LA PROTECCIÓN DE DATOS EN INVESTIGACIÓN CON SERES HUMANOS

1.- FINALIDAD

El presente documento pretende ayudar a conseguir el cuidado que debemos a los participantes en los proyectos de investigación en cuanto a la protección de su intimidad, privacidad y libertad, promoviendo la confidencialidad y el cumplimiento de la legalidad vigente. Debemos tener en cuenta siempre que el uso de datos personales en investigación es responsabilidad de quien investiga y es su deber proteger a quienes han accedido a ser sujetos de investigación; tanto en la investigación que requiere el uso de datos personales, como en la que se necesitan muestras biológicas humanas o de la participación directa de personas voluntarias.

Teniendo en cuenta lo anterior hemos de señalar que la protección de datos personales obedece a la voluntad de proteger la libertad y la vida privada de las personas lo que origina que sea una tarea éticamente valiosa y que se ha plasmado en leyes concretas.

2.- NORMATIVA DE REFERENCIA

Las referencias normativas que se han tenido en cuenta para realizar el presente documento son:

- 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), plenamente aplicable desde el 25 de mayo de 2018
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.
- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
- Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación
- Ley 14/2007 de 3 de julio, de Investigación Biomédica
- Ley de Autonomía del Paciente 41/2002

3.- JUSTIFICACIÓN JURÍDICA

El 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) extiende su protección, tal y como establece su artículo 1.2, a los derechos y libertades fundamentales de las personas físicas y,

en particular, su derecho a la protección de los datos personales, definidos en su artículo 4.1 como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."

Asimismo, el artículo 4.1 define "tratamiento" como "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".

Por lo tanto, cualquier Proyecto de Investigación de la especialidad que sea en la medida que contiene datos personales relativos a personas físicas, queda sometido a lo dispuesto en el RGPD.

4.- DATOS DE CARÁCTER PERSONAL

Entendemos por **DATOS DE CARÁCTER PERSONAL**, toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente.

Por tanto, dato personal es cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo sobre personas físicas identificadas o identificables. Las informaciones que hacen identificable a alguien son aquellas sobre su identidad física, fisiológica, económica, cultural, política, educativa, religiosa, etc. que permiten saber quién es la persona de la que procede la información.

Existen distintos tipos de datos de carácter personal que podemos clasificar de la siguiente manera:

1.- Datos especialmente protegidos: Ideología, afiliación sindical, religión, creencias, origen racial o étnico, salud, vida sexual, datos genéticos y biométricos (Art.9 del RGPD) así como datos relativos a condenas e infracciones penales (Art. 10 del RGPD). De los que hablaremos más detenidamente.

2.- Datos identificativos: DNI, dirección postal o electrónica, imagen, voz, nº Seguridad Social o Mutualidad, teléfono, fax, marcas físicas, nombre y dos apellidos, firma o huella, firma electrónica, tarjeta sanitaria.

3.- Datos relativos a las características personales: Datos de estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas.

4.- Datos relativos a las circunstancias sociales: Características de alojamiento, vivienda, situación familiar, propiedades, posesiones, aficiones y estilos de vida, pertenencia a clubes y asociaciones, licencias, permisos y autorizaciones.

5.- Datos académicos y profesionales: Formación, titulaciones, historial del estudiante, experiencia profesional, pertenencia a colegios o asociaciones profesionales.

6.- Detalles de empleo: Profesión, puestos de trabajo, datos no económicos de nómina, historial del trabajador.

7.- Datos que aportan Información comercial: Actividades y negocios, licencias comerciales, subscripciones a publicaciones o medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.

No obstante, debemos prestar especial atención a las **CATEGORÍAS ESPECIALES DE DATOS. (DATOS SENSIBLES O ESPECIALMENTE PROTEGIDOS).** Algunos de los datos personales son especialmente sensibles por revelar circunstancias o información de las personas sobre su esfera más íntima y personal. Se trata de datos que, debido a su incidencia especial en la intimidad, las libertades públicas y los derechos fundamentales de la persona titular de los mismos, hace necesario que se establezca una mayor protección que con el resto de los datos personales (RGPD art. 9 y considerandos 51-56). Forman parte de esta categoría de datos personales:

- Afiliación sindical.
- Religión u opiniones religiosas.
- Creencias o creencias filosóficas.
- Origen racial o étnico.
- Datos relativos a la salud.
- Vida u orientación sexuales.
- Violencia de género y malos tratos.
- Datos genéticos.
- Datos biométricos.
- Datos relativos a condenas y delitos penales.
- Datos relativos a sanciones administrativas.

