



Reglamento del Espacio Europeo de Datos de Salud (EHDS)

El pasado 05 de marzo se publicó en el DOUE el Reglamento (UE) 2025/327 (en adelante, el "Reglamento"), que establece el marco normativo del Espacio Europeo de Datos de Salud (en adelante, el "EHDS", por sus siglas en inglés), con el objetivo de garantizar el acceso seguro y eficiente a los datos de salud electrónicos en la Unión Europea.

Entrada en vigor

El Reglamento entrará en vigor el 26 de marzo de este año. No obstante, su aplicación será progresiva: las disposiciones generales serán aplicables a partir del 26 de marzo de 2027, mientras que algunas obligaciones específicas no entrarán en vigor hasta marzo de 2029 y marzo de 2031.

Objetivos del Reglamento

El principal objetivo del Reglamento es crear un marco común que permita el acceso seguro, interoperable y eficiente a los datos de salud electrónicos en toda la UE, tanto para mejorar la asistencia sanitaria (uso primario) como para fomentar la investigación, la innovación y la formulación de políticas basadas en datos (uso secundario).

Entre sus metas específicas, el EHDS busca reforzar el control de los datos de salud los pacientes, facilitando la interoperabilidad de los sistemas de historias clínicas electrónicas (en adelante, "EHR" por sus siglas en inglés), y estableciendo estándares de calidad y seguridad para el tratamiento de datos. Asimismo, promueve la reutilización de datos de salud para fines científicos y sociales, respetando los derechos fundamentales y la protección de datos personales, en línea con el RGPD.

Ámbito de aplicación

▶ Personas físicas que generan datos de salud electrónicos

Tendrán derechos específicos sobre sus datos de salud electrónicos como se verá más adelante en el presente documento.

▶ Tenedores de datos de salud

El artículo 2(2)(t) del Reglamento define a los tenedores de datos de salud como cualquier persona física o jurídica, autoridad pública, agencia u organismo que cumpla con los siguientes criterios:

- **Sectores afectados:** Operen en los sectores de la salud o el cuidado, incluyendo servicios de reembolso, o desarrollen productos o servicios destinados a estos sectores.
- **Control de datos:** Sean responsables del tratamiento de datos personales de salud (como responsables o corresponsables del tratamiento) o tengan la capacidad técnica de poner a disposición datos no personales relacionados con la salud.

Sobre BDO Abogados

Somos una firma de abogados internacional comprometida con ofrecer servicios de calidad y valor superior para impulsar el éxito de nuestros clientes en todo el mundo.

Adaptamos nuestro enfoque de trabajo, honorarios y equipos según las necesidades específicas que cada caso requiera, contando con una gran capacidad de recursos para abordar cualquier desafío legal con eficacia y eficiencia. Su éxito es nuestra prioridad.

*People helping people
achieve their dreams.*

Contacto



Marina Fontcuberta

Directora de Derecho Digital
marina.fontcuberta@bdo.es

www.bdo.es

- **Ejemplos de titulares de datos:** Proveedores de atención médica (hospitales, clínicas, médicos), fabricantes de aplicaciones de bienestar (wellness apps) que traten datos de salud o instituciones de investigación relacionadas con la salud.

Artículo 2(2)(t): «tenedor de datos de salud»: toda persona física o jurídica, autoridad pública, agencia u otro organismo del sector de la asistencia sanitaria o el asistencial, incluidos los servicios de reembolso cuando sea necesario, así como cualquier persona física o jurídica que desarrolle productos o servicios destinados al sector de la salud, el de la asistencia sanitaria o el asistencial, etc.»

► Las entidades del sector sanitario y asistencial

Incluidos hospitales, farmacias y otros prestadores de asistencia sanitaria, están obligadas a registrar, procesar y compartir datos de salud electrónicos en formatos interoperables, como el Formato Europeo de Intercambio de Historias Clínicas Electrónicas (en adelante, "EEHRxF") (artículos 13, 14 y 15). También deben garantizar la seguridad y la calidad de los datos, así como cumplir con las solicitudes de acceso y uso secundario de los datos por parte de los organismos de acceso a datos de salud (artículos 57 y 60).

