*Revista de Derecho y Genoma Humano, 62 – enero-diciembre 2026*

*Law and the Human Genome Review*

*e-ISSN 2605-1230*

*https://doi.org/10.1387/rdgh.28714*

**Doctrina / Articles**

Versión anticipada / Online first

# Los Actores del Espacio Europeo de Datos de Salud en la gobernanza del uso secundario de los datos de salud electrónicos

Laura Centeno Casado

Investigadora Predoctoral.

Instituto de Filosofía Consejo Superior de Investigaciones Científicas, Grupo de Ética Aplicada.

Facultad de Derecho, Universidad de Murcia, Grupo Innovación, Derecho y Tecnología. [1]

[1] Este artículo forma parte de la tesis doctoral de Laura Centeno Casado en el programa de doctorado «Bio-derecho: Bioética, Salud y Derechos Humanos» de la Universidad de Murcia, España, así como de las actividades de la unidad asociada BESO y de la Red de Enfermedades Raras del CSIC (rer-biomed.csic.es). Este trabajo ha sido financiado por el contrato de doctorado «Salud digital en España» (n.º de ref. CSIC JAEPR23093) y por el proyecto «HALO: un modelo de gobernanza de datos de confianza cero para el intercambio altruista de datos sanitarios» (CSIC PIE 202410E127). A su vez, la comunicación de este artículo fue galardonada con el Premio Carlos María Romeo Casabona en el XXXI Congreso Internacional sobre Derecho y Genoma Humano.

**Resumen:** El artículo analiza el Reglamento (UE) 2025/327, que establece un nuevo marco para el uso primario y secundario de datos de salud. Se detalla cómo deben preparase los nuevos actores afectados ante obligaciones legales, retos y oportunidades con el objetivo de proponer mecanismos de coordinación y gobernanza para su implementación efectiva.

**Palabras clave:** uso secundario, Espacio europeo de datos de salud, tenedores de datos, usuarios de datos, comités de ética de la investigación.

**Abstract:** The article analyses Regulation (EU) 2025/327, which establishes a new framework for the primary and secondary use of health data. It sets out how the new stakeholders concerned should prepare for the legal obligations, challenges and opportunities involved, with the aim of proposing coordination and governance mechanisms to ensure its effective implementation.

**Keywords:** secondary use, European health data space, data holders, data users, research ethics committees.

Versión anticipada / Online first

## I. Introducción

El Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud (en adelante, REEDS), representa un hito fundamental en la configuración de la transformación digital de los sistemas sanitarios de los Estados Miembros de la Unión Europea[2]. Este marco normativo que entró en vigor el 25 de marzo de 2025 establece un ecosistema complejo de actores interconectados cuyo objetivo principal es facilitar tanto el uso primario como el uso secundario de los datos de salud electrónicos, intentando equilibrar la protección de los derechos fundamentales con las necesidades de investigación, innovación y mejora de la asistencia sanitaria[3].

A su vez, la gestión de los datos electrónicos de salud, por su naturaleza, presenta características únicas que la distinguen de otros ámbitos de tratamiento de datos personales. Los datos de salud, catalogados como categoría especial de datos personales según el artículo 9 del Reglamento (UE) 2016/679 General de Protección de Datos (en adelante, RGPD),[4] requieren un nivel de protección reforzado debido a su especial sensibilidad y a su íntima conexión con la dignidad de la persona y el derecho fundamental a la vida privada y familiar[5], más allá del propio derecho a la protección de datos personales. Sin embargo, estos mismos datos constituyen un recurso con enorme potencial para promover el avance en la investigación biomédica, la medicina personalizada y la mejora de las políticas de salud pública, entre otros fines que el REEDS considera como prioridades para promover la compartición de los datos de salud y maximizar el valor e impacto que pueden tener para uso sistemas de salud más eficientes y resilientes[6].

Para poder lograr estos objetivos, el Espacio Europeo de Datos de Salud establece en sus artículos, concretamente en el capítulo cuatro, una propuesta de modelo de gobernanza multinivel; ya que involucra diversos actores con roles y responsabilidades específicas. En el reglamento se recogen los siguientes actores: organismos de acceso a datos, tenedores de datos, usuarios de datos,

Versión anticipada / Online first

[2] Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847, DOUE L 327, 5 de marzo de 2025.

[3] CASANOVA ASENCIO, Andrea Salud, «Espacio Europeo de Datos Sanitarios, uso primario y autonomía del paciente», en ANDREU MARTÍNEZ, María Belén (Dir.), Los datos de salud como eje de la transformación digital de la sanidad, Comares, Granada, 2023, pp. 107-135.

[4] 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), DOUE L 119, 4 de mayo de 2016.

[5] MARTÍNEZ NAVARRO, Enrique, «Argumentos éticos para fundamentar una política de protección de datos de salud coherente con las convicciones morales compartidas», en ANDREU MARTÍNEZ, María Belén (Dir.), Los datos de salud como eje de la transformación digital de la sanidad, Comares, Granada, 2023, pp. 1-16.

[6] ANDREU MARTÍNEZ, María Belén, «La necesaria actualización de la Ley de Autonomía del Paciente frente a los retos en la gestión de datos de salud», en ANDREU MARTÍNEZ, María Belén (Dir.), Los datos de salud como eje de la transformación digital de la sanidad, Comares, Granada, 2023, pp. 139-159.

autoridades de salud digital[7]. Esta multiplicidad de actores genera un entramado complejo de relaciones y responsabilidades jurídicas que requiere una coordinación efectiva para garantizar tanto la protección de los derechos de los interesados como la consecución de los objetivos de salud pública e investigación científica[8].

Los comités de ética de la investigación (CEIs) emergen en este contexto como actores centrales en la evaluación y supervisión del uso secundario de datos electrónicos de salud, asumiendo funciones que van más allá de su rol tradicional en la investigación biomédica[9]. Su intervención resulta especialmente crítica en un escenario donde la digitalización masiva de datos de salud y las técnicas que pongan a disposición un gran volumen de datos, son susceptibles de perpetuar o generar nuevos dilemas éticos que requieren una aproximación diversa e interdisciplinar.

El presente artículo parte de la hipótesis de que el éxito de la implementación del REEDS depende, en gran parte, de la articulación efectiva de un sistema de gobernanza multinivel que logre equilibrar tres elementos. En primer lugar, el encuadre de la protección reforzada de los datos de salud como categoría especial de datos personales, adaptándose y conociendo en profundidad las especificidades del nuevo marco que se ofrece para pacientes, profesionales, de la salud y demás agentes y la complementariedad con el tratamiento de datos de salud personales, incluyendo por diseño en la evaluación las salvaguardas en el tratamiento de datos personales. En segundo lugar, en el contexto del uso secundario de los datos de salud, incidir en la necesidad de facilitar el acceso a estos datos para fines de investigación e innovación sanitaria a aquellos que puedan obtener esos datos contribuyendo a la mejora del diagnóstico y tratamiento de distintas enfermedades, teniendo presente las salvaguardas jurídicas en el cumplimiento de la normativa nacional y europea, y las éticas que ya existían y que el REEDS complementa. Y el tercer elemento, aunando en la diversidad y multiplicidad de actores que se abren en la implementación del uso secundario de los datos de salud, el necesario desarrollo de una gobernanza funcional, que debe incluir una supervisión ética especializada que garantice el cumplimiento normativo y los principios de la bioética; autonomía, beneficencia, no maleficencia y justicia. Éste último especialmente, es relevante para aquellos que abordan el Espacio Europeo de Datos de Salud desde una perspectiva jurídica.

