

ARTÍCULO ESPECIAL



Gac Med Bilbao. 2025;122(1):47-54

El reglamento del espacio europeo de datos de salud: ¿Qué podemos esperar?

De Miguel-Beriain Íñigo^a, Loyo-Menoyo Mónica^b

(a) Investigador Distinguido, Departamento de Derecho Público, UPV/EHU & Ikerbasque, Basque Foundation for Science.

(b) Investigadora posdoctoral, Departamento de Derecho Público, UPV/EHU.

Recibido el: 7 de marzo de 2025; aceptado el 15 de marzo de 2025.

Resumen:

El pasado día 5 de marzo se publicó en el Diario Oficial de la UE el Reglamento del Espacio Europeo de Datos de Salud. Esta es una norma de crucial importancia que introducirá cambios fundamentales en lo que se refiere tanto al tratamiento de datos para fines clínicos como a su uso para investigación o innovación. En la parte clínica, destacan las reformas efectuadas sobre algunos derechos ya existentes, como el de acceso o el de portabilidad, que ahora adquieren una dimensión más amplia, así como la aprobación de nuevos derechos, como el de conocer quién ha accedido a la historia clínica electrónica o los de incorporar datos o bloquear accesos a esa misma historia. No obstante, es en el área del tratamiento de datos para investigación donde se introducen cambios de particular importancia, especialmente la construcción de una estructura de gobernanza novedosa encaminada a asegurar que los datos puedan utilizarse sin que ello suponga un atentado contra los derechos e intereses de los pacientes o ciudadanos.

© 2025 Academia de Ciencias Médicas de Bilbao. Todos los derechos reservados.

Europako osasun-datuen esparruko araudia: zer espero dezakegu?

Laburpena:

Joan den martxoaren 5ean argitaratu zen EBko Egunkari Ofizialean Osasun Datuen Europako Esparruaren Erregelamendua. Arau horrek berebiziko garrantzia du, eta funtsezko aldaketak egingo ditu, bai helburu klinikoetarako datuen tratamenduari dagokionez, bai ikerketarako edo berrikuntzarako erabilerari dagokionez. Alde klinikoan, lehendik dauden eskubide batzuen gainean egindako erreformak nabarmentzen dira, hala nola sarbidearena edo eramangarritasunarena, orain dimentsio zabalagoa hartzen baitute, bai eta eskubide berrien onarpena ere, hala nola historia kliniko elektronikora nor sartu den jakitearena edo datuak sartzeararena edo historia horretarako sarbideak blokeatzeararena.

PALABRAS CLAVE

Espacio Europeo de Datos de Salud.
Tratamiento de datos de salud.
Uso secundario de dato.
Datos de salud.

GILTZA-HITZAK

Osasun Datuen Europako Esparrua.
Osasun-datuen tratamendua.
Datuen bigarren mailako erabilera.
Osasun-datuak.

Hala ere, ikerketarako datuen tratamenduaren arloan sartzen dira garrantzi bereziko aldaketak, batez ere gobernantza-egitura berritzaile bat eraikitzea, datuak pazienteen edo herritarren eskubide eta interesen aurka egin gabe erabili ahal izango direla ziurtatzeko.

© 2025 Academia de Ciencias Médicas de Bilbao. Eskubide guztiak gordeta.

KEYWORDS

European Health Data Space.
Health data processin.
Secondary use of data.
Health data.

The european health data area regulation: What can we expect?

Abstract:

On March 5, the European Health Data Space Regulation was published in the Official Journal of the EU. This is a regulation of crucial importance that will introduce fundamental changes with regard to both the processing of data for clinical purposes and their use for research or innovation. On the clinical side, the reforms made to some existing rights, such as the right of access or portability, now take on a broader dimension, as well as the approval of new rights, such as the right to know who has accessed the electronic medical record or the right to incorporate data or block access to the same record. However, it is in the area of data processing for research that changes of particular importance are introduced, especially the construction of a novel governance structure aimed at ensuring that data can be used without infringing the rights and interests of patients or citizens.