Se deben aplicar una serie de medidas de seguridad en el tratamiento de estos datos:

- Cifrado de los datos en su comunicación y almacenamiento
- Registro de accesos, con fecha y personal que accedió
- Elaboración de una lista de personas autorizadas
- Establecer un procedimiento seguro para su tratamiento

En los proyectos de investigación, es frecuente utilizar todo tipo de datos sensibles, dado que se investiga en ciencias biológicas, biomédicas, técnicas, sociales, jurídicas, ciencias de la educación, trabajo social y de la conducta. Pero son especialmente delicados los siguientes:

DATOS RELATIVOS A LA SALUD. Todos aquellos que revelan información sobre el estado de salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria. De hecho, son datos de salud las informaciones relativas a enfermedad, discapacidad, riesgo de padecer enfermedades, tratamientos clínicos, estado fisiológico o biomédico, etc., independientemente de que la fuente sea su historia clínica o un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro, o incluso información transmitida por el propio participante en el proyecto de investigación.

No podemos perder de vista que, para los tratamientos de recogida, uso, conservación, etc. que vayas a hacer de esta información, la normativa en protección de datos se complementa, entre otras muchas, con la Ley de Autonomía del Paciente 41/2002, que regula los derechos y obligaciones en materia de información y documentación clínica y que incluyen comunicación, toma de decisiones, consentimiento informado, acceso a la historia clínica, etc.

DATOS GENÉTICOS. Datos específicos de salud que identifican la información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos.

DATOS BIOMÉTRICOS. Informaciones sobre las características físicas, fisiológicas o conductuales de una persona, obtenidas con técnicas específicas como imágenes faciales, datos dactiloscópicos, etc. que permiten o confirman la identificación única de dicha persona (RGPD. art. 4 .14).

DATOS DE MENORES. En principio no son datos sensibles, pero en la normativa se enuncia que debido a su condición de vulnerabilidad hay que tratar sus datos como tal, ya que estas personas pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes a la recogida y la utilización de sus datos y es responsabilidad de la persona que los recoge evitar que sean vulnerados.

Por ejemplo y a modo orientativo se considera que si los datos que se van a solicitar pueden generar al menor alguna tensión grave o afectación se consideraría una investigación invasiva y se tendría que pedir consentimiento a los representantes legales (padres o tutores) y asegurarte de que, a partir de los 12 años, además, el menor asiente. Cuando los datos no son de ese tipo solo se necesita la autorización de los representantes legales en los menores de 14 años, en el caso de mayores de 14 años son ellos mismos los que autorizan o no.

DATOS DE PERSONAS DE COLECTIVOS EN SITUACIÓN DE ESPECIAL VULNERABILIDAD. Es preciso que se tenga también un cuidado especial si el proyecto de investigación implica el uso de datos de personas de colectivos en situación de especial vulnerabilidad, como menores (ya citados), discapacitados, ancianos, personas con riesgo de exclusión social, personas en situaciones políticas comprometidas, inmigrantes sin papeles, prostitución, presos, etc.

Los datos de carácter personal pertenecen a la persona física titular de los datos.

5.- TRATAMIENTOS DE DATOS PERSONALES

Se denomina tratamiento de datos a cualquier actividad en la que estén presentes datos de carácter personal, o que, no siendo personales, su agrupación identifica a una persona ya se realice de manera manual o automatizada, total o parcialmente.

Se considera tratamiento de datos la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, su difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción de dichos datos. Según establece el art. 4 del RGPD

En una actividad de investigación por norma general se puede tener que incluir uno o varios tratamientos de datos personales. Por ejemplo:

- Siempre se va a tratar la información sobre los miembros del propio equipo investigador (datos personales).
- La gestión de la información solicitada a los participantes (recogida, archivo y utilización), la seudonimización, codificación o disociación, la conservación de los documentos escritos de consentimiento informado, etc.

Encontramos diferentes formas de llevar a cabo el tratamiento de los datos personales:

Anonimización de datos personales

Se produce una ruptura total de los datos personales que vamos a tratar con los datos identificativos, para que no se puedan asociar de ninguna manera con la persona titular de los mismos, es decir, para que no se pueda identificar a una persona concreta.

Por tanto, es el proceso por el cual se desvincula un dato de interés de un dato personal, hasta el punto de que la identificación personal a partir del dato anonimizado no sea posible mediante “todos los medios que puedan ser razonablemente utilizados”.