► Los desarrolladores y proveedores de sistemas EHR

Deben cumplir con los requisitos esenciales de interoperabilidad¹ y seguridad establecidos en el Reglamento (artículos 25 y 36). Esto incluye la implementación de componentes armonizados de software para la interoperabilidad y el registro, la obtención de la marca CE de conformidad y el registro de los sistemas en la base de datos de la UE (artículos 37, 39 y 49). Además, deben someter sus productos a pruebas automatizadas en entornos de prueba digitales antes de su comercialización (artículo 40).

Regulación de los Sistemas de IA

El Reglamento aborda la interacción entre los sistemas de historias clínicas electrónicas y los sistemas de IA, estableciendo requisitos específicos para garantizar la interoperabilidad, la seguridad y la protección de los datos de salud electrónicos.

► Interacción con el Reglamento de Inteligencia Artificial (AI Act)

Los sistemas EHR que incorporen funcionalidades de IA, como herramientas de triaje de emergencia, estarán sujetos tanto a los requisitos del EHDS como a los del AI Act. Esto incluye la clasificación de dichos sistemas como "sistemas de alto riesgo" bajo el AI Act, lo que implica la necesidad de cumplir con estrictos requisitos de seguridad, transparencia y evaluación de riesgos (artículo 27.2 del EHDS y artículo 6 del AI Act).

► Conformidad y Registro

Los fabricantes de sistemas EHR que integren IA deben demostrar la conformidad con los requisitos esenciales de ambos reglamentos. Para simplificar los procedimientos, el EHDS permite un registro coordinado en las bases de datos de sistemas de alto riesgo del AI Act y en la base de datos de sistemas EHR del EHDS (artículo 49.3 del EHDS).

► Evaluación de Conformidad

El reglamento establece que los procedimientos de evaluación de conformidad deben organizarse de manera que se minimice la carga administrativa para los fabricantes de sistemas EHR. Esto incluye la posibilidad de realizar evaluaciones conjuntas o coordinadas para cumplir con los requisitos de interoperabilidad y seguridad de ambos reglamentos (artículo 36 del EHDS y artículo 71 del AI Act).

► Protección de Datos y Seguridad

Los sistemas EHR con IA deben garantizar la protección de los datos de salud electrónicos personales, cumpliendo con las disposiciones del RGPD y las medidas de seguridad específicas del EHDS, como el uso de entornos de tratamiento seguros (artículo 73 del EHDS).

¹Los sistemas deben ser capaces de importar y exportar datos en el Formato Europeo de Intercambio de Historias Clínicas Electrónicas (EEHRxF).



Correlación con el RGPD

Derechos sobre los datos de salud electrónicos

El EHDS complementa y amplía los derechos establecidos en el RGPD, adaptándolos específicamente al ámbito de los datos de salud electrónicos, con el objetivo de garantizar una mayor protección y control por parte de los pacientes.

► Refuerzo de derechos ya existentes

- **Derecho de rectificación:** el EHDS refuerza el derecho de rectificación (artículo 6 EHDS), ya reconocido en el RGPD (artículo 16), al establecer mecanismos específicos para que los pacientes puedan solicitar la corrección de información incorrecta en sus datos de salud electrónicos.
- **Derecho de portabilidad:** el EHDS (artículo 7 EHDS) amplía el previsto en el RGPD (artículo 20), al exigir que los datos de salud puedan transferirse en un formato interoperable, como el formato EEHRxF. Esto facilita el intercambio de datos entre sistemas de salud y garantiza su uso efectivo.

► Nuevas garantías de seguridad y transparencia

- **Derecho a limitar el acceso:** el EHDS introduce el derecho de los pacientes a restringir el acceso a partes específicas de sus datos de salud (artículo 8 EHDS), reforzando la confidencialidad y la protección frente a accesos no autorizados, en línea con el principio de seguridad del RGPD (artículo 5.1.f).
- **Derecho a obtener información sobre accesos:** el EHDS establece que los pacientes tienen derecho a conocer quién ha accedido a sus datos de salud y cuándo (artículo 9 EHDS), ampliando el derecho de acceso del RGPD (artículo 15). Además, refuerza los derechos de los pacientes al garantizarles acceso inmediato y gratuito a las categorías prioritarias de datos² a través de servicios de acceso a datos de salud electrónicos.

