Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

Exp.: CN16-023

DICTAMEN Nº D16-035

CONSULTA PLANTEADA POR LA DIRECCIÓN DE RÉGIMEN JURÍDICO, ECONÓMICO Y SERVICIOS GENERALES DEL DEPARTAMENTO DE SALUD DEL GOBIERNO VASCO SOBRE CESIÓN DE DATOS PERSONALES DE SALUD PARA LA REALIZACIÓN DE ESTUDIOS O INVESTIGACIONES EPIDEMIOLÓGICOS

ANTECEDENTES

PRIMERO: Se ha recibido en esta Agencia Vasca de Protección de Datos (AVPD) consulta de la Dirección de Régimen Jurídico, Económico y Servicios Generales del Departamento de Salud del Gobierno Vasco sobre el asunto arriba referenciado.

SEGUNDO: El artículo 17.1 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, en su apartado n) atribuye a la AVPD la siguiente función:

> *"Atender a las consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta Ley, así como otras personas físicas o jurídicas, en relación con los tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de esta Ley".*

Corresponde a esta Agencia Vasca de Protección de Datos, en virtud de la normativa más arriba citada, la emisión del informe en respuesta a la consulta formulada.

CONSIDERACIONES

I

Solicita la administración consultante *"la emisión de informe sobre la actuación que debería seguir este departamento en relación con la cesión de datos contenidos en ficheros de datos de carácter personal bajo su responsabilidad para la realización de estudios de investigación epidemiológica"*. Se adjunta informe realizado por dicha administración con ocasión de la solicitud realizada por el Instituto Aragonés de Ciencias de la Salud de cesión de datos del fichero CMBD en el ámbito colaborativo del proyecto VPM del Sistema Nacional de Salud, así como otras cuatro solicitudes de cesión de datos recibidas en la Dirección de Planificación, Ordenación y Evaluación Sanitaria del Departamento de Salud para diversos proyectos de investigación.

Antes de responder a la solicitud de la administración consultante, y para una mejor comprensión de lo que en ella se contiene, abordaremos, con carácter previo, la regulación legal de la cesión de datos de carácter personal relativos a la salud para realizar estudios epidemiológicos y de investigación.

II

La Ley Orgánica 15/1999 de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD) establece un régimen especial para el tratamiento de datos de salud y, en su caso, comunicación, considerándolos datos especialmente protegidos, debiendo plantearse si existe algún supuesto en que la propia Ley Orgánica da cobertura a esa cesión.

La necesidad de obtener el consentimiento expreso e informado de los pacientes para incluir sus datos en el correspondiente fichero tiene su fundamento en el artículo 7 de la LOPD.

Como regla general, el artículo 7.3 de la LOPD dispone que "*los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, sólo podrán ser recabados, tratados y cedidos cuando por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente*". Este artículo determina el contenido esencial del derecho fundamental a la protección de datos de carácter personal debido a su carácter orgánico.

Dada la incidencia especial de los datos de salud, como datos sensibles, en la esfera íntima del afectado, la LOPD ha establecido una regulación específica y más rigurosa que la establecida con carácter general tanto en lo referente a los supuestos en que será posible el tratamiento de los datos como en lo que atañe a las medidas que habrán de adoptarse para garantizar la seguridad en el tratamiento de los datos, así como el cumplimiento de deberes de confidencialidad y sigilo que deben regir en el mencionado tratamiento, de tal manera que la necesidad de obtener el consentimiento expreso de los titulares de tales datos constituye la regla general para el tratamiento de los mismos.

No obstante, el mismo artículo 7.3 contempla la posibilidad de que dicho tratamiento pueda llevarse a cabo en los supuestos en los que una ley así lo disponga debiendo quedar dicha habilitación fundada en la existencia de razones de interés general.