La anonimización ha sido entendida por la AEPD como “la ruptura de la cadena de identificación de las personas.”

Por ejemplo, si únicamente enviamos nombres de personas físicas (sin otra información adicional como DNI, apellidos, etc.) que la puedan hacer identificable. O se envían datos estadísticos como número de personas en una franja de edad, u otros similares.

Debemos asegurarnos de que la combinación de datos que consideramos anónimos no permita la identificación, ya que, si esto ocurriera, evidentemente, estos datos dejarían de ser anónimos.

Seudonimización de datos personales

Para el RGPD es "aquella información que, sin incluir los datos denominativos de un sujeto, permiten identificarlo mediante información adicional, siempre que ésta 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." En palabras más simples, consiste en tratar los datos personales sin los datos identificativos del interesado, pero sin suprimir la vinculación entre los datos que consigan determinar la persona titular de los mismos.

Un ejemplo sería la sustitución de los nombres de clientes por un código o por un identificador numérico, es decir, cambiar los datos personales por seudónimos.

Preguntas frecuentes con relación a los procedimientos de anonimización o seudonimización:

¿Con qué fin se realizan estos procedimientos?
Son medidas para garantizar la seguridad de los datos de carácter personal que se van a tratar, especialmente cuando los datos tratados son sensibles (Ej.: datos de salud).

¿Quién tiene que realizar estos procedimientos?
Conforme al RGPD, serán llevados a cabo por el responsable del tratamiento o en su caso la persona o equipo que este autorice, pero siempre bajo su responsabilidad y por el encargado del tratamiento.

¿Es obligatorio llevar a cabo los procedimientos de seudonimización y anonimización?
Según el RGPD, no necesariamente. Su realización es potestativa, ya que pueden haberse adoptado otras medidas de seguridad.

¿Se requiere consentimiento del afectado para seudonimizar o anonimizar los datos personales?
No. Estos procedimientos se realizan como medidas de seguridad que se adoptan a nivel interno por el responsable y/o encargado del tratamiento.

¿En qué sectores es más común el uso de estos procedimientos?
Suelen encontrarse sobre todo en el ámbito sanitario, farmacias, fisioterapeutas ... etc.

Por regla general, se separa el dato identificativo del dato de salud con el fin de realizar encuestas, estudios, investigaciones, estadísticas, docencia…

Un ejemplo concreto sería el envío de una muestra biológica -sangre, orina…- a un laboratorio para que realicen las investigaciones que se soliciten. En este caso el laboratorio solamente tiene acceso a dichas muestras, en ningún caso podría acceder a los datos identificativos de la persona titular de las muestras.

¿Qué diferencias hay entre seudonimización y anonimización?
La anonimización es un procedimiento donde los datos identificativos se desasocian totalmente de los datos personales, es algo irreversible.

La seudonimización desvincula los datos identificativos, pero los datos seudonimizados mantienen datos adicionales que pueden reidentificar a los interesados, por tanto, es un procedimiento reversible.

¿Siempre se aplica a estos procesos la normativa de protección de datos?
Solamente los datos de carácter personal están sujetos a la normativa en materia de protección de datos.

Con relación a la pregunta anterior debemos considerar si la seudonimización y la anonimización tratan datos personales y si se encuentran por ello bajo el paraguas del RGPD. En el caso de la anonimización los datos dejan de ser datos personales y por ello se entiende que no estarían dentro de la ley de protección de datos. Esto se produciría cuando los datos identificativos sean imposibles de asociar a un sujeto determinado. Mientras que en el de la seudonimización, por el contrario, nunca se elimina toda la información relativa al sujeto, se cuenta con información adicional y personal que puede dar lugar a su identificación, por ello aquí resulta claro que la normativa en materia de protección de datos debe aplicarse siempre.

6.- RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento es la persona física o jurídica, pública o privada, que decide sobre la finalidad, contenido y uso del mismo, bien por decisión directa o porque así le viene impuesto por una norma legal. Tiene que estar siempre identificada como tal en toda investigación.

En nuestro caso, el CSEULS es responsable de todos los tratamientos de investigación consignados. Mientras que la persona investigadora principal, tutora o directora de tesis,

TFMs, TFGs, tiene la consideración de responsable interna del tratamiento a efectos prácticos, pero siempre es el CSEULS el responsable de todos los tratamientos con datos personales.