Por consiguiente, en esta propuesta se incide en incentivar la monitorización y evaluación del impacto ético durante todo el proceso de tratamiento de datos de salud, estén o no en formato

Versión anticipada / Online first

[7] LUQUIN BERGARECHE, Raquel, «Reutilización o uso secundario de los datos personales de salud», en EGUSQUIZA BALMASEDA, María Asunción / et al. (Coords.), Régimen jurídico de protección de datos de salud en el Espacio Europeo de Datos de Salud (EEDS), Colex, Madrid, 2025, pp. 200-260.
[8] TORRIJOS VALERO, Julián, «La reutilización de la información sanitaria desde la perspectiva de la regulación europea sobre gobernanza de datos», en ANDREU MARTÍNEZ, María Belén (Dir.), Los datos de salud como eje de la transformación digital de la sanidad, Comares, Granada, 2023, pp. 45-68.
[9] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, «Condiciones para el acceso y tratamiento de los datos de salud. Guía de preguntas frecuentes y propuestas», Proyecto BIODAT, junio de 2023. Disponible en: https://www.aepd.es (fecha de consulta: 3 de junio de 2026).

anonimizado y seudonimizado. A través del análisis de la normativa relativa a datos de salud, con especial atención a las obligaciones, responsabilidades y funciones de cada actor, el artículo tratara de proporcionar una serie de recomendaciones que puedan contribuir a la eficacia del sistema, haciendo énfasis en la necesidad de clarificación y armonización de las responsabilidades de los distintos actores, particularmente en lo que respecta a la cadena de custodia y tratamiento en el uso secundario de datos de salud electrónicos.

## II. Marco Normativo y Actores del Espacio Europeo de Datos de Salud.

### 1. Fundamentos normativos en materia de datos de salud.

El Espacio Europeo de Datos de Salud forma parte de dos políticas públicas en la agenda de la Unión Europea; la Estrategia Europea de Datos y la construcción de la Unión Europea de la Salud[10]. El desarrollo normativo para la implementación de estas políticas tiene sus orígenes en la armonización en el tratamiento de datos personales, específicamente en el Reglamento General de Protección de Datos (RGPD). Sin embargo, su evolución y sectorización; tal y como ocurrió con la Directiva (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos; introducen especificidades que responden a las particularidades del sector sanitario y a los objetivos de armonización e interoperabilidad transfronteriza entre los estados miembros de la Unión Europea. Desde el mandato genérico de que los Estados miembros son los responsables de su política sanitaria (art. 168 TFUE), derivan obligaciones que a su vez tienen que profundizarse y concretarse en su propia jurisdicción nacional. El REEDS, viene a dar una mayor fuerza al compromiso de la Unión Europea en su conjunto con los estados miembros de fortalecer el mercado interior (Artículo 114 TFEU) y la mejora de la asistencia sanitaria de todos los ciudadanos europeos. De hecho, el Reglamento proviene, al igual que paso con el RGPD, de la Directiva 2011/24/UE[11] establecida con el fin de mejorar la asistencia sanitaria transfronteriza, mediante la puesta en marcha a nivel administrativo e institucional, las condiciones efectivas desde la Unión Europea en coordinación con los Estados Miembros para el pleno ejercicio del derecho fundamental a la protección de la salud[12].

Respecto los principios fundamentales en los que se basa el Derecho de la Unión Europea, los Estados Miembros asumen nuevas obligaciones marcadas por la obligatoriedad del cumplimiento

[10] Art. 2.2.a) del Reglamento (UE) 2025/327.
[11] 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, s. f.
[12] CABALLERO PÉREZ, María José, «El derecho a la salud en el ámbito internacional y de la Unión Europea. Tratamiento actual y desafíos futuros», Revista de Derecho de la Seguridad Social, Núm. Extra 4, 2022, pp. 55-83.

Versión anticipada / Online first

del REEDS. Ejemplo de ello es la obligación de los Estados miembros a la designación de autoridades de salud digital sobre las que se exige la imparcialidad, especialmente la desconexión de intereses económicos con su actividad institucional; el establecimiento de las excepciones del acceso de las personas físicas a determinadas categorías de derechos[13]. Esto es una muestra de la intención de reforzar a través de las instituciones la gobernanza y cumplimiento con independencia, teniendo más presente la monitorización y control del proceso de digitalización de los sistemas de salud de todos los países europeos. Un aspecto relevante en este tipo de mandatos, son las características de cada Estado Miembro en cuestión de competencias en política social y sanitaria.

Otra novedad y palanca de cambio que proporciona la implementación del REEDS es la distinción clara entre el tratamiento de los datos según el uso que se les dé a esos datos, siendo los fines de tratamiento el aspecto clave para esta diferenciación. En el uso primario el tratamiento de datos tiene como fin la prestación de asistencia sanitaria al interesado, incluyendo el diagnóstico, el tratamiento y servicios de medicina preventiva. En el caso del uso secundario, éste engloba el tratamiento de datos para fines que trascienden la atención sanitaria individual, incluyendo la investigación, la innovación, la elaboración de políticas públicas, la preparación y respuesta ante emergencias sanitarias, las actividades regulatorias, o incluso la posibilidad de entrenamientos de modelos de Inteligencia Artificial, cuando dicho entrenamiento responda a alguno de los fines permitidos por el artículo 53 del REEDS[14].

Esta distinción resulta esencial para comprender el marco de gobernanza establecido, ya que cada modalidad de uso implica diferentes actores, procedimientos y salvaguardas organizaciones y técnicas para cumplir con los fundamentos normativos que generan obligaciones. Mientras que el uso primario se rige por principios consolidados del derecho sanitario y la protección de datos, el uso secundario requiere mecanismos específicos de autorización, supervisión y control que constituyen el núcleo innovador promovido por el Espacio Europeo de Datos de Salud.

## 2. Los organismos de acceso a datos de salud.

Los organismos de acceso a datos de salud son una entidad clave para el uso secundario de los datos sanitarios. Según el artículo 36 del REEDS, cada Estado miembro debe designar uno o varios organismos nacionales de acceso a datos de salud, los cuales actuarán como intermediarios

[13] Considerandos 30 y 10 del Reglamento (UE) 2025/327.

[14] Art. 2.2. aa) y 53 del Reglamento (UE) 2025/327.

Versión anticipada / Online first

especializados entre los tenedores de datos y los usuarios que soliciten acceso para uso secundario[15].

Estos organismos asumen funciones críticas en el ecosistema del REEDS como pueden ser (a) recepción y evaluación de solicitudes de acceso a datos de salud electrónicos; (b) verificación del cumplimiento de los requisitos legales y éticos para el acceso; (c) expedición de permisos de datos de salud; (d) supervisión del cumplimiento de las condiciones establecidas en los permisos; y (e) imposición de medidas correctivas o sancionadoras en caso de incumplimiento. Estos organismos son la puerta de salida y entrada, siendo a la vez las instituciones que garantizan el cumplimiento de que el proceso de permisos, acceso, control y desarrollo del tratamiento de los datos de salud electrónicos no personales conforme a los dispuesto en el REEDS.

El REEDS establece requisitos de independencia funcional y técnica que deben garantizar la objetividad de las decisiones y los motivos por los cuales permiten o deniegan al usuario, su petición de acceso a los datos. Sin embargo, la concreción de esta independencia en los ordenamientos nacionales, como puede ser la competencia sanitaria a nivel regional, puede presentar variaciones significativas que afecten la armonización pretendida por el REEDS[16]. La diversidad de las características de los sistemas sanitarios en los diferentes estados miembros de la Unión Europea plantea importantes retos de gobernanza en la configuración y puesta en marcha de la coordinación y designación de los organismos de acceso a datos, afectando a su vez a la implementación en la práctica del uso secundario de los datos de salud[17].