La aplicación del artículo 7.3 de la LOPD implica, en aplicación del principio de especialidad, la imposible aplicación a los datos referidos en el mismo de cualquiera de las causas legitimadoras del tratamiento previstas en el artículo 11.2 de la Ley Orgánica, quedando limitados los supuestos habilitantes del tratamiento y cesión de estos datos a los establecidos en norma especial o a aquéllos en los que la norma general se refiere expresamente a tales datos.

El artículo 8 de la LOPD dedicado específicamente a los datos de salud establece lo siguiente:

> *"Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad".*

Asimismo, artículo 11.2 f) de la LOPD establece la licitud de la cesión de determinados datos relacionados con la salud si la misma es "*necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica*".

En consecuencia, la Ley Orgánica 15/1999 viene a establecer una lista tasada de casos en que será posible el tratamiento de los datos relacionados con la salud, quedando el mismo limitado a los supuestos en que:

- El interesado haya prestado su consentimiento expreso para ello.
- Una norma con rango de Ley así lo prevea, por razones de interés público.
- El tratamiento sea necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, con las restricciones previstas en el artículo 7.6 de la Ley Orgánica, que deberá además ser objeto de una interpretación restrictiva, en los términos ya señalados.
- El tratamiento sea necesario para atender una urgencia vital.
- El tratamiento se lleve a cabo en el ámbito de la asistencia sanitaria respecto de los pacientes que acudan a los centros sanitarios, en los términos previstos en la legislación sectorial que resulte de aplicación.
- La comunicación de los datos sea precisa para solucionar una urgencia o para realizar los estudios epidemiológicos en los términos previstos en la legislación sectorial.

Así, tal y como ordena la LOPD, en el caso de cesiones de datos de salud para realizar estudios o investigaciones epidemiológicas, tendremos que acudir a la legislación sanitaria implicada: la Ley 14/1986, de 25 de abril, General de Sanidad; la Ley 16/2003, de Cohesión y Calidad del Sistema Nacional de Salud; la Ley 44/2003, de Ordenación de Profesiones Sanitarias; la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; el Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud; y en el ámbito del País Vasco, la Ley 8/1997, de 26 de junio, de Ordenación Sanitaria de Euskadi y Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica.

La normativa sectorial otorga a los datos de salud el carácter de confidenciales. Así el artículo 10.3 de la Ley 14/1986, de 25 de abril, General de Sanidad establece como uno de los derechos que todos tienen respecto a las distintas administraciones públicas sanitarias el de *"la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público"*.

En igual sentido el artículo 7.1 de la Ley 41/2002 dispone que "*toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley*"; y el artículo 11.2 del Decreto 38/2012 establece que *"Los datos existentes en las historias clínicas son confidenciales, por lo que toda persona que elabore o tenga acceso a la información y a la documentación clínica está obligada a guardar la reserva debida. Asimismo el personal de los centros y servicios sanitarios que acceda a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto"*.

En cuanto al acceso a la historia clínica, la Ley 41/2002, señala en el artículo 16 lo siguiente:

> *"1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.*
>
> *2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.*
>
> *3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.*
>
> *Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.*
>
> *Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.*
>
> *4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.*
>
> *5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.*
>
> *6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.*
>
> *7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso".*

De lo dispuesto en el precepto trascrito se desprende que la ley 41/2002, establece que la información con los fines a que se refiere el apartado 3 del artículo 16 sea tratada de modo anónima, salvo que el propio paciente preste su consentimiento, lo que obliga, con carácter general a disociar los datos.