7.- ENCARGADOS DE TRATAMIENTO

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. Los tipos de encargado del tratamiento y las formas en que se regulará su relación pueden ser tan variados como los tipos de servicios que puedan suponer acceso a datos personales.

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, inclusive en formato electrónico.

Como ejemplo vamos a ver la siguiente situación: Cuando el responsable de la investigación necesite los servicios de una persona o de una empresa que trate los datos personales bajo sus instrucciones, como, por ejemplo, una empresa de servicios informáticos es obligatorio que el CSEULS firme un Contrato de encargado de tratamiento con dicha persona física o jurídica.

8.- CESIÓN O COMUNICACIÓN DE DATOS

Se entiende por cesión o comunicación de datos como toda revelación de datos realizada a una persona distinta de su titular. Los destinatarios de los datos serán las personas físicas o jurídicas, autoridades públicas, servicios u otros organismos a los que se les comuniquen.

Cuando en una investigación se tiene que ceder datos de carácter personal a terceros ajenos a la misma (los terceros son aquellos que NO son ni las personas interesados, ni las personas investigadoras autorizadas, ni las personas encargadas de tratamiento) es obligatorio que se obtenga el consentimiento expreso y escrito de la persona que facilitó dichos datos, si además la información que se va a comunicar a terceras personas incluye datos obtenidos del sujeto de investigación o persona donante, que revelan o pueden revelar información de carácter personal de sus familiares, la cesión requerirá también el consentimiento expreso y escrito de todos ellos. En este consentimiento se debe informar de a quién y para qué proyecto concreto se ceden los datos.

9.- TRANSFERENCIAS INTERNACIONALES DE DATOS

Siempre que los datos personales se envían fuera del ámbito del Espacio Económico Europeo (EEE), que comprende todos los Estados miembros de la Unión Europea, más Noruega, Islandia y Liechtenstein, se produce una transferencia internacional de datos, ya se

realice para que el destinatario de los datos preste un servicio o para que los trate para una finalidad propia.

La transferencia internacional de datos consiste en la transmisión de datos de carácter personal fuera de la Unión Europea por lo que tanto el investigador como el CSEULS, que es responsable del tratamiento, serán exportadores porque están en territorio europeo y van a realizar una transferencia internacional.

Sólo se pueden realizar transferencias de los datos personales de una investigación a un país u organización internacional si garantizan un nivel de protección adecuado de acuerdo con las condiciones establecidas en el capítulo V del RGPD. Cuando los datos vayan a ser transferidos fuera de la CE a algún país, territorio o sector específico de ese tercer país u organización internacional que la Comisión Europea no haya considerado que garanticen un nivel de protección adecuado, debe darse alguna o algunas de las circunstancias recogidas en el mencionado capítulo. En estos casos se recomienda consultas con el DPD.

10.- DELEGADO O DELEGADA DE PROTECCIÓN DE DATOS (DPD)

El Reglamento General de Protección de Datos ha supuesto un cambio de paradigma en cuanto al modo de cumplir con sus obligaciones. Requiere no sólo su cumplimiento, sino poder demostrarlo, lo que implica una actitud proactiva o diligente por parte de los responsables del tratamiento. Una de las medidas de cumplimiento de ese deber de diligencia que el Reglamento establece es la de designar un delegado de protección de datos en determinados supuestos. Se trata de una persona especialista en protección de datos que las Universidad públicas y privadas y otras instituciones están obligadas a designar.

Entre sus funciones se encuentran las de informar, asesorar y supervisar el cumplimiento de la normativa sobre protección de datos, así como la de resolver reclamaciones que se puedan plantear, además de ser el interlocutor con la Agencia Española de Protección de Datos y con los interesados.

Además, es miembro del Comité de Ética en la Investigación (CEI) que informará sobre los proyectos, por lo que la relación entre las tareas de investigación con datos personales y su trabajo como DPD es obligada, directa y constante.

11.- PRINCIPIO DE LICITUD, LEALTAD Y TRANSPARENCIA

Los datos han de ser tratados de manera lícita, leal y transparente en relación con su titular. No se pueden recoger ni tratar más datos personales que los estrictamente necesarios para la finalidad perseguida en cada caso. Lo que quiere decir es que se deben cumplir con las condiciones para que el tratamiento de los datos personales en una investigación sea

legítimo, esté bien hecho y sea legalmente seguro.

Para que el tratamiento de los datos sea lícito en una investigación debemos:

- Identificar los datos que se van a recoger.
- Saber de quiénes se van a recoger.
- Qué tratamiento se va a dar a los mismo.

