ús d'eines d'intel·ligència artificial.
  - Utilització de tècniques d'explotació de dades amb tecnologies Big Data.
  - Utilització de sistemes de biometria.
  - Utilització de sistemes de geolocalització.

- Per aquest motiu en tot projecte de recerca s'ha de verificar si es necessita d'una avaluació d'impacte, conforme a la disposició addicional 17.2.f de la LOPD-GDD, que estableix que qualsevol projecte de recerca realitzat d'acord a l'establert a l'article 89 del RGDP requerirà la realització d'una avaluació d'impacte, sempre i quan estiguem en una de les situacions d'alt risc pels drets i llibertats dels titulars de les dades, previstes a l'article 35 del RGPD, o ens trobem en un dels supòsits previstos per les Autoritats de Protecció de Dades.

- En el marc de la recerca, serà molt freqüent la necessitat de realitzar una avaluació d'impacte, ja que es tracten dades de salut, i freqüentment els projectes de recerca contenen altres elements de risc com l'ús de tecnologies innovadores (tècniques d'intel·ligència artificial, wearables o apps, sistemes de realitat virtual, geolocalització o biometria), el tractament de col·lectius especialment vulnerable (menors, incapaços), perfilat de dades o el tractament massiu de dades, que fan necessària la realització d'una avaluació d'impacte.

- A fi d'obtenir més informació en relació a la necessitat i la forma de realitzar una avaluació d'impacte cal que consulteu al coordinador de protecció de dades de la vostra institució.

EXEMPLE

D'acord amb l'establert a l'article 35 del RGPD s'ha realitzat la corresponent avaluació d'impacte del projecte. El projecte consisteix en la validació d'una eina d'intel·ligència artificial, però d'acord amb l'anàlisi realitzat a la corresponent avaluació d'impacte no implica una decisió automatitzada, no sent d'aplicació l'establert a l'article 22.

D'acord amb l'establert a l'article 35 del RGPD, el projecte no reuneix les característiques necessàries que obliguen a la realització de la corresponent avaluació d'impacte.

- **Perfilatge i decisions automatitzades.** L'article 22 del RGPD, estableix el dret a no ser objecte d'una decisió automatitzada, sense que hi hagi cap tipus d'intervenció humana. Per determinar si hi ha participació humana, aquesta supervisió humana ha de portar-se a terme de forma que sigui significativa per a la presa de la decisió, no únicament simbòlica. S'ha de portar a terme per 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 el corresponent anàlisis. En aquestes situacions, quan es porta 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.

  Per aquest motiu, quan desenvolupem un projecte de recerca on utilitzem un algoritme de recolzament al diagnòstic, hem de fonamentar que el grau d'intervenció del metge és suficient per evitar l'aplicació de l'article 22 del RGPD.

6. Contingut del full d'informació i consentiment

Quin és el contingut del full d'informació i consentiment ?

- Quan preparem el protocol de recerca, s'ha d'incorporar al full d'informació i consentiment del participant al projecte de recerca l'apartat relatiu al tractament de les seves dades, amb el contingut establert als articles 13 i 14 RGPD.

- El participant al projecte de recerca sempre ha de ser informat del tractament de les seves dades, encara que la base legítima per al tractament de les dades no sigui el consentiment. En aquests casos la informació es pot proporcionar de forma alternativa, per exemple mitjançant la web del centre de recerca.

  El contingut mínim és:

  - **Nom del tractament.**
  - **Responsable del tractament.**
  - **Dades de contacte del delegat de protecció de dades.**
  - **Finalitats del tractament.**
  - **Base jurídica o legitimació per al tractament.**
  - **Altres destinataris a qui es comuniquen les dades.**
  - **Conservació de les dades.**
  - **Exercici de drets i dret a presentar una reclamació front l'APDCAT.**

EXEMPLE

DOCUMENT INFORMACIÓ DADES

QUE ÉS EL PROJECTE [*]

El projecte [*] ofereix [*]

COM ES TRACTARÁN LES SEVES DADES?

El Projecte, consistirà en [*], responsabilitat del [*], portat a terme amb col·laboració amb [*], en la seva condició d'encarregat de tractament.

