IdISSC
INSTITUTO de
INVESTIGACIÓN SANITARIA
Hospital Clínico San Carlos

# Investigación Biomédica y Datos Personales

*Formación práctica: tratamiento de Datos Personales en Investigación Biomédica*

Hospital Clínico San Carlos
FUNDACION PARA LA INVESTIGACIÓN BIOMÉDICA Hospital Clínico San Carlos
Comunidad de Madrid
UNIVERSIDAD COMPLUTENSE MADRID
POLITÉCNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

INSTITUTO de INVESTIGACIÓN SANITARIA Hospital Clínico San Carlos

# 1. Conceptos fundamentales del RGPD

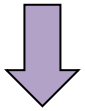
## *Derecho Fundamental*

Protección de datos de carácter personal como **Derecho Fundamental:**

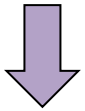
- Europa: Recogido en art. 8.1 Carta de los DDFF de la UE y art. 16.1 TFUE - *Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*

- España: Recogido en Constitución Española, art. 18.4:

*"La ley limitará el uso de la informática para **garantizar el honor y la intimidad personal** y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*



Búsqueda de protección de la privacidad e intimidad de las personas físicas durante el tratamiento de sus datos.



Necesario legislación que reconozca derechos a las personas e imponga obligaciones a quienes traten sus datos personales.

# 1. Conceptos fundamentales del RGPD

*Contexto Normativo*

**Normativa Vigente:**

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (**RGPD**, o GDPR por sus siglas en inglés).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (**LOPDgdd**).

**Ámbito aplicación normativa**:

- Objetivo: **personas físicas** en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos;
- Material: tratamiento de **datos personales**, automatizados o no automatizados;
- Territorial:
  - RGPD: responsables o encargados del tratamiento establecidos en la Unión Europea + responsables y encargados del tratamiento no establecidos en la Unión Europea, siempre que realicen tratamientos derivados de una oferta de bienes o servicios destinados a interesados que se encuentren en UE o como consecuencia de una monitorización y seguimiento de su comportamiento;
  - LOPDgdd: normativa nacional.

# 1. Conceptos fundamentales del RGPD

*Fundamentos*

**Datos personales:** toda información sobre una persona física identificada o identificable («el interesado»). **Identificable**: persona cuya identidad pueda determinarse, directa o indirectamente a través de:

- elementos propios de la identidad física, fisiológica, genética, psíquica, económica y cultural o social; ó
- por identificadores, como, por ejemplo, el nombre, un número de identificación, datos de localización o un identificador en línea

Estaremos ante datos personales si podemos determinar la identidad de esa persona mediante singularización o inferencia. Ejemplo: en un grupo de personas, conocemos suficiente información de un sujeto (edad, género, estatura, etc.) como para identificarlo.

**Interesado:** persona física de la cual se tratan los datos. Es el propietario de los datos y respecto al que se debe poner el foco → protección de los derechos y libertades del interesado.

**Tratamiento**: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

**Sujetos intervinientes – dependiendo de la forma que sujeto realice el tratamiento de datos:**

- **Responsable del Tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios** del tratamiento → tomará las decisiones sobre qué datos tratar, de quién, para qué finalidad, dónde conservarlos, qué medidas implementar para protegerlos, etc. → debe cumplir las obligaciones impuestas por la normativa para garantizar los derechos del interesado (por ejemplo: informar sobre el tratamiento de los datos, incluyendo en el consentimiento informado de los participantes del proyecto).

  Normalmente, en proyectos de investigación, FIBHCSC únicamente asumirá esta figura cuando sea Promotor y decida sobre la finalidad y uso de los datos.

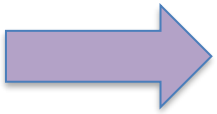
- **Encargado del Tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que **trate datos personales por cuenta** del responsable del tratamiento → trata los datos bajo las instrucciones del responsable, no podrá utilizar los datos para otras finalidades ni para las suyas propias.