Solo será legítimo que se haga dicho tratamiento cuando tengamos el consentimiento informado de las personas que van a participar en la investigación y que han de otorgar el consentimiento de manera libre, específica, explícita e inequívoca para todos los fines en los que se vayan a utilizar. (art. 6 .1,2 RGPD).
Otras bases jurídicas para el tratamiento de datos como son la obligación legal, el interés público o el ejercicio de poderes públicos, en el ámbito de la investigación con seres humanos no restan valor ni sustituyen al deber de información y de consentimiento, solo reflejan algunas situaciones en las que la persona participante en una organización conoce que existe un interés público (art. 8 LOPDGDD y art. 9 RGPD).

Para cumplir con la legalidad es necesario que se den los siguientes requisitos:

1. Obtener el consentimiento explícito por escrito de las personas que participan en la investigación que confirme que acceden a dar sus datos, para qué servirán y cómo se tratarán.
2. Cumplir con el principio de minimización de datos, es decir, asegurarse de la calidad de esa información, que son datos adecuados, veraces y pertinentes para la investigación. Valorar si todos los datos que se van a recoger son realmente indispensables para llevar a cabo la actividad de investigación.
3. Asegurarse de que la recogida no se hace de forma desleal, fraudulenta o ilícita.
4. En el caso de que se recojan datos de salud para la investigación, se debe facilitar cualquier información que se obtenga relacionada con la salud del participante y que le sea útil.
5. Realizar un juicio de proporcionalidad entre la finalidad científica que se persigue y el medio que se va a utilizar.
6. Cuando se necesite para la investigación datos de salud procedentes de la historia clínica de la persona interesada hay que recoger siempre una hoja o documento de información y consentimiento que incluya:
    a. Nombre del profesional y del centro donde ha sido atendido el paciente.
    b. Propósitos de la petición.
    c. Expresa conformidad de publicación del caso clínico en publicaciones científicas dirigidas a profesionales de la salud.
    d. Nombre del paciente.
    e. Documento de identidad o pasaporte y su firma autorizando expresamente que se utilicen los datos de su historia clínica en las condiciones que se describen en el informe.

7. Asegurarse del cumplimiento del deber de secreto y del compromiso de confidencialidad por parte de las personas que tienen acceso a los datos, incluso cuando la relación que vincule a las partes haya finalizado.

12.- DEBER DE INFORMAR

La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos recae sobre el responsable del tratamiento en la figura del investigador principal de la actividad que debe informar en nombre del CSEULS.

La información se debe poner a disposición de los participantes en el momento en que se soliciten los datos, previamente a la recogida o registro, si es que los datos se obtienen directamente del interesado.

En el caso de que los datos no se obtengan del propio interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, el responsable informará a las personas interesadas dentro de un plazo razonable, pero, en cualquier caso:

- antes de un mes desde que se obtuvieron los datos personales,
- antes o en la primera comunicación con el interesado,
- antes de que los datos, en su caso, se hayan comunicado a otros destinatarios

Esta obligación se debe cumplir sin necesidad de requerimiento alguno, y el responsable deberá poder acreditar con posterioridad que la obligación de informar ha sido satisfecha.

El CSEULS pone a tu disposición en el siguiente enlace (https://www.lasallecentrouniversitario.es/investigacion/comite-de-bioetica/9) el modelo de Consentimiento Informado validado por la asesoría de protección de datos. No obstante, hay que tener en cuenta que la LOPD-GDD introduce el concepto de información por capas o niveles, refiriéndose a cómo presentar la información a la persona a la que se solicita los datos.

En un primer nivel se informa de forma resumida, en el mismo momento y en el mismo medio en el que vas a recoger los datos.

Después se puede remitir más información adicional en un segundo nivel, con una presentación más detallada de las informaciones y usando el medio que se considere más adecuado para su presentación, comprensión o incluso, para su archivo.

Ejemplo: un documento en papel de solicitud de consentimiento informado (CI) para participar en la investigación, que incluya el consentimiento informado para la donación de datos necesarios para la investigación, recoge la primera capa de información y ese mismo documento en papel incluyes un enlace a la web donde está la segunda capa de

información.

En resumen, la información que debe tener clara la persona a la que le solicitas los datos es la siguiente:

En cuanto al contenido la información debe ser:

- Veraz y suficientemente extenso, preciso, claro y comprensible.
- Se aconseja suministrar toda la información por escrito en el documento de consentimiento.
- Poner siempre el enlace de acceso a la información completa si lo hubiera

En cuanto a la forma:

- Adaptar la información al modelo de recogida de datos.
    - Formularios en papel.
    - Formularios en la web.
    - Entrevista.
- Utilizar los modelos de consentimiento facilitados por el CSEULS para facilitar la correcta recogida.