© 2025 Academia de Ciencias Médicas de Bilbao. All rights reserved.

Introducción

El pasado día 5 de marzo de 2025 se publicó finalmente en el Diario Oficial de la UE el Reglamento para el Espacio Europeo de Datos de Salud (REEDS), una norma destinada a mejorar la regulación de los datos electrónicos de salud en el ámbito de la UE. Su aprobación traerá consecuencias de gran calado tanto a nivel asistencial como en lo que se refiere al uso secundario de datos para investigación e innovación, por ejemplo. Con ello se pretende suplir algunas de las carencias que muestra el actual marco normativo, así como impulsar algunas de las previsiones que ya existen, pero no han obtenido la aplicación esperada. Es importante destacar que el REEDS no está llamado a reemplazar, sino a complementar lo dispuesto en otras normas ya existentes, tanto a nivel nacional como internacional. De hecho, deberán adoptarse interpretaciones compatibles con el Reglamento General de Protección de Datos, de 2016 (RGPD), la Ley de Gobernanza de Datos, el Reglamento de Productos Sanitarios, etc, de modo que uno no debería pensar que todo lo que ahora mismo se halla en vigor vaya a dejar de estarlo sólo por la aprobación de esta norma.

En este artículo vamos a intentar mostrar algunas de las principales medidas incluidas en el REEDS. Con tal fin, dividiremos el texto en dos partes, la primera destinada al uso de los datos en atención sanitaria y la segunda dirigida al uso secundario de datos. Permítasenos avisar al lector de que mucho de lo que podrá leer aquí será, necesariamente, una versión simplificada de todo lo que contiene el texto normativo. Así tendrá que ser, por motivos de espacio. Creemos, con todo, que hemos sido capaces de incluir aquí lo más relevante del REEDS. Esperemos que esto sirva para acercarnos a todos un poco más a esta herramienta.

Uso de los datos en la asistencia sanitaria

Los datos electrónicos de salud

El capítulo II del REEDS es el que regula el uso de los datos electrónicos de salud para fines asistenciales. No todo tipo de datos, en realidad, sino especialmente los que figuran en su artículo 5 y a los que el documento denomina “categorías prioritarias de datos personales de salud electrónicos², entre los que se encuentran: (a) resúmenes de pacientes; (b) recetas electrónicas; (c) dispensaciones electrónicas; (d) estudios de imagen médica e informes de imagen relacionados; (e) resultados de pruebas médicas, incluidos resultados de laboratorio y otros resultados diagnósticos e informes relacionados; (f) informes de alta. El Anexo I, a su vez, proporciona mayor detalle sobre las características principales de cada una de estas categorías. Pues bien, respecto a estos datos, principalmente, el REEDS establece una serie de derechos nuevos, que analizaremos a continuación, a la par que introduce modificaciones significativas en otros, como el derecho de acceso o de portabilidad.

Derecho de acceso

El derecho de acceso en el ámbito de la UE jugaba ya un papel importante en la Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza. De hecho, sus artículos 4.2.f) y 5.d) señalaban que el Estado miembro en el que se debía proporcionar la atención sanitaria y el Estado miembro en el que residiera el sujeto deberían garantizar que «los pacientes que deseen recibir o reciban asistencia sanitaria transfronteriza tengan acceso o dispongan al menos de una copia de su historial médico

de conformidad con las medidas nacionales de aplicación de las disposiciones de la Unión en materia de protección de datos personales y con sujeción a las mismas»⁴. Por tanto, al menos en teoría la Directiva ya incluía el deber de generar y actualizar un historial médico del paciente, así como la obligación de poner a disposición de la persona interesada una copia de dicho historial médico (que incluya algo más que datos personales), aunque no necesariamente de forma gratuita. No obstante, la aplicación de la Directiva ha sido sumamente dispar entre los Estados miembros, hasta el punto de que en general se podría tildar de fracaso en lo que se refiere al acceso a las historias clínicas, sin ir más lejos. De otro lado, incluso en el ámbito de un mismo país, se han producido demoras en el acceso a las historias clínicas, que a veces se siguen proporcionando en papel, o como documentos escaneados.