Teniendo en cuenta la importancia de las funciones del organismo de acceso a datos, y los diferentes fines para el uso secundario de datos de salud electrónicos, resulta especialmente relevante que empiecen a prepararse, contando con una formación y concienciación multidisciplinar que incluya el desarrollo de competencias jurídicas, técnicas, éticas y sanitarias. Esta configuración responde a la complejidad inherente a la evaluación de solicitudes de acceso a datos sanitarios, que requiere una comprensión integral de los aspectos técnicos del tratamiento de datos, las implicaciones éticas de su uso, técnicas de seudonimización y anonimización; y la capacidad de monitorear y sancionar la mala praxis en el uso de los datos, siendo los guardianes y encargados del cumplimiento y el respeto de los fines legítimos, en especial, cuando los usos legítimos se abren más allá del sector público. Los usos a los que se deberá prestar atención desde la perspectiva jurídica, debido a la legislación europea y complementaria relativa a los mismos, son los fines educativos y formativos en el sector

Versión anticipada / Online first

[15] Capítulo IV del Reglamento (UE) 2025/327.
[16] SÁNCHEZ GARCÍA, Alfonso, «El altruismo de datos en el ámbito sanitario», en ANDREU MARTÍNEZ, María Belén (Dir.), Los datos de salud como eje de la transformación digital de la sanidad, Comares, Granada, 2023, pp. 69-105.
[17] QUINN, Paul, «Health Data Access Bodies under the European Health Data Space – A technocratic colossus or rubber stamp forum?», Technology and Regulation, 2025, pp. 60-80. Disponible en: https://doi.org/10.71265/vbfvpb76 (fecha de consulta: 3 de junio de 2026).

de la salud o la mejora de la prestación de los servicios relacionados con los cuidados de la salud. No obstante, dónde el rol de los organismos de acceso a datos va a necesitar prestar más atención, es el fin de la letra (e) del Artículo 53, la investigación científica relacionada con la salud, incluyendo actividades de desarrollo e innovación de productos o servicios; y especialmente en la formación, ensayo y evaluación de algoritmos, incluidos los utilizados en productos sanitarios para diagnóstico in vitro, sistemas de inteligencia artificial y aplicaciones de salud digital[18].

La configuración de los criterios de actuación para autorizar o denegar el acceso de los usuarios de los datos de salud, debe tener en cuenta desde el principio del proceso qué medidas técnicas, legales y organizativas se les deben exigir desde el organismos de acceso a datos a los usuarios de datos, para evitar y prevenir que el desarrollo del tratamiento del uso secundario de los datos electrónicos de salud, puedan transformarse durante la investigación o desarrollo del producto que se pueda caer en los fines prohibidos del REEDS como la toma de decisiones en relación con una persona física o un grupo de personas físicas que dé lugar a una discriminación contra ellas sobre la base de los datos sanitarios obtenidos o que, y esto a nivel nacional, actividades que contravengan las disposiciones éticas establecidas en la legislación nacional[19]. Es en este punto, la relevancia de los CEIs que será analizada con posterioridad juega un papel relevante a la hora de poder tener claro el marco por el cual se puede autorizar o no el uso secundario y las salvaguardas no solo normativas sino éticas que operan actualmente en la investigación científica con datos de salud, en escenarios es el desarrollo de dispositivos médicos o ensayos clínicos.

Por último, los organismos de acceso a datos para poder evaluar solicitudes de acceso a datos con fines de investigación científica, deben coordinar la interpretación del concepto los fines del tratamiento de con fines de investigación científica más allá de las excepciones del Artículo 89 del RGPD y las disposiciones nacionales.[20] El propio Comité Europeo de Protección de Datos recalca en su última consulta pública, en que no existe una definición universalmente aceptada de investigación científica y en la necesidad de aclarar el concepto de tratamiento de datos personales con fines de investigación científica[21].

Aunque los datos que se vayan a utilizar son por defecto anonimizados, en pleno cumplimiento con los principios de protección de datos personales, como el principio de minimización de datos por

Versión anticipada / Online first

[18] Artículo 53.2 Reglamento (UE) 2025/327.
[19] DE MIGUEL BERIAIN, Íñigo / LÓPEZ DE LA PEÑA DE PABLO, Mercedes / LOYO-MENOYO, Mónica, «El nuevo reglamento europeo relativo al espacio europeo de datos de salud: su impacto en la gobernanza del dato y su uso ético y seguro», Revista de Derecho y Genoma Humano / Law and the Human Genome Review, Núm. 61, 2025, pp. 59-82, DOI: 10.1387/rdgh.27342.
[20] RECUERO, Mikel, «La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado», [Premios de Investigación en Protección de Datos Personales Emilio Aced, 2020-02.],
[21] EDPB – COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Guidelines 2026/01 on Scientific Research under the GDPR, 2026. Disponible en: https://www.edpb.europa.eu/system/files/2026-04/edpb_guidelines_202601_scientificresearch_en.pdf (fecha de consulta: 3 de junio de 2026).

defecto. Aun así, habrá casos, debido a necesidades justificadas, se otorgará acceso a datos seudonimizados; y esto abre la necesidad de entender los entornos de tratamiento seguro como una caja cerrada y confiable; la cual debe asegurarse antes de la solicitud por parte del tenedor y el usuario, durante y después del proceso; para asegurar el cumplimiento del REEDS, por parte de autoridades independientes con potestades y recursos[22].

### 3. Los tenedores de datos de salud.

El concepto de tenedor de datos de salud engloba a una amplia variedad de entidades que disponen de datos de salud electrónicos susceptibles de ser utilizados para fines secundarios. El artículo 2.2.l) del Reglamento define esta categoría de manera inclusiva, abarcando tanto entidades del sector público, incluyendo servicios de salud, autoridades sanitarias, organismos de investigación públicos; como del sector privado, hospitales privados, empresas farmacéuticas, desarrolladores de dispositivos médicos.

Las obligaciones de los tenedores de datos se articulan en torno a dos ejes principales: la puesta a disposición de datos para uso secundario y el cumplimiento de estándares técnicos y de seguridad. Respecto al primer eje, el Reglamento establece una obligación general de facilitar el acceso a los datos de salud electrónicos que obren en su poder cuando concurran los requisitos legales correspondientes[23]. Esta obligación se modula en función de la naturaleza pública o privada del tenedor, estableciéndose regímenes diferenciados dependiendo de la responsabilidad y si los tenedores son privados o públicos.

Los tenedores del sector público enfrentan una obligación más intensa de puesta a disposición de datos, coherente con los principios de transparencia y servicio al interés general que rigen su actuación. Por el contrario, los tenedores privados mantienen un mayor margen de discrecionalidad, aunque sujeto a los límites establecidos por el interés público en el avance de la investigación sanitaria.

El segundo eje de obligaciones se refiere al cumplimiento de estándares técnicos que garanticen la interoperabilidad, la seguridad y la calidad de los datos. Estos estándares incluyen requisitos de formato, codificación, metadatos, y medidas de seguridad que deben implementarse tanto en el almacenamiento como en la transmisión de datos. La armonización de estos aspectos técnicos resulta esencial para la operatividad del REEDS como espacio único de intercambio de datos

Versión anticipada / Online first

[22] Recital 77 Reglamento (UE) 2025/327.
[23] Arts. 40 y 41 del Reglamento (UE) 2025/327.

sanitarios, y ejemplos como SNOMED, OpenEHR o HL7-FHIR, ofrecen una estandarización que habla el mismo idioma a nivel europeo y que cumple con las previsiones establecidas en el REEDS[24].

Ahora bien, dentro de los tenedores de datos, hay excepciones de las obligaciones anteriormente descritas. Los investigadores a título individual, las personas jurídicas que reúnan los requisitos para ser consideradas microempresas[25]. Otro punto relevante dentro de la configuración de actores es el hecho de que el REEDS deja abierto que los Estados miembros puedan disponer en su legislación nacional excepciones a ciertas organizaciones que se encuentren bajo su jurisdicción, y también pueden abrir la posibilidad de que haya intermediarios de datos que pongan a disposición los datos de varios tenedores de datos de salud. Las diferencias y variabilidades que surjan por la designación de los tenedores de datos de salud deberán ser notificadas a la Comisión Europea antes del 26 de marzo de 2029, para asegurar una interpretación clara de qué entidades o no forman parte de ese ecosistema con el objetivo de garantizar la implementación del uso secundario de datos de salud.