Y por último debemos informar de la custodia de los datos se han de guardar en el soporte o lugar más apropiado, el justificante de que se ha informado y se ha consentido, es decir, los consentimientos informados firmados por los participantes en la actividad de investigación.

INFORMACIÓN SOBRE LOS DERECHOS DE ACCESO RECTIFICACIÓN, SUPRESIÓN, OPOSICIÓN, PORTABILIDAD Y LIMITACIÓN (ARSOPL)

Cuando hablamos de estos derechos, nos referimos a los derechos que todo ciudadano tiene reconocidos, en orden a una correcta protección de los datos de carácter personal de los que se es titular. Con esta información siempre se trata de promover la capacidad de decisión y de control sobre los propios datos personales. Por ello, el responsable de la investigación tiene que informar al participante en la investigación sobre sus derechos, sobre cómo puede ejercerlos y sobre la forma de ponerse en contacto para hacerlo. Estos derechos son los siguientes:

- **Derecho de Acceso** o derecho a solicitar información al responsable sobre si sus datos están siendo tratados y en caso afirmativo qué datos son.
- **Derecho de Rectificación** o derecho a solicitar la modificación de datos que sean inexactos o incompletos.
- **Derecho de Supresión** o derecho a solicitar la supresión de los datos en determinados supuestos, pero no se suprimirán los resultados ya obtenidos.
- **Derecho de Oposición** o derecho a oponerse al tratamiento de sus datos personales por motivos relacionados con su situación particular.
- **Derecho a la Portabilidad de los datos** o derecho a solicitar que se le faciliten los

datos en un formato estructurado, de uso común y lectura mecánica y el derecho a transmitirlos a otro responsable.

- **Derecho a la Limitación del tratamiento** o derecho a solicitar que se limite el tratamiento de sus datos en determinadas condiciones.

Por lo que respecta al ejercicio de los derechos, el interesado deberá ejercerlo ante el responsable del tratamiento y este deberá contestar, tal y como establece el artículo 12.3 del RGPD en el plazo de un mes a contar desde la recepción de la solicitud.

INFORMACIÓN SOBRE EL TIEMPO DE CONSERVACIÓN DE LOS DATOS

Al informar sobre el tiempo de conservación en el CI, hay que indicar al posible donante que el plazo mínimo de conservación es de cinco años, con fines de auditoría y verificación de la investigación realizada con esos datos. También hay que informar de que se pueden conservar los datos recogidos para la investigación mientras no solicite su supresión y esos datos sigan respondiendo a la finalidad para la que fueron obtenidos y así como de que no pueden pedir que se supriman los resultados obtenidos con sus datos hasta el momento de la solicitud de supresión.
Por último, si se aplican medidas técnicas apropiadas, como la anonimización, los datos pueden ser conservados durante más tiempo.
En el caso de que se produzca cambio de condiciones, tipo de datos o forma de acceso, habría que informar al CEI.

INFORMACIÓN SOBRE UNA POSIBLE CESIÓN DE DATOS

Para compartir, comunicar, y dejar que otro acceda o traspasar datos de la persona donante a un tercero, dicha persona debe tener constancia de la posible cesión, ya que será quien permita o no ese traspaso.

En el consentimiento informado, en el apartado de información sobre protección de datos, hay un apartado para indicar esta cesión, se debe poner como ya se indicó a quién y para qué se van a ceder esos datos.

TRATAMIENTOS POSTERIORES O USOS ADICIONALES DE LOS DATOS

Se puede dar el caso de que, una vez informada la persona donante y habiendo aceptado, se plantee una nueva investigación con un nuevo tratamiento de datos compatible con el anterior. En este caso, hay que informarle por correo postal, por medios electrónicos u otros y es necesario un Informe Favorable previo del Comité de Ética de Investigación.

13.- CONTACTO

El DPD y el comité de ética que evalúa el proyecto puede orientar sobre las dudas que surjan porque la casuística es muy variada y la ley no es taxativa en esta cuestión. Los datos de contacto son:
Secretaria Comité Bioética: María Gracia Carpena - email: mgcarpena@lasallecampus.es
Delegada de Protección de Datos: Natalia González – email: dpo@lasallemadrid.es