El tractament d'aquestes dades es realitzarà en compliment del Reglament (UE) 2016/679 del Parlament Europeu i de Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa a el tractament de dades personals i a la lliure circulació d'aquestes dades, i la Llei Orgànica 3/2018, de Protecció de Dades i garantia dels drets digitals, i per això li comuniquem que vostè podrà exercir els seus drets d'accés, rectificació, supressió, oposició, limitació del tractament i portabilitat de dades, front [*] com a responsable del tractament amb NIF [*] i domicili a [*], mitjançant l'adreça de correu electrònic [*]. Pot contactar amb el Delegat de Protecció de Dades a través de [*].

Així mateix, l'informem del seu dret a presentar una reclamació davant de l'Autoritat Catalana de Protecció de Dades front qualsevol actuació del Departament de Salut que consideri que vulnera els seus drets.

Les seves dades seran tractades exclusivament amb les finalitats [*], de conformitat amb l'article 6.1, 9.2. [*], i la Disposició Addicional 17 2 [*], de la Llei Orgànica 3/2018, de Protecció de Dades i garantia dels drets digitals, per [*], i es conservaran durant el temps necessari per a la realització del projecte.

[*], tindrà accés a les dades de forma pseudonimitzada, amb l'única i exclusiva finalitat de portar a terme l'estudi de [*], havent-se adoptat mesures de seguretat específiques per evitar la reidentificació i l'accés de tercers no autoritzats. No es preveuen transferències internacionals de dades [*], però en cas que es produïssin, serà únicament a països que garanteixen l'adequat compliment de la normativa de protecció de dades per existir una decisió d'adequació o qualsevol altre mecanisme legalment habilitat.

Per a més informació pot contactar a […]

7. Proposta de formulari pel protocol

1) Dades del projecte:

- El projecte tracta dades personals: Sí / No
- En cas de resposta afirmativa:
  - ☐ Quines dades es tracten:
    - Conté identificadors personals (incloent les inicials dels pacients o la data completa de naixement)? Sí / No
      - la utilització de dades anònimes en origen (p.ex. PADRIS)
      - utilització de dades pseudonimitzades per un tercer amb separació tècnica i funcional (com la DOSI)
      - l'accés a la història clínica del pacients per la recollida de dades
  - ☐ Qui les tracta: Responsable/Coresponsables
  - ☐ Comunicacions: Encarregats, ...

2) Legitimació per al tractament de dades i origen:

- S'ha previst sol·licitar al pacient el consentiment per al tractament de les seves dades amb finalitats de recerca? Sí / No
- Si no s'ha previst sol·licitar el consentiment, justificar els impediments existents (recordeu que el fet que el projecte sigui retrospectiu o merament observacional no eximeix per sí mateix de l'obligació de sol·licitar el consentiment).
- Si no s'ha previst sol·licitar el consentiment, quin dels següents supòsits seria la base legitimadora per al tractament de les dades en el projecte? (marcar el que més s'aproximi):
  - ☐ Supòsit 1 (p. ex. estudis epidemiològics d'interès general en situacions d'emergència autoritzats per l'Autoritat Sanitària)
  - ☐ Supòsit 2 (p .ex. dades pseudonimitzades)
  - ☐ ….
  - ☐ …
- Origen de les dades:
  - ☐ Interessat
  - ☐ ...

3) Tractament de les dades, indiqueu:

- Eines utilitzades
  - ☐ S'utilitzen dispositius electrònics? Sí /No
    - Lloc on es desarà informació
  - ☐ On s'ubica el servidor?
  - ☐ S'utilitzen bases de dades compartides de forma telemàtica amb altres centres o investigadors? Sí /No
- Descripció de les mesures de seguretat:
  - ☐ Indicació de mesures per evitar l'accés indegut de tercers no autoritzats
  - ☐ Altres mesures de seguretat

4) Hi haurà transferència internacional de dades?

- Sí /No. Mecanisme per efectuar la transferència: Decisió d'adequació

5) Aspectes per a projectes amb usos avançats de les dades

- Usos avançats
  - ☐ Realització de perfilat de dades o presa de decisions automatitzades respecte participants individuals.
  - ☐ Ús d'eines d'intel·ligència artificial.
  - ☐ Utilització de tècniques d'explotació de dades amb tecnologies Big Data.
  - ☐ Utilització de sistemes de biometria.
  - ☐ Utilització de sistemes de geolocalització.
- Mesures de seguretat adoptades per aquestes actuacions
- Recordatori: Necessari adjuntar Avaluació d'Impacte