Teniendo esto presente, el REEDS surge con la vocación de ofrecer a las personas físicas un modo más eficaz de acceder a sus propios datos sanitarios electrónicos personales, ya sean el propio interesado o sus representantes legales. Su artículo 3 dispone explícitamente que tienen derecho a acceder de forma gratuita e inmediata, respetando la viabilidad tecnológica, a las categorías prioritarias definidas de datos personales de salud electrónicos, que hemos descrito en el apartado precedente, a través de un servicio de acceso a datos de salud electrónicos. Y esto con independencia de dónde se procese, del tipo de proveedor de asistencia sanitaria, de las fuentes de datos o del país de afiliación del paciente. Por tanto, en principio un sanitario finlandés deberá poder acceder a las categorías de datos citados desde su país, si un paciente se lo demanda. Asimismo, el paciente tendrá la posibilidad de delegar en un representante el ejercicio del derecho. Y esto de forma inequívocamente gratuita, frente a lo que estipula el artículo 15 del RGPD, que introduce algunos casos en los que es posible trasladar algún tipo de coste al interesado.

El derecho de portabilidad

El derecho de portabilidad va más allá del acceso a los datos de un paciente, ya que implica la posibilidad de transferir sus datos a otro responsable en un formato electrónico. Por desgracia, hasta ahora esto ha sido muy difícil de lograr, no sólo por las limitaciones técnicas, sino también por las deficiencias del marco jurídico actual⁸.

El REEDS pretende superarlas declarando que el derecho de portabilidad se ejercerá sobre todo tipo de datos, sin que importe cómo se hayan recogido o quién los haya facilitado al responsable, o si este los ha inferido, o el fundamento jurídico del tratamiento, o de la condición del responsable del tratamiento como organización pública o privada. Y se ejercerá también con independencia del Estado miembro en el que se traten dichos datos, el tipo de prestador de asistencia sanitaria, las fuentes de datos o el Estado miembro de afiliación de la persona física⁹. A partir de esta visión, el articulado del REED

se centra, en primer lugar, en asegurar la creación de estándares en cuanto a los formatos de los diferentes sistemas, de tal manera que pueda garantizarse efectivamente su interoperabilidad. Esta es una cuestión absolutamente esencial, por cuanto si los lenguajes no son mutuamente compatibles, es imposible garantizar la portabilidad. Para hacer viable el sistema, y en contraste con la falta de concreción del RGPD sobre la cuestión de la interoperabilidad, la REEDS impone explícitamente a los fabricantes y a los importadores de sistemas de HCE la obligación de garantizar su interoperabilidad, siendo este uno de los requisitos esenciales de los sistemas de HCE que figuran en su anexo II. Su articulado encomienda a la Comisión Europea el mandato de desarrollar especificaciones técnicas al respecto. Estas previsiones se extienden en el REEDS a las aplicaciones de bienestar que intercambien información con los sistemas de HCE, a través de una declaración voluntaria de conformidad con los requisitos del anexo II que se incluirá en el etiquetado. Por fin, hay que subrayar que el derecho de portabilidad incluido en el REEDS parece extenderse a todos los datos sanitarios, no sólo a los personales.

Otros derechos: derecho de los pacientes a incluir datos en la HCE, a conocer quién ha accedido a ella, o a restringir el acceso a su HCE

El REEDS también crea nuevos derechos, que se podrán ejercer en el marco de las estructuras descritas por este mismo Reglamento. Entre ellos se cuenta, en primer lugar, el derecho de los pacientes o sus representantes a introducir datos en su historia clínica electrónica. Esto constituye una novedad palmaria, que tiene claras consecuencias positivas, en cuanto que le permitirá al paciente dotarse de un mayor control sobre su historial, aportando datos que pueden ser importantes para él, pero también podría crear problemas serios, dada la posible falta de calidad de esos datos. En consecuencia, será necesario que la HCE muestre qué parte de los datos ha sido añadido por el paciente o sus representantes. Este derecho, no obstante, no incluye la posibilidad de modificar los datos introducidos en la HCE por los profesionales sanitarios.