### 4. Los usuarios de datos de salud.

La categoría de usuarios de datos de salud, la conforman las entidades que soliciten y obtengan acceso a datos de salud electrónicos para fines de uso secundario. Esta categoría de usuarios abarca desde investigadores académicos, como empresas farmacéuticas, incluyendo desarrolladores de tecnología sanitaria, y también a la administración pública a nivel nacional, europeo e internacional. Ahora bien, no todos los usuarios pueden acceder a los mismos usos secundarios de datos de salud. Las entidades del sector público pueden acceder a fines que empresas no pueden. Esos fines legítimos y concretos son el interés público, especialmente en salud pública o laboral para poder mejorar la calidad y seguridad de la asistencia sanitaria; en este caso agencias de evaluación, serán usuarios de datos de salud destacados y frecuentes, teniendo la posibilidad de cruzar, comparar y acceder a catálogos de datos más completos. Por otro lado, el uso secundario de los datos de salud abre la posibilidad a las instituciones de tomar decisiones basadas en evidencia generada por grandes conjuntos de datos en la elaboración de políticas públicas, en la propuesta de mejora de las existentes regulaciones y en la mejora integral de las funciones que son inherentes a su mandato[26].

Las obligaciones con respecto a los usuarios de datos se componen de tres fases temporales: pre-acceso, durante el acceso, y post-acceso. En primer lugar, la fase pre-acceso, los usuarios deben

Versión anticipada / Online first

[24] PEDRERA-JIMÉNEZ, Miguel / GARCÍA-BARRIO, Noelia / FRID, Santiago / et al., «Can OpenEHR, ISO 13606, and HL7 FHIR Work Together? An Agnostic Approach for the Selection and Application of Electronic Health Record Standards to the Next-Generation Health Data Spaces», Journal of Medical Internet Research, Vol. 25, 2023, e48702, DOI: 10.2196/48702.
[25] Artículo 50 Reglamento (UE) 2025/327.; Tal y como se definen en el artículo 2, apartado 3, del anexo de la Recomendación 2003/361/CE de la Comisión.
[26] TORRIJOS, Julián VALERO, «Datos abiertos y reutilización en el contexto de la Estrategia europea de datos», Tábula, Núm. 24, 2021, pp. 201-213.

demostrar el cumplimiento de requisitos de elegibilidad que incluyen capacidad técnica, solvencia ética, y legitimidad del propósito de uso. Durante el acceso, deben cumplir las condiciones que habían incluido en el permiso correspondiente, incluyendo medidas de seguridad, limitaciones de uso, y obligaciones de reporte. Por último, en la fase post-acceso, deben cumplir con las obligaciones de conservación segura o destrucción de datos, reporte de resultados, y cumplimiento de compromisos de publicación o retorno de beneficios a la comunidad.

Un aspecto particularmente relevante es la exigencia de que el uso de datos se realice en entornos de tratamiento seguro que cumplan especificaciones técnicas armonizadas. Estos entornos deben garantizar que los datos permanezcan bajo control del organismo de acceso a datos correspondiente, limitando las posibilidades de extracción o manipulación no autorizada. Para lograr la autorización de datos aprobada con el organismo de acceso a datos, deben contar con garantías y tendrán la obligación de acceder al entorno únicamente los que están incluidos en la petición de acceso a datos. Este punto es relevante para evitar que los datos puedan ponerse a disposición de terceros.

Otra cuestión muy relevante de estos actores es la obligación de transparencia, es decir, de publicar los resultados o productos del uso secundario, incluida la información relevante para la prestación de asistencia sanitaria, en un plazo de 18 meses a partir de la finalización del tratamiento de los datos sanitarios electrónicos en el entorno de tratamiento seguro. Estas obligaciones lo que generan es la necesidad de un seguimiento y diálogo permanente entre los usuarios de datos y los garantes que permiten y autorizan el uso secundario de los datos, es decir, los organismos de acceso a datos. Asimismo, durante el proceso de uso de los datos, directrices éticas como la integridad de la investigación científica, se cristalizan en obligaciones como la de informar de hallazgos significativos, hacer público resultados relevantes y citar la fuente de los datos y que su uso ha sido obtenido siguiendo el procedimiento establecido en el REEDS.

## III. La relevancia de los comités de ética de la investigación en el espacio europeo de datos de salud.

Los comités de ética de la investigación (en adelante CEIs) han experimentado una evolución significativa desde su concepción original como órganos de evaluación de la investigación biomédica tradicional. El desarrollo de las tecnologías digitales y su implicación en el sistema sanitario ha ampliado sustancialmente su ámbito de competencia, requiriendo nuevas habilidades y enfoques metodológicos y estructurales para abordar y evaluar las solicitudes de proyectos de investigación relacionados con la salud y la tecnología.

Versión anticipada / Online first

El Espacio Europeo de Datos de Salud expone en sus recitales[27], la necesidad de garantizar el uso lícito y ético y la reutilización de los datos de salud, intentando superar la fragmentación y las interpretaciones dispares que actualmente existen en la Unión Europea. Anteriormente, el Reglamento General de Protección de Datos, ya de por sí establecía un estándar mínimo de cumplimiento, para autorizar la utilización de datos personales con fines de investigación científica en el artículo 89[28].

Con la entrada en vigor del REEDS, se comienza la construcción de criterios y fines comunes por los cuales se pueden compartir y acceder a datos de salud. Los fines establecidos en el artículo 53 REEDS ya ofrecen un marco sobre para qué o no se pueden compartir datos de salud. Aunque ese marco se amplíe y edifique sobre lo ya construido en el Reglamento General de Protección de Datos, las flexibilidades legales deben conciliarse en el caso de la investigación, con los principios éticos arraigados en multitud de declaraciones (como la Declaración de Helsinki),[29] guías e incluso normativas nacionales. Es ahí, donde los CEIs, actúan como guardianes para asegurar la conducta ética de la investigación, ya que un proyecto que cumpla con los requisitos legales y la normativa vigente puede no ser lo suficientemente ético como para que se autorice.

Es por ello por lo que, en el contexto del Espacio Europeo de Datos de Salud, los CEIs pueden ser susceptibles de asumir funciones que trasciendan de la evaluación de protocolos de investigación individual, para abarcar la valoración ética de sistemas complejos de tratamiento de datos que pueden afectar a millones de personas. Esta transformación requiere una reconceptualización de los métodos de evaluación ética, incorporando perspectivas de ética de la información, ética de la inteligencia artificial, y ética de la salud pública. Más concretamente, en el análisis de los comités, la aplicación de la legislación de protección de datos no es meramente un ejercicio técnico de interpretación jurídica. Cuando las dimensiones éticas se combinan con las normas jurídicas, se requiere una reflexión, es decir, un juicio ético, esencial para gestionar el alto riesgo asociado a las categorías especiales de datos de salud, ya de por sí, protegidas como categorías de datos especiales en el artículo 9 del Reglamento General de Protección de Datos.

El REEDS establece referencias específicas a la necesidad de que los organismos de acceso a datos cooperen y cuenten intervención de CEIs en varios contextos, subrayando aquellos establecidos por

Versión anticipada / Online first

[27] RECUERO, 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, Núm. 2, 2024, pp. 525-551, DOI: 10.31009/InDret.2024.i2.13.

[28] TRONCOSO REIGADA, Antonio, «Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales», Revista de Derecho y Genoma Humano / Law and the Human Genome Review, Núm. 49, Vol. 2, 2018, pp. 187-266, DOI: 10.14679/1204.