  En proyectos de investigación, la CRO será encargado.

Responsable y encargado de tratamiento deben firmar el **contrato de encargado de tratamiento**

**Sujetos intervinientes – dependiendo de la forma que sujeto realice el tratamiento de datos:**

- **Corresponsable:** cuando **dos o más** responsables determinen **conjuntamente los objetivos y los medios** del tratamiento serán considerados corresponsables del tratamiento → los dos corresponsables decidirán cómo llevar a cabo ese tratamiento. **Ejemplo**: Promotor y el Centro si deciden conjuntamente.



Corresponsables deben firmar el **acuerdo de corresponsables**.

- ***Responsables respectivos***: concepto no incluido en la normativa vigente. Cada uno es responsable de sus respectivos tratamientos (finalidades distintas), correspondiendo a cada uno de ellos las obligaciones derivadas de su actividad.

**Ejemplo:** El Centro es el responsable de todos los datos que figuren en la historia clínica y que puedan identificarle y el Promotor de los que se recogen en este estudio de forma codificada (seudonimizada).

¿Cuándo hay una responsabilidad respectiva de la FIBHCSC y el Hospital? En el caso en el que la FIBHCSC sea responsable del tratamiento de los datos del estudio (datos personales), y el Hospital sea responsable del tratamiento de los datos asistenciales de los pacientes, por lo que la finalidad con la cual los datos de los pacientes serán tratados es diferente, y ha sido/será determinada de forma independiente.

**Principios relativos al tratamiento** (art. 5 del RGPD):

- Datos personales tratados de manera **lícita, leal y transparente**. Lícito si:
  - Interesado ha dado su consentimiento (corresponde al responsable demostrar que interesado dio su consentimiento) – condiciones para prestar consentimiento;
  - Tratamiento necesario para:
    - Ejecución de un contrato
    - Obligación legal
    - Proteger intereses vitales del interesado o de otra persona física
    - Interés público
    - Satisfacción de intereses legítimos perseguidos por responsable o tercero
- Limitación de la **finalidad**: recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines;
- **Minimización** de datos: adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados;
- **Exactitud** de los datos;
- Limitación del **plazo de conservación**: identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento;
- **Integridad y confidencialidad** de los datos personales;
- **Responsabilidad proactiva**: Responsable debe cumplir con el RGPD y debe ser capaz de demostrarlo.

# 2. Datos seudonimizados VS datos anonimizados: la importancia de conocer la diferencia

*Datos seudonimizados*

**Datos seudonimizados NO es lo mismo que datos anonimizados** → importante diferenciarlo para determinar si aplica la normativa de protección de datos personales (identificabilidad).

**Seudonimización**: tratamiento de datos de carácter personal, de manera que ya no puedan atribuirse a un interesado sin utilizar información adicional.

- Información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable:
- Separar el dato identificativo del resto de los datos;
- Se trata de una medida técnica que reduciría el vínculo existente entre los datos de carácter personal y la persona a la que identifican;
- Codificación;
- Proceso seudonimización requiere cumplimiento de normativa de protección de datos.

↓

Datos seudonimizados **SON datos personales** → para ambas partes, incluso para la parte que no tiene la "llave" para reidentificar.

↓

Aplica la normativa de protección de datos personales, deberán tenerse en cuenta las obligaciones, responsabilidades, etc.

## 2. Datos seudonimizados VS datos anonimizados: la importancia de conocer la diferencia

*Datos anonimizados*

**Anonimización:** tratamiento de datos, de manera que ya no resulte posible (nivel de reidentifibalidad dependiendo de tecnología disponible, tiempo, coste, etc.) atribuir a una persona física identificada o identificable.