El segundo derecho de nueva creación es el que permitirá a los pacientes restringir el acceso de los profesionales de la salud y los prestadores de asistencia sanitaria a la totalidad o parte de sus datos personales de salud electrónicos. Obviamente, este es un derecho que de un lado refuerza considerablemente su derecho a la autodeterminación informativa, dotándole de un poder que ahora mismo no posee, pero, de otro, puede acarrearle consecuencias negativas. De ahí que el REEDS estipule que cuando las personas ejerzan este derecho, se les informará de que la restricción del acceso puede repercutir en la calidad de la prestación de la asistencia sanitaria que se les preste. En todo caso, tal negativa perdería efecto en caso de que una emergencia vital hiciera necesario acceder a estos datos para el profesional sanitario.

La cuestión del uso secundario de datos

Introducción: la filosofía de fondo del REEDS en torno al uso secundario de datos de salud

Explicado ya lo esencial acerca de los cambios en el uso de los datos para fines clínico, hora es ya de abordar la cuestión de su uso secundario para fines de particular importancia en las sociedades actuales, como, por ejemplo, “la investigación, la innovación, la formulación de políticas, la preparación y respuesta ante las amenazas para la salud, incluidas la prevención y respuesta ante futuras pandemias, la seguridad de los pacientes, la medicina personalizada, las estadísticas oficiales o las actividades de regulación” (Considerando 1). Pues bien, en torno a este tema conviene comenzar destacando el artículo 53 del REEDS, y, en particular, su letra e), que es la que incluye entre tales fines “la investigación científica relacionada con el sector sanitario o asistencial que contribuya a la salud pública o a la evaluación de tecnologías sanitarias o que procure niveles elevados de calidad y seguridad de la asistencia sanitaria, de los medicamentos o de los productos sanitarios, con el objetivo de beneficiar a los usuarios finales, como los pacientes, los profesionales sanitarios y los administradores sanitarios, incluidas: i) las actividades de desarrollo e innovación para productos o servicios; ii) el entrenamiento, la prueba y la evaluación de algoritmos, también con respecto a productos sanitarios, productos sanitarios para diagnóstico in vitro, sistemas de IA y aplicaciones sanitarias digitales”.

Como cabe apreciar, la intención del REEDS está clara: poner a disposición de quien desee acometer los objetivos de investigación e innovación citados en este artículo todos los datos necesarios al efecto. Ahora bien, ¿cómo se articulará esta intención? ¿De qué datos estamos hablando? ¿Cuál será el papel del ciudadano/paciente? ¿Cómo se sufragará todo esto? En los siguientes apartados intentaremos responder a estas preguntas.

Los datos y sus titulares. ¿De qué datos estamos hablando? Catalogando los datos existentes

Empecemos por lo esencial. El REEDS tiene como objeto los “datos sanitarios electrónicos”. Este es un concepto amplísimo, en tanto que abarca los datos relativos a la salud y los datos genéticos, tal como se definen en el Reglamento (UE) 2016/679 (RGPD), pero también los datos relativos a factores determinantes de la salud, o los datos tratados en relación con la prestación de servicios sanitarios, que se traten en formato electrónico, como señala el artículo 51. También los “datos sanitarios electrónicos no personales”, esto es, los relativos a datos sanitarios y genéticos en formato electrónico, que hayan sido anonimizados de manera que ya no se relacionen con una persona natural identificada o identificable, así como los datos que nunca se hayan relacionado con un sujeto de datos, esto es, los datos anónimos en sentido estricto. El REEDS aclara, en todo caso, que, siguiendo el

principio de minimización de datos del RGPD, en general sólo se permitirá el acceso a los datos personales cuando la investigación no pueda desarrollarse con datos anonimizados. E, incluso en este caso, será necesario pseudonimizar los datos previamente.