Ha de tenerse en cuenta que la finalidad de la historia clínica es prestar la adecuada asistencia sanitaria a los pacientes, y que los fines epidemiológicos, de salud pública, de

investigación y de docencia no repercuten en beneficio del propio paciente sino de la sociedad en su conjunto, de ahí que la propia La Ley General de Sanidad en su artículo 8 establece como actividad principal del sistema sanitario la realización de estudios epidemiológicos para la prevención de los riesgos de salud, y en su artículo 23 la creación de registros para organizar la información sanitaria, vigilancia y acción epidemiológica. También la Ley 41/2002 se refiere en su exposición de motivos a la "concepción comunitaria del derecho de salud". Más que una facultad de comunicar datos se trata de una obligación de ceder información bajo el amparo de un interés público. De ahí que el artículo 11.2 f) de la LOPD excepcione del consentimiento la cesión de datos relativos a la salud además de cuando sea necesario solucionar una urgencia que requiera acceder a un fichero, cuando la cesión persiga realizar estudios epidemiológicos, pero en los términos establecidos en la legislación sobre sanidad estatal y autonómica. El derecho de los ciudadanos a la información epidemiológica es reconocido también en el art. 6 de la Ley 41/2002, pero esta misma norma básica obliga a preservar los datos de identificación personal del paciente separados de los de carácter clínico asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

En definitiva, la ley no impide la posterior utilización de los datos de salud obrantes en las historia clínica, sin perjuicio de que, lógicamente, se introduzcan medidas para garantizar la *confidencialidad del paciente, dada la especial naturaleza y sensibilidad de los datos* sometidos a tratamiento o que constan en la historia clínica. De este modo, los datos de la historia clínica podrán ser utilizados para los fines beneficiosos que se indican, pero siempre dentro de la adecuada confidencialidad que garantice que sólo aquellos pacientes que hayan prestado su consentimiento para ello van a resultar conocidos.

De este modo, si bien con carácter general el acceso a datos contenidos en las historias clínicas con fines epidemiológicos debe llevarse a cabo de forma que queden disociados los datos personales de los de carácter clínico-asistencial, la propia norma recoge la posibilidad de que las Administraciones sanitarias accedan, en los términos señalados en el precepto transcrito, a los datos identificativos de los pacientes por razones epidemiológicas cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población.

En el mismo sentido, el artículo 16 del Decreto 38/2012 del Gobierno Vasco, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica establece lo siguiente:

> *"1. – Se podrá también acceder a la historia clínica, con sujeción a lo previsto en las leyes, con los siguientes fines:*
>
> *– Investigación.*
>
> *– Docencia.*
>
> *– Estudio epidemiológico o de salud pública.*
>
> *– Dirección, planificación o programación del sistema sanitario.*
>
> *– Facturación de servicios sanitarios.*
>
> *– Judiciales.*

2.– El acceso a la historia clínica con los fines del apartado anterior obliga, conforme a lo dispuesto en el artículo 16.3 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, a preservar los datos de identificación personal del o de la paciente separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que la propia persona paciente haya dado su consentimiento para no separarlos.

3.– Se exceptúan de lo previsto en el apartado anterior de este artículo, conforme dispone la Ley, los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos de la propia persona paciente con los clínico-asistenciales. En estos casos se estará a lo que dispongan los Jueces o Juezas y Tribunales en el proceso correspondiente.

4. – A las compañías de aseguramiento privado únicamente se les podrá facilitar aquellos datos de la historia clínica imprescindibles a efectos de facturación, con la finalidad de la justificación del gasto. Cualquier otra información clínica solicitada por la compañía aseguradora requerirá el consentimiento expreso de la persona paciente.

5. – El acceso conforme a los procedimientos previstos en este artículo requerirá de la previa solicitud a la persona responsable del centro o servicio sanitario, de la que quedará constancia, así como de las entregas que procedan".

III

A la vista de todo lo anteriormente expuesto, para ceder los datos relativos a la salud con fines de estudio o investigación epidemiológica, la Administración consultante deberá ajustarse a la LOPD y a la normativa sectorial a que la misma se remite.

Para ello, es obligatorio preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de forma que quede asegurado el **anonimato**. Esta obligación sólo cede en el caso de que el paciente haya dado su consentimiento expreso para no separar dichos datos (artículo 16.3 Ley 41/2002).

Por tanto, es requisito esencial para la cesión, salvo consentimiento expreso del paciente, la anonimización de los datos personales.