- Datos anonimizados no permiten identificar de ninguna manera al sujeto porque no hay vínculo entre identificador y el sujeto → En ningún caso será posible la vinculación del dato con la persona a la que hubiese identificado;
- Imposible volver a identificar a la persona a través de ese dato;
- Información que no guarda relación con una persona física identificada o identificable;
- Informacion agregada, estadística;
- Proceso anonimización requiere cumplimiento de normativa de protección de datos.

↓

Datos anonimizados **NO son datos personales**

↓

NO Aplica la normativa de protección de datos personales → deberá tenerse en cuenta si aplica otra normativa

# 2. Datos seudonimizados VS datos anonimizados: la importancia de conocer la diferencia

*Controversia e importancia*

**Controversia seudonimización VS anonimización:**

- La definición teórica es clara, pero, hoy en día es complejo, en el campo de la investigación y por la tecnología que existe, concluir que un dato está anonimizado (salvo datos agregados).

- Aunque no pueda unir el conjunto de información con el dato identificativo, el conjunto de la información sí permite singularizar o inferir a la persona (datos seudonimizados).

**Importancia** de conocer la diferencia:

- Datos seudonimizados: entran dentro de ámbito de aplicación de la normativa de protección de datos personales → deben determinarse las responsabilidades y cumplirse todas las obligaciones establecidas en el RGPD y la LOPDgdd → asesoramiento del DPO de la FIBHCSC.

- Datos anonimizados: no entran dentro de ámbito de aplicación del RGPD ni LOPDgdd → no asesoramiento del DPO.

# 2. Datos seudonimizados VS datos anonimizados: la importancia de conocer la diferencia

*Controversia e importancia*

**Ejemplo**: proyecto de investigación en el que se va a recabar determinada información de los participantes (edad, género, estatura, origen racial, peso, código postal de residencia, código de identificación del paciente) pero no se recabaran datos identificativos (nombre, apellidos, DNI). Estaremos ante tratamiento de datos seudonimizados por lo que aplicarán todas las **obligaciones** de la normativa:

- Valorar el tratamiento de datos que se va a realizar;
- Determinar que figura (responsable, encargado, etc) se va a ocupar respecto a esos datos;
- Principios de tratamiento de tales datos;
- Licitud del tratamiento;
- Informacion relativa al tratamiento a facilitar al interesado;
- Aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo;
- Firmar los contratos de encargado de tratamiento/corresponsabilidad/otros, en su caso;
- Privacidad desde el diseño y por defecto;
- Atender ejercicios de derecho del interesado ;
- Etc.

# 2. Datos seudonimizados VS datos anonimizados: la importancia de conocer la diferencia

*10 malentendidos relacionados con la anonimización - AEPD*

## Equívoco 1. «La seudonimización es lo mismo que la anonimización».

Realidad: «La seudonimización no es lo mismo que la anonimización»

## Equívoco 2. «El cifrado es anonimización».

Realidad: El cifrado no constituye una técnica de anonimización, pero puede ser una buena herramienta de seudonimización.

## Equívoco 3. «Los datos siempre pueden anonimizarse».

Realidad: No siempre es posible reducir el riesgo de reidentificación por debajo de un umbral definido de forma previa y mantener, al mismo tiempo, la utilidad de un conjunto de datos para un tratamiento específico.

## Equívoco 4. «La anonimización es permanente».

Realidad: Existe un riesgo de que ciertos procesos de anonimización puedan revertirse en el futuro. Las circunstancias pueden cambiar a lo largo del tiempo y los nuevos avances técnicos y la disponibilidad de información adicional pueden poner en peligro los procesos de anonimización previos.

## Equívoco 5. «La anonimización siempre reduce la probabilidad de reidentificación de un conjunto de datos a cero»

Realidad: El proceso de anonimización y la forma en que se aplique tendrán una influencia directa en la probabilidad de riesgos de reidentificación.

# 2. Datos seudonimizados VS datos anonimizados: la importancia de conocer la diferencia

*10 malentendidos relacionados con la anonimización - AEPD*

## Equívoco 6. «La anonimización es un concepto binario que no puede medirse»

Realidad: El grado de anonimización puede analizarse y medirse.