Dichos datos, a su vez, han de estar en poder de un tenedor de datos, esto es, toda persona física o jurídica, autoridad pública, agencia u otro organismo del sector de la asistencia sanitaria o el asistencial, que tengan el derecho o la obligación, de conformidad con el Derecho de la Unión o nacional aplicable y en su calidad de responsable o corresponsable del tratamiento, de tratar datos de salud electrónicos personales, o la capacidad de poner a disposición datos de salud electrónicos no personales mediante el control del diseño técnico de un producto y de los servicios conexos. Se trata, por tanto, de una categoría amplísima, que incluye de hecho a todos aquellos agentes que operen en el sector de la salud bajo cuyo control se encuentran grandes bases de datos de salud o genéticos, salvo (artículo 50.1 (b)) los investigadores individuales, las personas naturales y las microempresas, salvo que los Estados miembros decidan lo contrario a través de su normativa nacional (art. 50.2).

Pues bien, todos estos tenedores de datos tendrán, en primer lugar, la obligación de declarar la existencia de las bases de datos que se encuentren bajo su control. De esta forma, se hará posible la creación de un catálogo de conjuntos de datos disponibles en la UE y evaluar su posible utilidad para una acción concreta. Con ello conseguiremos obtener, por primera vez, información precisa sobre las bases de datos y sus características esenciales, de tal modo que sea posible optimizar su uso para fines de investigación e innovación por parte de los usuarios de datos.

La articulación del sistema. Usuarios de datos y Organismos de Acceso

A partir del conocimiento de la existencia de esos datos, cualquier usuario podrá acceder libremente a ellos en aras de lograr alguno de los fines previstos en el artículo antes citado. Es importante subrayar que estos usuarios pueden ser personas o empresas radicadas en la UE o no. No hay nada en el REEDS que permita concluir que se limita el acceso a los datos a las empresas o personas externas a la UE, siempre que obtengan las autorizaciones administrativas que el Reglamento impone. Es, de hecho, importante remarcar que tanto usuarios de datos como tenedores de datos pueden ser entes públicos o empresas privadas, personas jurídicas o personas naturales, trabajando en su propio beneficio o por encargo de un tercero de carácter público, sin que todo ello implique diferencias relevantes, más allá de las que afectan a algunas de las finalidades previstas en el artículo 53, que exploraremos más adelante, o los matices que cabe hallar en torno a la figura de la autoexclusión u opt-out, también a analizar en otro apartado de este Informe¹⁴.

Ahora bien, el acceso a los datos no será directo, sino a través de una figura que ha sido creada especialmente para servir como garante de todo el proceso: los Organismos de Acceso a los Datos (OAs). Estas entidades, de naturaleza eminentemente administrativa, desempeñarán un papel crucial en la supervisión y facilitación del acceso a los datos electrónicos en los Estados miembros que dependan de ellos, así como en la consecución de una aplicación coherente del REEDS. El artículo 55 y ss del Reglamento son los encargados de regular los OAs. En ellos se define que habrá al menos un Organismo de Acceso en cada Estado miembro, sin que se descarte que pueda haber más y tendrán carácter de organismos públicos. Su composición puede variar sustancialmente de unos casos a otros. En algunos casos serán organismos ya existentes que pasen a actuar como tales, mientras que en otros se crearán *ex novo*.

El proceso: los permisos de datos

Una vez definidos ya sus principales actores, podemos describir cuál será el procedimiento de acceso a los datos. En general, este se articulará en torno a una herramienta clave, el permiso de datos, que está regulada en el artículo 67 del REEDS. El procedimiento de acceso comienza cuando un usuario solicita uno de estos permisos, proporcionando a los organismos de acceso a los datos sanitarios varios elementos de información que los ayuden a evaluar la solicitud y decidir si el solicitante puede recibirlo, incluyendo: la base jurídica que avala su acceso a los datos (ejercicio de una misión de interés público asignada por ley o interés legítimo), los fines para los que se utilizarían los datos, la descripción de los datos necesarios y las posibles fuentes de datos, una descripción de las herramientas necesarias para tratar los datos, así como las características del entorno seguro que se necesitan, el periodo durante el que se tratarán los datos en ese entorno, las garantías previstas para asegurar que no haya un mal uso de los datos y para proteger los derechos e intereses de las personas asociadas a los datos, etc. En el caso de que se pidan datos sujetos a un *opt out*, también deberán aducir la razón por la que se necesiten esos datos de manera insoslayable.