► Introducción de nuevos derechos

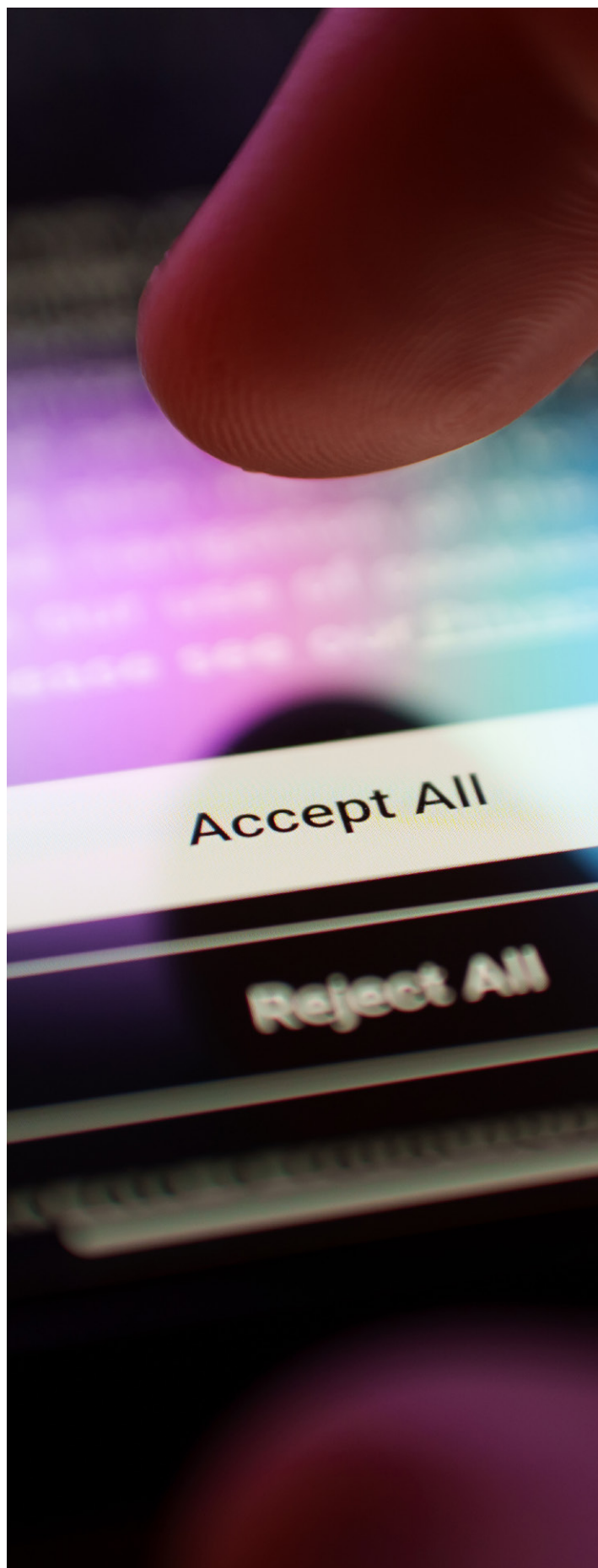
- **Derecho a añadir información:** una de las principales innovaciones del EHDS es el derecho de los pacientes a añadir información en su historia clínica electrónica (artículo 5 EHDS). Este derecho, no contemplado en el RGPD, permite a los pacientes complementar su historial médico con datos relevantes, como información de aplicaciones de bienestar, fomentando su participación activa en la gestión de su salud³.

Responsabilidad y medidas de seguridad

Tanto el RGPD como el EHDS destacan la importancia de la responsabilidad de los responsables del tratamiento (artículo 24 RGPD) y la necesidad de adoptar medidas de seguridad para proteger los datos frente a accesos no autorizados, alteraciones o pérdidas.