[29] WMA – ASOCIACIÓN MÉDICA MUNDIAL, «Declaración de Helsinki de la AMM. Principios éticos para las investigaciones médicas en seres humanos». Disponible en: https://www.wma.net/es/policies-post/declaracion-de-helsinki-de-la-amm-principios-eticos-para-las-investigaciones-medicas-en-seres-humanos/ (fecha de consulta: 3 de junio de 2026).

ley europea y nacional.[30] Sin embargo, estas referencias dejan la puerta abierta a que sean los Estados Miembros los que establezcan el rol y las condiciones de la relación de los CEIs con los organismos de acceso a datos. Esto es debido, a que, en la cuestión relativa al uso secundario de datos de salud electrónicos, el Reglamento introduce la figura de los organismos de acceso a datos de salud, que son los intermediarios fundamentales en la gestión, autorización y monitoreo del cumplimiento y uso secundario de los datos como se ha mencionado anteriormente. Por consiguiente, cabe esperar que los organismos de acceso a datos se alineen o complementen en funciones ya ejercidas por los CEI; ya que toman decisiones y evalúan solicitudes dónde, aunque los datos sean de carácter anonimizado o seudonimizados o anonimizados, no dejan de ser datos que provienen de historias clínicas de pacientes, y que tienen un gran valor y riesgo para la investigación científica.

El proceso de concesión de permisos de datos por parte de los organismos de acceso a datos implica necesariamente una evaluación que tiene un componente ético y que históricamente ha sido labor de los CEIs. Los organismos de acceso a datos tienen según el artículo 57 y 58, tienen el deber de garantizar la calidad y la ética en el tratamiento de datos. Además, en el ejercicio de sus tareas, los organismos de acceso a datos deben cooperar con los CEI, cuando corresponda de acuerdo con la legislación de la Unión Europea o nacional.

Las opciones que se presentan incluyen la posible aprobación de proyectos de investigación que impliquen el uso secundario de datos de salud electrónicos. También pueden constituirse como órganos consultivos para los organismos de acceso a datos en casos de especial complejidad ética.

Es por ello, que considerando la relación que existe entre los futuros organismos de acceso a datos, y la actual situación respecto a los CEIs se proponen dos modelos en este artículo dos posibles modelos.

1. **Modelo de Asesoramiento o Acompañamiento (Secuencial):** Bajo este modelo si la legislación nacional lo requiriera, los CEIs deberían poner a disposición, su experiencia al organismo de acceso a datos de forma consultiva. Para ello debería establecerse una reforma en el caso de España de la Ley 14/2007 de Investigación Biomédica, en concreto el artículo 12 referido a las funciones y competencias de los comités de ética de la investigación[31].

Versión anticipada / Online first

[30] Recital 68 y Artículo 57.2 b) Reglamento (UE) 2025/327.
[31] ESPAÑA, Ley 14/2007, de 3 de julio, de Investigación biomédica, BOE Núm. 159, 4 de julio de 2007.

Implementando este modelo, los CEIs[32] intervienen primero, en el momento en el que se prepara la solicitud de acceso a datos; incluyendo el informe favorable del comité de ética para el proyecto de investigación, de salud pública o de desarrollo tecnológico que tenga que utilizar gran cantidad de datos de salud electrónicos no personales. Una vez se obtiene el informe, el organismo de acceso a datos en una fase posterior, verifica analizando la solicitud, la solicitud de acceso a datos que ya cuenta con una acreditación y evaluación ex-ante del cumplimiento de normativa y principios éticos establecidos por instrumentos sectoriales, como es el caso de la Declaración de Helsinki en la investigación biomédica. Con este modelo, los usuarios de datos de carácter público seguirían el procedimiento ya establecido, llegando al momento de la solicitud a los organismos de acceso a datos con mayor legitimidad y confianza. No obstante, para operadores privados cabría preguntarse cuál sería el modelo, abriéndose la opción de tener que pasar por los CEIs de los tenedores de datos o establecer un procedimiento concreto por parte del organismo de acceso a datos. Esas preguntas tendrán que darse por parte de la legislación nacional, teniendo en cuenta criterios comunes y buenas prácticas de proyectos piloto como TEHDAS 2 o de experiencias de otros países, que serán analizadas en el Consejo del Espacio Europeo de Datos de Salud[33].

2. **Modelo de Integración:** Los Estados Miembros pueden optar por integrar los órganos de ética dentro de la propia configuración del organismo de acceso a datos. En este caso se trataría de que los CEIs evaluaran las solicitudes de acceso a datos para uso secundario, asegurando el cumplimiento de los principios éticos. Esto incluye verificar que el uso de los datos se realice con un fin ético para el paciente y que no se desvíe a fines como la investigación de mercado, una vez se ha recibido la solicitud por parte del usuario de datos. En este caso sería necesario incluir específicamente la composición y competencias de los organismos de acceso a datos en la versión final del Anteproyecto de Ley de Salud Digital,[34] la normativa nacional que busca adaptar y compatibilizar el marco nacional con la implementación del REEDS.

Si este modelo cobrara forma, la proporción de proyectos y solicitudes aumentaría exponencialmente, debiendo contar con profesionales de diversas disciplinas con una disponibilidad cercana al tiempo completo. Esto se debe principalmente a los tiempos que el Reglamento del Espacio Europeo de Datos de Salud dispone entre que se procesa la solicitud del usuario de datos,

Versión anticipada / Online first

[32] URANGA, Amaia M., «El Espacio Europeo de Datos Sanitarios: una oportunidad para promover la investigación biomédica», I+S: Revista de la Sociedad Española de Informática y Salud, Núm. 161, 2024, pp. 9-11.

[33] REGLAMENTO DE EJECUCIÓN (UE) 2026/771 de la Comisión, de 7 de abril de 2026, por el que se establecen las medidas necesarias para el establecimiento y el funcionamiento del Consejo del Espacio Europeo de Datos de Salud.

[34] MINISTERIO DE SANIDAD, Anteproyecto de Ley de Salud Digital, 22 de septiembre de 2025. Disponible en: https://www.sanidad.gob.es/normativa/docs/2025.09.22_CPP_CPP_APL_Salud_Digital1_.pdf (fecha de consulta: 3 de junio de 2026).

el organismo de acceso a datos la procesa, y en caso de aprobación, solicita al tenedor de datos la puesta a disposición de los datos de salud electrónicos no personales.

Según el Artículo 68, apartado 7 del Reglamento del Espacio Europeo de Datos de Salud, los organismos de acceso a datos proporcionan acceso a los datos al usuario de datos "dentro de los dos meses siguientes a la recepción de los datos de los tenedores de datos", salvo que especifiquen un marco temporal más amplio justificado. Este plazo temporal, incorporando la deliberación y el acuerdo de un comité de ética integrado, necesita de un proceso ágil para poder cumplir con el periodo establecido. Aunque los CEIs tienen un mandato de celeridad, el equilibrio entre solicitudes y recursos si se opta por este modelo será una cuestión fundamental.

Estos dos modelos son planteados a partir de una serie de cuestiones prácticas de implementación práctica que conviene tener en cuenta.

Por ejemplo, en el supuesto de que un usuario de datos solicitara acceso a datos seudonimizados (en lugar de anonimizados), la solicitud debe incluir información sobre la evaluación de los aspectos éticos del procesamiento, de conformidad con la ley nacional aplicable. A su vez, los principios expuestos en el RGPD exponen la necesidad de minimización de datos por defecto, si se va a ir más allá, es el usuario el que tiene que justificar y convencer por qué se necesitan los datos en ese formato.

En la práctica actual, los CEIs son cruciales para determinar cuándo la anonimización de los datos como tratamiento durante el desarrollo del proyecto de investigación, es insuficiente para fines científicos legítimos. Estos criterios y estudios ya planteados representan una enorme oportunidad para que los organismos de acceso a datos deben incluir en su evaluación. A su vez, en la actualidad, los CEIs, deben asegurar que el usuario ha tomado medidas específicas para proteger a las personas afectadas. Para la investigación científica, la aprobación de un CEI será necesaria para validar la perspectiva ética del usuario, esto deberá ir unido al mismo nivel, cuando se trate de acceder a grandes conjuntos de datos.