Cuando se solicite el acceso a los datos personales en formato pseudonimizado, el solicitante de datos deberá explicar por qué es necesario y por qué los datos anonimizados no serían suficientes. También deberá incluir una descripción del modo en que el tratamiento cumpliría la legislación nacional y de la Unión aplicable en materia de protección de datos y privacidad. A su vez, podrá solicitarse una evaluación ética con arreglo al Derecho nacional. En el caso de nuestro país, esto implicaría, en la práctica, una evaluación previa de un comité de ética de la investigación, que deberá ser un comité de ética de la investigación con medicamentos y productos sanitarios (CEIm) si el sistema que se pretende desarrollar o entrenar gracias al acceso a los datos es un producto sanitario.

Los organismos de acceso a los datos sanitarios y, en su caso, los tenedores de datos, deberán ayudar a los usuarios de datos en la selección de los conjuntos de datos o fuentes de datos adecuados para la finalidad prevista del uso secundario. El organismo de acceso correspondiente evaluará la solicitud y si la considera pertinente otorgará al solicitante un permiso de datos en un plazo de tres meses a partir de la recepción de la solicitud, extensible a seis.

Una vez presentada la solicitud, los organismos de acceso a los datos decidirán conceder el acceso a los datos sanitarios electrónicos en función de si se cumplen o no una serie de criterios acumulativos (apartado 1 del artículo 68 del REEDS). Caso de que se conceda, el tratamiento deberá tener lugar, en general, en espacios seguros, en los que se garantice que no se incumple lo estipulado por el propio REEDS. La duración del permiso de datos será exclusivamente la duración necesaria para cumplir con los fines solicitados, el cual no deberá exceder los diez años. Esta duración puede ser extendida una vez, a solicitud del usuario de los datos de salud, basándose en argumentos y documentos que justifiquen esta extensión presentados, un mes antes de la expiración del permiso de datos, por un período que no puede exceder los diez años. El organismo de acceso a los datos sanitarios podrá cobrar tasas crecientes para reflejar los costes y riesgos de almacenar los datos sanitarios electrónicos durante un periodo de tiempo más largo que el periodo inicial. También podrá, a fin de reducir dichos costes y tasas, proponer al usuario de los datos sanitarios que almacene el conjunto de datos en un sistema de almacenamiento con capacidades reducidas.

Existe un procedimiento acelerado que se activará para los organismos del sector público y las instituciones, órganos y organismos de la Unión con un mandato legal en el ámbito de la salud pública si el tratamiento de los datos debe llevarse a cabo para los fines previstos en el artículo 53, apartado 1, letras a), b) y c). En virtud de este procedimiento acelerado, los organismos de acceso expedirán o denegarán un permiso de datos en un plazo de dos meses a partir de la recepción de una solicitud de acceso a datos completa. Podrán ampliar el plazo de respuesta a una solicitud de acceso a datos en un mes adicional cuando sea necesario (su artículo 68.6).

Por fin, conviene destacar que, si el usuario de datos considera que puede alcanzar los objetivos de su investigación a través de datos anonimizados, puede sustituir el largo proceso de obtención de un permiso de datos formulando una solicitud directa de información en formato estadístico anonimizado, siguiendo lo previsto en el artículo 69 del REEDS.

El papel del paciente. El derecho de auto exclusión u opt out.

De cara a preservar la autonomía del paciente el REEDS dota a este de un derecho a optar por no participar, o derecho de autoexclusión, recogido en su artículo 71, apartado 1.