## Equívoco 7. «La anonimización puede automatizarse totalmente»

Realidad: Es posible utilizar herramientas automáticas durante el proceso de anonimización, pero, dada la importancia del contexto en la evaluación de dicho proceso, la intervención del experto humano es necesaria.

## Equívoco 8. «La anonimización inutiliza los datos»

Realidad: Un proceso de anonimización adecuado mantiene la funcionalidad de los datos para un fin determinado. – En investigación biomédica dependerá del caso concreto, ya que puede quedar mermado el fin detal investigación.

## Equívoco 9. «Seguir un proceso de anonimización que otros utilizaron con éxito hará que nuestra organización obtenga resultados equivalentes»

Realidad: Los procesos de anonimización deben adaptarse a la naturaleza, el alcance, el contexto y los fines del tratamiento, así como a los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas.

## Equívoco 10. «No existe un riesgo ni interés alguno en saber a quién se atribuyen estos datos»

Realidad: Los datos personales tienen un valor en sí mismos, para los propios individuos y para terceros. La reidentificación de un individuo podría tener una repercusión grave en lo relativo a sus derechos y libertades.

*Fuente: Agencia Española de Protección de Datos 10 Malentendidos relacionados con la anonimización*

**Casos prácticos en materia de investigación aplicados al tratamiento de datos personales**.

Hasta ahora hemos hablado de conceptos generales que son fundamentales conocer para poder aplicarlos a **supuestos prácticos** que se dan en el día a día de la FIBHCSC, como los que vamos a exponer a continuación.

Los supuestos en los que normalmente nos encontramos, desde el punto de vista de protección de datos, cuando revisamos un proyecto de investigación (independientemente de que se trate de un EECC, EEOO, etc.), siempre desde el punto de vista de la FIBHCSC:

- ❑ **FIBHCSC actúa en calidad de mero gestor económico del proyecto de investigación.**
- ❑ **FIBHCSC actúa en calidad de Promotor.**
- ❑ **FIBHCSC actúa como encargado del tratamiento.**
- ❑ **En el proyecto participan uno o varios empleados de la FIBHCSC tratando datos de carácter personal.**
- ❑ **Cesiones de datos y muestras.**

A continuación, vamos a analizar cada uno de los supuestos anteriores desde la siguiente perspectiva:

- ✓ Papel de los implicados, relación entre ellos y documentación que deben firmar.
- ✓ Tratamiento de datos personales de los pacientes y voluntarios participantes en el proyecto.

## ❑ FIBHCSC actúa en calidad de mero gestor económico del proyecto de investigación

En este caso, la FIBHCSC no tratará datos personales de los pacientes ni voluntarios participantes en el proyecto, por lo menos no datos relacionados con la investigación. Como gestor económico del proyecto, la FIBHCSC podrá tratar datos económicos de pacientes con la única finalidad de realizarles un reembolso de gastos, si fuera el caso.

Si la FIBHCSC actúa como **mero gestor económico**, será porque el Hospital ha iniciado un proyecto de investigación con un Promotor, y ellos asumirán la responsabilidad del tratamiento de los datos de los pacientes y voluntarios participantes en el proyecto, determinando si actúan como responsables del tratamiento respectivos o corresponsables, dependiendo del proyecto de investigación concreto ante el que nos encontremos.

Entre Hospital y Promotor se deberá firmar un acuerdo de corresponsabilidad en caso de resultar corresponsables del tratamiento respecto a los datos de los datos pacientes y voluntarios.

Normalmente, será en el Protocolo dónde se definirá el papel de las partes y las funciones que ejerzan en el proyecto, y de ahí se podrá extraer la responsabilidad de éstos desde el punto de vista de protección de datos. Siendo los DPOs de ambas entidades los que determinen este aspecto.