Asimismo, los CEIs con su experiencia en la evaluación de la relación riesgo/beneficio en la investigación clínica, tienen la experiencia para asesorar en la evaluación de riesgos de protección de datos, un enfoque firmemente arraigado en el Reglamento General de Protección de Datos. Por ejemplo, los CEI pueden asesorar en la realización de la prueba de ponderación requerida en el impacto de la investigación y las motivaciones que pueda tener un tercero en acceder a un catálogo de datos,), especialmente para aquellos usuarios de datos del sector privado. En este caso, los protocolos ya existentes deberían integrarse en las evaluaciones de los organismos de acceso a datos.

Versión anticipada / Online first

En lo que respecta a las prohibiciones del artículo 54 recogidas en el Reglamento del Espacio Europeo de Datos de Salud, el rol de los CEIs ayuda a validar si el uso secundario previsto no conlleva un riesgo de estigmatización o daño a la dignidad de personas o grupos. El REEDS prohíbe explícitamente el uso de datos para tomar decisiones perjudiciales o discriminatorias contra personas, como, por ejemplo, aumentar las primas de seguros de salud. Independientemente del modelo por el que se opte, los CEIs deben implementar elementos de supervisión continua de proyectos de larga duración o de impacto ya que la evaluación ética en el contexto del REEDS, debe abordar dimensiones que van más allá de bioética clínica. Los CEIs en conjunto con los organismos de acceso a datos deberán tener en cuenta dimensiones como la evaluación del equilibrio entre beneficios científicos y riesgos para la privacidad; la proporcionalidad para escoger el formato anonimizado o seudonimizado; la supervisión de aspectos de justicia distributiva en el acceso a los beneficios e impacto de los proyectos de investigación.

## IV. Responsabilidades de los actores en el uso secundario de los datos de salud electrónicos.

El uso secundario de datos de salud genera una cadena compleja de responsabilidades que se extiende desde el principio, en los catálogos de datos con los que cuentan los tenedores de datos hasta los que maximizan el valor y la calidad de los datos como usuarios de datos, pasando por los organismos de acceso a datos y los proveedores de infraestructuras tecnológicas. La atribución de responsabilidades en caso de incidentes de seguridad, uso indebido de datos, o daños a los interesados presenta importantes desafíos jurídicos.

En primer lugar, el principio de responsabilidad establecido en el Reglamento General de Protección de Datos se proyecta sobre todos los actores del ecosistema del Espacio Europeo de Datos de Salud, requiriendo que cada uno pueda demostrar el cumplimiento de sus obligaciones específicas. Sin embargo, la interacción entre múltiples responsables y encargados de tratamiento puede generar zonas grises en la atribución de responsabilidades. Aunque los organismos de acceso a datos asumen una responsabilidad particular como garantes del sistema, garantizando que solo se autorice el acceso a entidades que cumplan los requisitos establecidos; su responsabilidad se extiende tanto a la evaluación ex ante de las solicitudes como a la supervisión continua del cumplimiento de las condiciones de acceso[35].

La gestión de riesgos en el uso secundario de datos de salud requiere una aproximación multidimensional que considere riesgos técnicos, legales, éticos y sociales. Técnicamente, se pueden dar fallos de seguridad, brechas de datos, y vulnerabilidades en los sistemas implementados por los titulares de datos para garantizar la anonimización, seudonimización o cifrado de los datos.

[35] DE MIGUEL-BERIAIN, Íñigo / LOYO-MENOYO, Mónica, «El reglamento del espacio europeo de datos de salud: ¿qué podemos esperar?», Gaceta Médica de Bilbao, Vol. 122, Núm. 1, 2025, pp. 47-53.

Versión anticipada / Online first

Estos incidentes técnicos conllevan la vulneración de la norma, con su consecuente posible sanción administrativa por parte de las autoridades de protección de datos, entre otras posibles responsables en materia civil o penal.

A nivel ético, pueden generarse usos discriminatorios de datos, comercialización inadecuada de información sanitaria asimetrías de conocimiento y de acceso entre los operadores del ecosistema de la investigación biomédica, entre otros, que irán apareciendo una vez vaya avanzando la implementación del REEDS. Esto se une a los potenciales efectos sobre la confianza pública en el sistema sanitario. La implementación de medidas de salvaguarda apropiadas requiere una evaluación de impacto integral que considere todos estos aspectos. Las evaluaciones de impacto sobre la protección de datos, exigidas por el artículo 35 del RGPD, deben complementarse con evaluaciones de impacto ético y social que permitan una valoración holística de los riesgos que conlleva el uso secundario de los datos de salud electrónico como forma funcional de abordar la gobernanza de estos datos entre los actores del uso secundario de los datos de salud.

Otro principio rector del REEDS es la transparencia, que se manifiesta en múltiples dimensiones: transparencia hacia los titulares de datos sobre el uso de su información, transparencia hacia la comunidad científica sobre los datos disponibles y las condiciones de acceso, y transparencia hacia la sociedad sobre el funcionamiento del sistema y sus resultados. Es por ello por lo que los organismos de acceso deben mantener registros públicos de las autorizaciones concedidas, los proyectos en curso, y los resultados obtenidos. A su vez, esta información debe presentarse de manera accesible y comprensible para ciudadanos, investigadores, y responsables de políticas públicas, entre otros. Para poder cumplir con esas obligaciones, requiere mecanismos de supervisión independiente y evaluación externa del funcionamiento del sistema. Los informes periódicos, las auditorías externas, y la evaluación de impacto social podrían ser importantes herramientas para garantizar que el REEDS cumpla sus objetivos sin comprometer los derechos fundamentales.

A pesar de la relevancia ética, la implementación del papel de los CEI enfrenta desafíos significativos debido a la falta de uniformidad y recursos. El REEDS no ha implementado medidas a nivel del reglamento para garantizar la uniformidad en el proceso de aprobación ética, dejando este aspecto a la discreción de los Estados miembros. En el caso de España, el Anteproyecto de Salud Digital debe tener en cuenta este aspecto a la hora de definir y regular aspectos del uso secundario. Otro desafío intrínseco de los CEIs es la diversidad de pareceres. Los juicios variables de los comités de ética al considerar la compatibilidad de las solicitudes de reprocesamiento de datos con los protocolos originales de los ensayos constituyen una enorme barrera de impredecibilidad para los investigadores. Eso se debe, a las diferencias de capacitación, especialmente en materia de supervisión legal, incidiendo en que, en el caso específico de los CEIs, se necesita una transformación y adaptación al nuevo marco regulatorio. El reto parte ya de una base contrastada pero que necesita actualizaciones, con el objetivo de que el rol de estas organizaciones que siempre

Versión anticipada / Online first

están presentes en procesos de investigación que implican el tratamiento de datos personales (incluyendo en ocasiones muestras humanas), pueden seguir siendo transcendentales.

Por otro lado, un aspecto relevante para tener en cuenta es la necesidad de establecer protocolos claros de coordinación entre el CEI, el organismo de acceso a datos y otras autoridades de supervisión (como las Agencias de Protección de Datos), evitando así, un potencial riesgo de que los investigadores y los futuros usuarios de datos se enfrenten a un proceso burocrático complejo e incierto.

Sin embargo, la adecuación de los CEIs a las exigencias del REEDS requiere una revisión que podría afectar a su composición y competencias. Los comités tradicionales, configurados para la evaluación de investigación clínica, necesitan incorporar profesionales preparados para valorar proyectos de ciencia de datos, inteligencia artificial, o investigación en salud pública, proponiéndose la incorporación de expertos en protección de datos, especialistas en tecnologías de la información, científicos de datos, y expertos en ética digital. Asimismo, la perspectiva de los colectivos de pacientes debería ser incluida en los criterios para autorizar o denegar el acceso a los datos, por razones como la evolución de análisis de datos, requiriendo una actualización constante de conocimientos que permita una evaluación informada y rigurosa.