En este sentido, hay que decir que la anonimización de los datos personales hace que éstos dejen de tener esta consideración y, por tanto, dejen de ostentar la protección de que gozan los datos personales.

Puede definirse la anonimización, de conformidad con la Directiva 95/46/CE, de 24 de octubre de 1995, como aquel tratamiento de datos personales que impida la identificación de una persona física mediante "*el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por terceros*" (considerando 26 de la Directiva).

Ahora bien, hay que tener presente que es necesario introducir medidas encaminadas a minimizar, tanto como sea posible, la existencia de algún tipo de riesgo que puede conllevar el proceso de anonimización, teniendo en cuenta que el riesgo cero no existe. Entre dichas medidas habría que destacar las siguientes:

- La implementación de un buen sistema de anonimización.
- La determinación de medidas dirigidas a evitar procesos que inviertan el proceso y permitan identificar a los pacientes una vez ya se ha realizado el proceso de anonimización.
- La introducción de medidas de control y realización de auditorías periódicas internas y externas que evalúen el uso de los datos y las medidas de seguridad utilizadas que detecten posibles irregularidades y eviten la entrada en el sistema de la piratería informática.

El Grupo de Trabajo sobre Protección de las Personas en lo que respecta al tratamiento de datos personales, creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, emitió el 10 de abril de 2014 el *Dictamen 05/2014 sobre técnicas de anonimización*, en el que se recoge a modo de resumen lo siguiente:

> *"(…) El Grupo de Trabajo reconoce el valor potencial de la anonimización, en particular como estrategia para permitir a las personas y la sociedad en su conjunto beneficiarse de los «datos abiertos» al mismo tiempo que se mitigan los riesgos para los interesados. No obstante, los estudios de caso y las publicaciones científicas muestran la dificultad de crear un conjunto de datos verdaderamente anónimo conservando, sin embargo, toda la información subyacente requerida para la tarea.*
>
> *A la luz de la Directiva 95/46/CE y de otros instrumentos jurídicos pertinentes de la UE, la anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación. En este proceso, los responsables del tratamiento deben considerar distintos aspectos y valorar todos los medios que puedan utilizarse «razonablemente» para la identificación de los datos (ya sea por el responsable del tratamiento o por terceros).*
>
> *La anonimización implica un tratamiento posterior de los datos personales. Por tanto, debe satisfacer el requisito de compatibilidad teniendo en cuenta las circunstancias y los fundamentos jurídicos de dicho tratamiento. Por otra parte, aunque los datos anonimizados se encuentren fuera del alcance de la legislación sobre protección de datos, es posible que los interesados tengan derecho a protección en virtud de otras disposiciones legales (como las que protegen la confidencialidad de las comunicaciones).*
>
> *(…)*
>
> *En este documento se aborda también la seudonimización, para aclarar algunos errores e ideas falsas: la seudonimización no es un método de anonimización; simplemente, reduce la vinculabilidad de un conjunto de datos con la identidad original del interesado y es, en consecuencia, una medida de seguridad útil.*
>
> *La conclusión del presente dictamen es que las técnicas de anonimización pueden aportar garantías de privacidad y usarse para generar procesos de anonimización eficientes, pero solo si su aplicación se diseña adecuadamente, lo que significa que han de definirse con claridad los requisitos previos (el contexto) y los objetivos del proceso para obtener la anonimización deseada al mismo tiempo que se generan datos útiles. La solución óptima debe decidirse caso por caso y puede conllevar la combinación de diversas técnicas, aunque siempre respetando las recomendaciones prácticas que se formulan en este documento.*
>
> *Por último, los responsables del tratamiento deben ser conscientes de que un conjunto de datos anonimizado puede entrañar todavía riesgos residuales para los*

interesados. Efectivamente, por una parte, la anonimización y la reidentificación son campos de investigación activos en los que se publican con regularidad nuevos descubrimientos y, por otra, incluso los datos anonimizados, como las estadísticas, pueden usarse para enriquecer los perfiles existentes de personas, con la consiguiente creación de nuevos problemas de protección de datos. En suma, la anonimización no debe contemplarse como un procedimiento esporádico, y los responsables del tratamiento de datos han de evaluar regularmente los riesgos existentes".