En su virtud, las personas podrán negarse a que se otorguen permisos que incluyan sus datos personales para los fines previstos. El REEDS especifica que serán los organismos de acceso de cada Estado miembro los que establezcan un mecanismo de exclusión voluntaria accesible y fácilmente comprensible, mediante el cual se ofrecerá a las personas físicas la posibilidad de manifestar explícitamente su voluntad a tal efecto. Será también imperativo proporcionar a las personas físicas información suficiente y completa sobre este derecho, incluyendo sus beneficios y desventajas. Las personas físicas no estarán obligadas a dar ninguna razón para optar por no participar y deberían tener la posibilidad de reconsiderar su elección en cualquier momento. Sin embargo, para ciertos propósitos con un fuerte vínculo con el interés público, se prevé la posibilidad de que los Estados miembros establezcan, en función de su contexto nacional, un mecanismo para proporcionar acceso a los datos de las personas naturales que hayan ejercido el derecho de exclusión, para garantizar que se puedan poner a disposición conjuntos de datos completos en esas situaciones. La normativa contempla este supuesto si se dan tres condiciones acumulativas descritas en su artículo 71.4, básicamente que la investigación la realice una entidad pública, que los datos no puedan obtenerse por medios alternativos de manera oportuna y eficaz en condiciones equivalentes y que el usuario de datos justifique la necesidad de su tratamiento.

¿Una mejora significativa?

Una cuestión que merece la pena analizar es si, o de qué forma, el REEDS mejora nuestra normativa nacional en torno al uso secundario de datos. La respuesta aquí debería ser que, efectivamente, lo mejora, pero menos que en otros países, en los que este uso todavía se basa exclusivamente en el consentimiento, porque aquí nuestra normativa nacional ya nos había dado ciertas posibilidades, a través de la Disposición Adicional Decimoséptima de la LOPDyGDD.

El cambio más importante es que el EEDS permitirá resolver definitivamente el problema que implica la obligación que impone el artículo 2(d)1º de la DA17 de la LOPD y GDD, esto es, que, cuando los datos se quieran utilizar sin el consentimiento de los pacientes, concurra “una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación”. Esta condición ha creado muchos problemas, porque no es fácil asegurar esa separación en la práctica. En el marco trazado por el REEDS, es obvio que esta separación existirá, ya que los usuarios de datos accederán a una información ya seudonimizada, sin que en ningún momento traten los datos personales identificativos. Por tanto, el EEDS facilitará las cosas en estos términos.

Obviamente, hay que tener presente que este sistema introducido por el EEDS, como ya hemos señalado

anteriormente no supone sino una alternativa al sistema actual, sino en todo caso un complemento. Esto quiere decir que podrá seguir realizándose investigación basada en el uso secundario de datos con el consentimiento de los interesados. Y en algunos casos será muy pertinente, sobre todo si la investigación no puede realizarse con datos seudonimizados.

Conclusión

En definitiva, lo que dicta el REEDS es un sistema que, en general, permite que se puedan utilizar los datos de salud de los individuos, siempre pseudonimizados, salvo que estos digan lo contrario a través de los mecanismos creados al efecto, y siempre que no concurran en las excepciones anteriormente definidas. Gracias a esta nueva norma, el consentimiento no será ya la base legal fundamental para el tratamiento de datos de investigación. Por supuesto, esto facilitará el acceso a datos para la investigación y la salud pública. Se accederá a una mayor cantidad de datos de manera más ágil, fundamental para fines científicos y estadísticos.

También mejorará la eficiencia en los proyectos de investigación y reducirá la carga para los responsables del tratamiento de datos, ya que no tendrán que recolectar activamente el consentimiento de cada individuo o sufrir el bloque de los que no quieren otorgarlo. Con el REEDS, ello requerirá que los ciudadanos sean quienes tomen la iniciativa para manifestar el deseo de que no se utilicen sus datos de salud. El grado en el que se acogerán a él dependerá, obviamente de varios factores. Sobre todo, dependerá de que estén adecuadamente informados sobre este derecho. Aunque, en la práctica, no todos cuenten con el mismo nivel de conocimiento ni de acceso a la información sobre sus derechos, ni estén al tanto de la repercusión del uso secundario de sus datos.