## V. Retos específicos en la implementación del uso secundario de los datos de salud.

Uno de los principales retos en la implementación del REEDS es encontrar el equilibrio adecuado entre la armonización necesaria para crear un espacio europeo integrado y el respeto a la subsidiariedad en la organización de los sistemas sanitarios nacionales establecida en el Artículo 168 del Tratado de Funcionamiento de la Unión Europea.[36] Esta tensión se manifiesta particularmente en la configuración de los organismos de acceso a datos y en la definición de estándares técnicos y procedimentales, siendo en el caso de España la fragmentación territorial, uno de los retos respecto a la implementación práctica del REEDS.

La diversidad de tradiciones jurídicas, organizativas y culturales en el ámbito sanitario europeo requiere flexibilidad en la interpretación y puesta en marcha del Reglamento. Sin embargo, esta flexibilidad no debe comprometer la interoperabilidad y la coherencia del sistema. La experiencia previa con la implementación del RGPD muestra los riesgos de interpretaciones divergentes que pueden fragmentar el mercado único en materia digital.

Versión anticipada / Online first

[36] DE LA MATA BARRANCO, Isabel, «Ciudadanía sanitaria europea. La salud y la Unión Europea (European health care citizens. Health and the European Union)», Revista de Administración Sanitaria Siglo XXI, Núm. 7, Vol. 4, 2009, pp. 541-548.

La implementación efectiva del REEDS requiere inversiones significativas en infraestructuras técnicas, desarrollo de competencias profesionales, y un cambio de paradigma en las organizaciones del sector de la salud. Las disparidades existentes entre Estados miembros en términos de digitalización sanitaria, capacidades de investigación, y recursos disponibles pueden generar implementaciones asimétricas que afecten la coherencia del sistema. El desarrollo de las especificaciones técnicas para la interoperabilidad, previsto en el artículo 15 del REEDS, constituye otro elemento que determinará la viabilidad práctica del intercambio transfronterizo de datos. Las especificaciones deben ser detalladas para garantizar la interoperabilidad, pero flexibles para adaptarse a la evolución tecnológica, siendo los actores en el uso secundario, los promotores de la inclusión de esos cambios. Otro rasgo esencial para el éxito de la implementación de REEDS depende de la aceptación social y la confianza por parte de todos los operadores y elementos del sistema, en especial los pacientes. La construcción de confianza requiere no solo el cumplimiento formal de los requisitos legales, sino también la demostración práctica de que el sistema genera beneficios tangibles para los ciudadanos y la sociedad. Acciones como visualizar los beneficios, la comunicación de resultados de investigación, y la participación ciudadana en la gobernanza del sistema contribuyen a mantener la legitimidad del REEDS.

## VI. Conclusiones.

El análisis realizado pone de relieve que la implementación del REEDS en materia de uso secundario de datos de salud se enfrenta a tres grupos de problemas jurídicos principales: la distribución y coordinación de competencias entre organismos de acceso, tenedores, usuarios y comités de ética de la investigación; la gestión de una cadena de responsabilidades compleja en un entorno multinivel y transfronterizo; y la necesidad de conciliar la explotación intensiva de datos de salud con la salvaguarda y protección de los derechos fundamentales, el marco de protección de datos personales ya existente en el RGPD.

Frente a estos retos, el trabajo propone la configuración de un sistema de supervisión ética multinivel, en el que los CEIs se especialicen en la evaluación de proyectos relacionados con el uso secundario de datos de salud, desempeñando un papel estructural en la autorización y seguimiento del uso secundario. Se circunscribe que los CEI deberían integrarse en la gobernanza del REEDS, bien mediante un modelo secuencial de asesoramiento previo a la decisión de los organismos de acceso, o bien mediante un modelo de integración orgánica, según determinen los Estados miembros en su legislación de desarrollo; necesitando en ambos supuestos, una estrecha coordinación con los organismos de acceso a datos y con criterios armonizados que provengan en sus líneas de actuación básicas del Consejo del EEDS, y sus pilares de actuación e implementación en la legislación nacional.

Versión anticipada / Online first

Para que este sistema resulte jurídicamente operativo, se considera imprescindible la adopción de directrices que clarifiquen la distribución de responsabilidades entre los distintos actores, especialmente en supuestos de incidentes de seguridad, reidentificación o usos discriminatorios prohibidos por el art. 54 REEDS. Dichas directrices deberían abordar tanto la atribución de daños y la distribución de costes de las medidas correctoras como los procedimientos de cooperación entre organismos de acceso, CEIs y autoridades de protección de datos. Asimismo, se sostiene que la adaptación del ordenamiento español al REEDS no puede limitarse a una mera traslación terminológica. Es necesario revisar la Ley 14/2007 de Investigación Biomédica en lo relativo a las competencias de los CEIs e incorporar de manera expresa la figura de los organismos de acceso a datos en la futura Ley de Salud Digital, garantizando su independencia funcional, su capacidad técnica y su coordinación con las autoridades de protección de datos. Solo así se respetará la distribución interna de competencias sanitarias derivada del art. 168 TFUE sin comprometer la armonización mínima exigida por el REEDS.

Los CEIs han venido representado un pilar en la construcción de la confianza pública de pacientes, profesionales sanitarios e investigadores para compartir grandes volúmenes de datos de salud. Sin embargo, los organismos de acceso a datos, como elementos innovadores del sistema de gobernanza, se enfrentan al desafío de actuar como garantes efectivos que de la protección de derechos sin impedir el progreso científico. Por otro lado, tenedores y usuarios de datos, como actores afectados y beneficiados deben asumir responsabilidades específicas en la cadena de valor de los datos de salud, implementando medidas técnicas y organizativas que garanticen el cumplimiento de los principios de protección de datos y los objetivos del REEDS.

Finalmente, se subraya que la arquitectura de gobernanza propuesta reviste una especial importancia para los datos genéticos y los datos relativos a enfermedades raras. En estos ámbitos, los riesgos de reidentificación, de estigmatización de grupos y de usos contrarios al principio de justicia exigen reforzar las evaluaciones de impacto (jurídicas, éticas y sociales), incrementar la participación de organizaciones de pacientes y asegurar una transparencia efectiva sobre los proyectos autorizados y los resultados obtenidos. Solo un modelo de gobernanza que combine armonización normativa, desarrollo de capacidades y construcción activa de la confianza pública permitirá que el REEDS cumpla su promesa de impulsar la investigación y la innovación en salud sin erosionar los derechos fundamentales que sustentan el proyecto europeo.

Versión anticipada / Online first

## VII. Referencias bibliografías.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, «Condiciones para el acceso y tratamiento de los datos de salud. Guía de preguntas frecuentes y propuestas», Proyecto BIODAT, junio de 2023. Disponible en: https://www.aepd.es (fecha de consulta: 3 de junio de 2026).

ANDREU MARTÍNEZ, María Belén / SÁNCHEZ GARCÍA, Alfonso / CASANOVA ASENCIO, Andrea Salud, Los datos de salud como eje de la transformación digital de la sanidad, Comares, Granada, 2024.

ANDREU MARTÍNEZ, María Belén / MARTÍNEZ GUTIÉRREZ, Rubén / MARÍN SALMERÓN, Andrés / NAVARRO GÓMEZ, Florencio, Arquitectura jurídica de los espacios de datos, Comares, Granada, 2026, disponible en acceso abierto. Disponible en: https://doi.org/10.55323/9788413699783 (fecha de consulta: 3 de junio de 2026).

ASENCIO CASANOVA, Andrea Salud, «Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias», InDret, 2019, s. p. Disponible en: https://raco.cat/index.php/InDret/article/view/354517 (fecha de consulta: 3 de junio de 2026).