El citado Dictamen 05/2014 sobre técnicas de anonimización subraya como conclusión que *"las técnicas de anonimización pueden aportar garantías a la privacidad, pero solo si su aplicación se diseña adecuadamente, lo que significa que han de definirse con claridad los requisitos previos (el contexto) y los objetivos del proceso para obtener el grado de anonimización deseado"*.

Asimismo y como recomendaciones habría que destacar las "*buenas prácticas de anonimización*" para reducir los riesgos de identificación que se exponen en el Dictamen 05/2014:

"Reglas generales:

- Publicar los datos y luego olvidarse de ellos no es una práctica fiable. Dado el riesgo residual de identificación, los responsables del tratamiento de datos deberían:

1. Identificar nuevos riesgos y evaluar regularmente los riesgos residuales.

2. Valorar si los controles para la identificación de riesgos son eficaces y modificarlos si fuera necesario.

3. Supervisar y controlar los riesgos.

- Como parte de estos riesgos residuales, se debería considerar el potencial de identificación de la parte no anonimizada de un conjunto de datos (si es que existe), especialmente cuando se combina con la parte anonimizada, además de otras eventuales correlaciones entre atributos (p. ej., entre ubicaciones geográficas y datos de nivel de riqueza).

Elementos contextuales:

- Los objetivos que deben alcanzarse mediante el conjunto de datos anonimizado deben fijarse con toda claridad, ya que desempeñan un papel clave al determinar el riesgo de identificación.

- Esto va asociado a la valoración de la totalidad de los elementos contextuales relevantes. Por ejemplo: la naturaleza de los datos originales, los mecanismos de control que se hayan implementado (incluidas las medidas de seguridad encaminadas a restringir el acceso a las bases de datos), el tamaño de la muestra (características cuantitativas), la disponibilidad de los recursos de información públicos (en los que se basan los destinatarios) o la entrega prevista de los datos a terceros (limitada o ilimitada: p. ej., en Internet, etc.).

- No debe olvidarse la posibilidad de aparición de atacantes. Para ello, se debe valorar el atractivo que pueden tener los datos para determinados atacantes. A este respecto, la sensibilidad de la información y la naturaleza de los datos vuelven a ser factores claves.

<u>Elementos técnicos</u>:

- Los responsables del tratamiento deben revelar la técnica o el conjunto de técnicas de anonimización que se hayan utilizado, sobre todo si tienen la intención de publicar el conjunto de datos anonimizado.

- Deben eliminarse del conjunto de datos los atributos obvios (es decir, los raros) y los cuasi identificadores. (…)".

Además de asegurar el anonimato, habrá que tener presente que la cesión de datos relativos a la salud deberá ser congruente con los principios de protección de datos y, en particular, con los consagrados en el artículo 4 de la LOPD, cuyo apartado 1 dispone que "*Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido*". De este modo la comunicación de datos deberá limitarse a aquéllos estrictamente necesarios para la finalidad pretendida (principio de calidad de los datos).

Asimismo, en el tratamiento de datos de salud, deberán observarse las medidas de seguridad que deberán ser, además de las de nivel medio y básico, las de nivel alto, conforme señala el artículo 81.3 a) del Reglamento de desarrollo de la LOPD, y que se concretan en sus artículos 89 y siguientes.

Las cesiones de datos de salud para la realización de estudios de investigación epidemiológica serán conformes a la normativa de protección de datos siempre y cuando las mismas se ajusten a lo dispuesto en el cuerpo de este dictamen.

En Vitoria-Gasteiz, a 19 de julio de 2016