- **FIBHCSC actúa en calidad de Promotor.**

En este caso, la FIBHCSC si actúa como Promotor y además decide sobre la finalidad y uso de los datos personales de los pacientes y voluntarios participantes en el proyecto, actuará en calidad de **responsable del tratamiento** desde el punto de vista de protección de datos.

Si la FIBHCSC es Promotor del proyecto y el Hospital también participa en dicho proyecto, o cualquier Centro, se deberá determinar, igual que en el caso anterior, si actúan como responsables del tratamiento respectivos o corresponsables, dependiendo del proyecto de investigación concreto ante el que nos encontremos.

Entre Hospital y Promotor (FIBHCSC en este caso) se deberá firmar un acuerdo de corresponsabilidad en caso de resultar corresponsables del tratamiento respecto a los datos de los datos pacientes y voluntarios.

Normalmente, será en el Protocolo dónde se definirá el papel de las partes y las funciones que ejerzan en el proyecto, y de ahí se podrá extraer la responsabilidad de éstos desde el punto de vista de protección de datos. Siendo el DPO de la FIBHCSC (Alaro) junto con el DPO del Hospital, o el Centro que corresponda, los que determinen este aspecto.

- **FIBHCSC actúa como encargado del tratamiento.**

En este caso, la FIBHCSC actuaría como encargado del tratamiento en un proyecto de investigación si el propio Hospital o un tercero le contrata para prestar servicios de Monitorización, Farmacovigilancia, Tareas de apoyo a investigadores y otros, Procesamiento de muestras/datos, Análisis genéticos rembolsos/compensaciones pacientes, Gestión programas formación, etc. Aquí la FIBHCSC **no decidirá sobre la finalidad y uso** de los datos, sino que seguirá las instrucciones del Hospital o tercero que le contrate para la realización de esas tareas.

Entre FIBHCSC y Hospital, o tercero que contrate esas tareas, se deberá firmar el correspondiente contrato de encargado de tratamiento.

Normalmente, será en el Protocolo dónde se definirá el papel de las partes y las funciones y tareas que ejerzan y desarrollen en el proyecto, y de ahí se podrá extraer la responsabilidad de éstos desde el punto de vista de protección de datos.

- **En el proyecto participan uno o varios empleados de la FIBHCSC tratando datos de carácter personal.**

Este caso puede ser más **complicado** de detectar. Si la FIBHCSC, actuando o no como gestor económico, cuenta con empleados propios que participan en el proyecto (no empleados del Hospital, porque entonces lo que indicamos a continuación afectará al Hospital, no a la FIBHCSC).

En este caso, será fundamental determinar el papel que juegan los empleados en el tratamiento de los datos de los pacientes y voluntarios participantes en el proyecto:

- ¿deciden sobre la finalidad y uso de los datos? → SÍ, responsable del tratamiento
- ¿actúan por cuenta de un tercero como pudiera ser el Hospital o el Promotor, es decir, según sus instrucciones porque, por ejemplo, tienen encomendada una tarea concreta? → Sí, encargado del tratamiento.

Respecto a la documentación a firmar en este caso concreto, dependiendo del papel de la FIBHCSC de responsable o encargado se firmará una documentación u otra, teniendo en cuenta los puntos anteriores ya desarrollados.

## ❑ Cesiones de datos y muestras.

Analizamos este caso por separado, para explicar qué ocurre en aquellos proyectos de investigación en los que se produce una cesión de datos y/o muestras.

En este caso, habrá dos figuras, el **cedente** de los datos y/o las muestras (el que las "transfiere") y el **cesionario** de los mismos (el que las "recibe"). El papel de la FIBHCSC en este caso concreto puede ser uno u otro indistintamente, si bien hay que tener en cuenta que, desde el punto de vista de protección de datos, se recomienda firmar un contrato de cesión entre ambas entidades (cedente y cesionario).