ASENCIO CASANOVA, Andrea Salud, «Mecanismos de prevención del acceso indebido a la historia clínica por parte del personal sanitario y nueva legislación de protección de datos», Bioderecho.es, Núm. 7, 2018, pp. 1-20.

ASENCIO CASANOVA, Andrea Salud, «Espacio Europeo de Datos Sanitarios, uso primario y autonomía del paciente», en ANDREU MARTÍNEZ, María Belén (Dir.), Los datos de salud como eje de la transformación digital de la sanidad, Comares, Granada, 2023, pp. 107-135.

BARROSO ASENJO, Porfirio / CALVACHE PÉREZ, Laura, «Comités de ética asistencial (CEA) en España y en Europa», Revista Bioética y Ciencias de la Salud, Vol. 5, Núm. 2, 2002

CABALLERO PÉREZ, María José, «El derecho a la salud en el ámbito internacional y de la Unión Europea. Tratamiento actual y desafíos futuros», Revista de Derecho de la Seguridad Social, Núm. Extra 4, 2022, pp. 55-83.

DE LA MATA BARRANCO, Isabel, «Ciudadanía sanitaria europea. La salud y la Unión Europea (European health care citizens. Health and the European Union)», Revista de Administración Sanitaria Siglo XXI, Núm. 7, Vol. 4, 2009, pp. 541-548.

DE MIGUEL BERIAIN, Íñigo / LOYO MENOYO, Mónica / LÓPEZ DE LA PEÑA DE PABLO, Mercedes, «El nuevo reglamento europeo relativo al espacio europeo de datos de salud: su impacto en la gobernanza del dato y su uso ético y seguro», Revista de Derecho y Genoma Humano / Law and the Human Genome Review, Núm. 61, 2025, pp. 59-82, DOI: 10.1387/rdgh.27342.

Versión anticipada / Online first

DE MIGUEL-BERIAIN, Íñigo / LOYO-MENOYO, Mónica, «El reglamento del espacio europeo de datos de salud: ¿qué podemos esperar?», Gaceta Médica de Bilbao, Vol. 122, Núm. 1, 2025, pp. 47-53.

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, DOUE L 88, 4 de abril de 2011.

EGUSQUIZA BALMASEDA, María Asunción / et al. (Coords.), Régimen jurídico de protección de datos de salud en el Espacio Europeo de Datos de Salud (EEDS), Colex, Madrid, 2025.

EGUSQUIZA BALMASEDA, María Asunción, «Cesión altruista de datos en el Espacio Europeo de Datos de Salud», en EGUSQUIZA BALMASEDA, María Asunción / et al. (Coords.), Régimen jurídico de protección de datos de salud en el Espacio Europeo de Datos de Salud (EEDS), Colex, Madrid, 2025, pp. 117-193.

ESPAÑA, Ley 14/2007, de 3 de julio, de Investigación biomédica, BOE Núm. 159, 4 de julio de 2007.

JIMÉNEZ GONZÁLEZ, Javier, «De la historia clínica impresa a la historia clínica digital. Evolución y retos», en ANDREU MARTÍNEZ, María Belén (Dir.), Los datos de salud como eje de la transformación digital de la sanidad, Comares, Granada, 2023, pp. 17-43.

LUQUIN BERGARECHE, Raquel, «Reutilización o uso secundario de los datos personales de salud», en EGUSQUIZA BALMASEDA, María Asunción / et al. (Coords.), Régimen jurídico de protección de datos de salud en el Espacio Europeo de Datos de Salud (EEDS), Colex, Madrid, 2025, pp. 200-260.

PEDRERA-JIMÉNEZ, Miguel / GARCÍA-BARRIO, Noelia / FRID, Santiago / et al., «Can OpenEHR, ISO 13606, and HL7 FHIR Work Together? An Agnostic Approach for the Selection and Application of Electronic Health Record Standards to the Next-Generation Health Data Spaces», Journal of Medical Internet Research, Vol. 25, 2023, e48702. Disponible en: https://doi.org/10.2196/48702 (fecha de consulta: 3 de junio de 2026).

POLO CURTO, María Mercedes, «El uso secundario de datos de salud electrónicos protegidos por Propiedad Intelectual y secretos comerciales a la luz del Reglamento (UE) 2025/327, del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud», Revista Propiedad Intelectual e Innovación Digital, Vol. 3, Núm. 1, 2026, pp. 41-72, DOI: 10.36151/RPIID.2026.3.1.02.

Versión anticipada / Online first

QUINN, Paul, «Health Data Access Bodies under the European Health Data Space – A technocratic colossus or rubber stamp forum?», Technology and Regulation, 2025, pp. 60-80. Disponible en: https://doi.org/10.71265/vbfvpb76 (fecha de consulta: 3 de junio de 2026).

RECUERO, Mikel, «La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado», [datos de revista por completar], 2019.

RECUERO, 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, Núm. 2, 2024, pp. 525-551, DOI: 10.31009/InDret.2024.i2.13.

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 (Reglamento general de protección de datos), DOUE L 119, 4 de mayo de 2016.

REGLAMENTO (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847, DOUE L 327, 5 de marzo de 2025.

REGLAMENTO DE EJECUCIÓN (UE) 2026/771 de la Comisión, de 7 de abril de 2026, por el que se establecen las medidas necesarias para el establecimiento y el funcionamiento del Consejo del Espacio Europeo de Datos de Salud, DOUE L.

SÁNCHEZ GARCÍA, Alfonso, «El altruismo de datos en el ámbito sanitario», en ANDREU MARTÍNEZ, María Belén (Dir.), Los datos de salud como eje de la transformación digital de la sanidad, Comares, Granada, 2023, pp. 69-105.

TRONCOSO REIGADA, Antonio, «Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales», Revista de Derecho y Genoma Humano / Law and the Human Genome Review, Núm. 49, Vol. 2, 2018, pp. 187-266, DOI: 10.14679/1204.

VALERO TORRIJOS, Julián, «La reutilización de la información sanitaria desde la perspectiva de la regulación europea sobre gobernanza de datos», en ANDREU MARTÍNEZ, María Belén (Dir.), Los datos de salud como eje de la transformación digital de la sanidad, Comares, Granada, 2023, pp. 45-68.

VALERO TORRIJOS, Julián, «Datos abiertos y reutilización en el contexto de la Estrategia europea de datos», Tábula, Núm. 24, 2021, pp. 201-213.

Versión anticipada / Online first

URANGA, Amaia M., «El Espacio Europeo de Datos Sanitarios: una oportunidad para promover la investigación biomédica», I+S: Revista de la Sociedad Española de Informática y Salud, Núm. 161, 2024, pp. 9-11.

VIDÁN PEÑA, José, «Servicios de telemedicina: protección de datos de salud del paciente y usuario», en EGUSQUIZA BALMASEDA, María Asunción / et al. (Coords.), Régimen jurídico de protección de datos de salud en el Espacio Europeo de Datos de Salud (EEDS), Colex, Madrid, 2025, pp. 11-46.

WMA – ASOCIACIÓN MÉDICA MUNDIAL, «Declaración de Helsinki de la AMM. Principios éticos para las investigaciones médicas en seres humanos». Disponible en: https://www.wma.net/es/policies-post/declaracion-de-helsinki-de-la-amm-principios-eticos-para-las-investigaciones-medicas-en-seres-humanos/ (fecha de consulta: 3 de junio de 2026).

EDPB – COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Guidelines 2026/01 on Scientific Research under the GDPR, 2026. Disponible en: https://www.edpb.europa.eu/system/files/2026-04/edpb_guidelines_202601_scientificresearch_en.pdf (fecha de consulta: 3 de junio de 2026).

COMISIÓN EUROPEA, Informe sobre la aplicación del Reglamento (UE) 2016/679 (COM(2020) 264 final), Bruselas, 24 de junio de 2020.

Versión anticipada / Online first