Declaración de autoría

Iñigo de Miguel Beriain concibió el artículo y redactó su primer borrador. Mónica Loyo Menoyo revisó el borrador, añadió notas y lo adecuó a los requerimientos de la revista. Todos los autores aprobaron la versión final. Iñigo de Miguel Beriain es el responsable del artículo.

Financiación

Esta publicación se ha realizado en el marco del Grupo de Investigación del Sistema Universitario Vasco en Ciencias Sociales y Jurídicas aplicadas a las Nuevas Tecnologías (GI CISJANT, ref. IT1541-22), y del proyecto «GODAS: Gobernanza de los usos secundarios de datos de salud y genéticos en espacios compartidos» (PID2022-1371400B-I00) concedido por la Agencia Estatal de Investigación española.

Conflicto de intereses

Los autores declaran que no existe conflicto de interés alguno.

Bibliografía

1. 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) Disponible en <https://www.boe.es/doue/2016/119/L00001-00088.pdf>
2. Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R0868>
3. Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) nº 178/2002 y el Reglamento (CE) nº 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo. Disponible en <https://www.boe.es/buscar/doc.php?id=DOUE-L-2017-80916>
4. DI FEDERICO, Giacomo, From Dusk Till Dawn. The Case of FT v DW and the Right to Access Electronic Medical Records in Light of the Future European Health Data Space Regulation. *European Papers-A Journal on Law and Integration* nº2, 2024, p. 463-77.
5. KOTSARELI, Kalliopi; TSACHOURIDIS, Petros, European Health Data Space: A New Era in EU Health. *HAPSc Policy Briefs Series vol.4, nº2,*, 2023, p. 91-6.
6. DI FEDERICO, Giacomo, From Dusk Till Dawn. The Case of FT v DW and the Right to Access Electronic Medical Records in Light of the Future European Health Data Space Regulation. *European Papers-A Journal on Law and Integration*, 2024 (2), p. 463-77.
7. BORGOGNO, Oscar; COLANGELO, Giuseppe, Data sharing and interoperability: Fostering innovation and competition through APIs. *Computer Law & Security Review*, 2019, 35 (5), p. 105314.
8. DE HERT, Paul, et al., The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*. 2018, 34 (2) p. 193-203.
9. JORQUI AZOFRA, María, El derecho a la portabilidad de los datos en el Espacio Europeo de Datos Sanitarios, en GIL MEMBRADO, Cristina y LUQUIN BERGARECHE, Raquel, *Salud Digital, Aplicaciones móviles, telemedicina y chatbots*. Dykinson, 2024, pp. 183-232
10. LI, Wenkai; QUINN, Paul, The European Health Data Space: An expanded right to data portability? *Computer Law & Security Review* v2024 (52), p. 105913
11. GALLEGO RIESTRA, Sergio; RIAÑO GALÁN, Isolina, ¿Tiene el paciente derecho a saber quiénes y por qué han accedido a su historia clínica? *Revista Derecho y salud*, 2012(22), p. 85-95.
12. RECUERO, Mikel, El Espacio Europeo de Datos de Salud: retos y oportunidades para la protección de datos de carácter personal, en BUENO DE MATA, Federico (dir.) / GONZÁLEZ PULIDO, Irene (coord.), *Fodertics 10.0: estudios sobre derecho digital*, Comares, Granada, 2022, pp. 389
13. DE MIGUEL BERIAIN, Iñigo, El uso de datos de salud para investigación biomédica a la luz de la Propuesta del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios, *Revista Jurídica de Castilla y León*, 2023 (60), pp. 7 ss.
14. NAVAS NAVARRO, Susana, Datos sanitarios electrónicos: el espacio europeo de datos sanitarios, Reus, 2023.
15. RECUERO LINARES, Mikel El uso secundario de datos de salud electrónicos: el futuro Reglamento del Espacio Europeo de Datos de Salud y su interacción con la protección de datos personales, *InDret* 2024 (2) ,pp. 525-51.
16. DE MIGUEL BERIAIN, Iñigo, El uso de datos de salud para investigación biomédica a la luz de la Propuesta del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios, *Revista Jurídica de Castilla y León* 2023 (60), pp. 7 ss.