Para la cesión de muestras (y datos asociados, aunque estén codificados) de un cedente a un cesionario será necesario informar al paciente o voluntario que participa en el proyecto, y, cuando proceda, solicitarle el consentimiento.

Cuando la FIBHCSC es cesionaria de los datos, además de firmar el contrato de cesión, recomendamos que requiera al cedente de la evidencia de haber recabado el consentimiento (cuando proceda) y, en todo caso, de haber informado a los pacientes o voluntarios de la comunicación de sus datos a la FIBHCSC.

## Aspectos controvertidos en los proyectos de investigación

*La determinación del tratamiento de datos personales:*

Se tiende a indicar que no se tratan datos personales en los proyectos de investigación porque no se puede identificar al paciente (ya comentado al comienzo de la exposición). Sin embargo, en la mayoría de los casos, ya hemos visto que sí se tratan datos personales de manera seudonimizada.

Por lo que es muy importante que todos los investigadores tengan en cuenta la diferencia, explicada anteriormente, entre datos seudonimizados y anonimizados.

*Especial referencia al interesado (paciente o voluntario):*

El interesado es el centro de todo lo que hemos estado hablando hasta ahora. A estas alturas ya sabemos que el interesado cuyos datos se van a tratar con fines de investigación son los pacientes o voluntarios inscritos en el proyecto de investigación. Todos los puntos que hemos ido desarrollando anteriormente, tanto los conceptos clave, como el papel de las partes, como la documentación a firmar entre ellas, es fundamental para proteger los derechos y libertades de los pacientes y voluntarios inscritos.

## Aspectos controvertidos en los proyectos de investigación

*FIBHCSC vs Hospital (entidades distintas):*

Se tiende a tratar indistintamente a la FIBHCSC y al Hospital en términos de investigación. Es fundamental determinar que cada una de estas entidades, tiene personalidad jurídica propia y su propio CIF, por ello cada entidad juega un papel diferente y tiene sus propias responsabilidades en los proyectos, tal y como hemos ido viendo hasta el momento.

Así mismo, cada entidad cuenta con su propio Delegado de Protección de Datos (DPO) que asesora en esta materia a cada una de las entidades:

FIBHCSC:
Alaro Avant, S.L.
dpo.fibclinicosancarlos@alaroavant.com

Hospital:
Secretaría del Comité Delegado de Protección de Datos. Consejería de Sanidad de la Comunidad de Madrid
protecciondedatos.sanidad@madrid.org

**Diferentes base legítimas para el tratamiento de datos personales con fines de investigación biomédica**

(*Disposición Adicional 17ª de la Ley Orgánica 3/2018, apartado segundo*).

Cuando los proyectos revistan un evidente interés para la salud pública o de terceros, el consentimiento puede ceder:

- no consentimiento en situaciones de excepcional relevancia y gravedad para la salud publica (incluso manteniéndose los datos de identificación del sujeto fuente);

- reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial;

- no consentimiento siempre que:
  - los datos seudonimizados;
  - separación técnica y funcional entre quien realice la investigación y quien seudonimice;
  - confidencialidad.

**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**

Tratar datos de salud con la función de prevenir y luchar en un escenario epidémico o pandémico no persigue un fin discriminatorio.

Informe sobre Big Data en salud de 2017 (Comité Internacional de Bioética (IBC) de la UNESCO): el Big Data puede considerarse ya un bien común de la humanidad, siempre que no sea a costa de vulnerar el derecho que cada individuo tiene a sus datos personales.

Importancia:

i) Del origen legítimo de los datos;
ii) Interés muy relevante para la salud de la colectividad;
iii) Garantías suficientes como la seudonimización;
iv) Fijar periodos de conservación de los datos.

IdISSC INSTITUTO de INVESTIGACIÓN SANITARIA Hospital Clínico San Carlos

# Preguntas y aclaraciones

## Muchas gracias por su atención

**Natalia Olivares**
**Sarai Nieto**