²Conforme al artículo 14 del EHDS, las categorías prioritarias de datos de salud electrónicos personales serán las siguientes: las historias clínicas resumidas de los pacientes; las recetas electrónicas; las dispensaciones electrónicas; los estudios de diagnóstico por imagen y los informes de imágenes correspondientes; los resultados de pruebas diagnósticas, incluidos los resultados de laboratorio y otros resultados de diagnóstico e informes correspondientes; y los informes de altas hospitalarias.

³La introducción de información por parte de las personas físicas o sus representantes no implica que éstos puedan modificar directamente los datos de salud electrónicos introducidos por profesionales sanitarios.



Reparación de daños

El RGPD (artículo 82) garantiza el derecho a recibir del responsable o el encargado del tratamiento una reparación íntegra por daños, incluyendo los morales, en caso de infracción de las normas de protección de datos. El EHDS refuerza este principio al establecer mecanismos claros para proteger los derechos de los pacientes en el ámbito de los datos de salud electrónicos.

Actos de Ejecución Clave del EHDS

Los actos de ejecución se fundamentan en el artículo 291 del TFUE, que permite a la Comisión Europea adoptar medidas para garantizar la aplicación uniforme de los actos jurídicos de la UE. En el caso del EHDS, los actos de ejecución son esenciales para desarrollar especificaciones técnicas, requisitos de interoperabilidad y medidas de seguridad.

El artículo 105 del Reglamento establece un cronograma para la adopción de los actos de ejecución, que deben ser aprobados en un plazo de dos años desde el 26 de marzo de 2027. Los actos de ejecución más relevantes incluyen:

- ▶ Especificaciones técnicas para el EEHRxF (artículo 15).
- ▶ Requisitos de calidad de los datos para el uso primario (artículo 13).
- ▶ Especificaciones comunes para los componentes armonizados de los sistemas EHR (artículo 36).
- ▶ Requisitos para los entornos de tratamiento seguros (artículo 73).
- ▶ Requisitos para la infraestructura transfronteriza MyHealth@EU (artículo 23).
- ▶ Modelos para solicitudes de acceso a datos y permisos de datos (artículo 70).
- ▶ Etiqueta de calidad y utilidad de los datos (artículo 78).

Conclusiones

El EHDS representa un avance significativo en la regulación del tratamiento de datos de salud electrónicos en la Unión Europea. Refuerza los derechos de los pacientes, establece requisitos claros para los sistemas de historias clínicas electrónicas y promueve el uso secundario de datos para investigación e innovación, especialmente en el ámbito de la inteligencia artificial.

Los diferentes actores implicados, desde pacientes hasta fabricantes de sistemas de IA, deberán adaptarse a estos nuevos requisitos para garantizar el cumplimiento normativo y aprovechar las oportunidades que ofrece.

Cuestiones que mantener en el radar:

- ▶ Aplicaciones de bienestar.
- ▶ Definición de roles de encargado, responsable y corresponsable del tratamiento.
- ▶ Introducción de nuevos derechos.

Esta publicación ha sido redactada en términos generales y debe ser contemplada únicamente como una referencia general. Esta publicación no puede utilizarse como base para amparar situaciones específicas y usted no debe actuar, o abstenerse de actuar, de conformidad con la información contenida en este documento sin obtener asesoramiento profesional específico. Póngase en contacto con BDO en cualquiera de nuestras oficinas para tratar estos asuntos en el marco de sus circunstancias particulares. BDO, sus socios y empleados, no aceptan ni asumen cualquier responsabilidad ante cualquier pérdida derivada de cualquier acción realizada o no por cualquier individuo al amparo de la información contenida en esta publicación o ante cualquier decisión basada en ella.

BDO Abogados y Asesores Tributarios, S.L.P., una sociedad limitada española independiente, es miembro de la red internacional de BDO, constituida por empresas independientes asociadas de todo el mundo, y creada por BDO International Limited, una compañía limitada por garantía del Reino Unido.

BDO es la marca comercial utilizada por toda la red BDO y para todas sus firmas miembro.

Copyright © 2025. Todos los derechos reservados. Publicado en España.