

Reglamento Espacio Europeo de Datos Sanitarios

I. Contexto y objetivos.

Después de la revisión de las respuestas del Ministerio de Sanidad a las primeras propuestas de AseBio, el equipo de la Asociación, junto con el grupo de trabajo de inteligencia artificial y nuevas tecnologías, ha realizado un análisis en profundidad del **capítulo IV** relativo al **uso secundario de los datos**, y perteneciente al [Reglamento \(EU\) 2025/327 relativo al Espacio Europeo de Datos de Salud \(EEDS\)](#), publicado en marzo de 2025 por parte del Parlamento Europeo y del Consejo en el Diario Oficial de la Unión Europea.

El objetivo principal de este análisis es extraer los focos más relevantes en la aplicación del Reglamento en las actividades desarrolladas por el sector biotecnológico, a la par que perfilar y argumentar las propuestas de AseBio de forma anticipada a la aplicación de las normas sobre el uso secundario de la mayoría de las categorías de datos. En paralelo, AseBio considera que estas propuestas pueden ser una aportación valiosa para la futura Ley de Salud Digital.

Este documento se estructura en dos secciones.

Por un lado, el posicionamiento e iniciativas de colaboración en aspectos destacados del capítulo IV:

1. Organismos de acceso a los datos sanitarios.
2. Entorno de tratamiento seguro.
3. Acceso al dato.
4. Remuneración del Health Data Holder.

Por otro lado, una propuesta de cooperación para la elaboración de una guía de buenas prácticas que posicione a España en las posiciones de liderazgo en cuanto a la implementación de este Reglamento.

II. Análisis del Capítulo IV. Uso Secundario.

El uso secundario de datos en salud representa un pilar fundamental para el avance de la investigación biomédica, el fortalecimiento de la salud pública y el desarrollo de soluciones médicas innovadoras. El presente Reglamento busca la creación del **Espacio Europeo de Datos de Salud (EEDS)**, con el propósito de facilitar el uso secundario de estos datos para fines de interés público, como la investigación, la innovación, la formulación de políticas, la preparación y respuesta ante amenazas para la salud, la seguridad del paciente, la medicina personalizada, las estadísticas oficiales y la regulación sanitaria. Dicho uso se debe habilitar tanto para organizaciones públicas como privadas, siempre que los propósitos estén dentro de los establecidos por la regulación.

1. Organismos de acceso a los datos sanitarios.

Conforme al reglamento EEDS, en su artículo 55, los Estados Miembros designarán uno o varios **organismos de acceso a los datos sanitarios (Health Data Access Body, HDAB)** responsables de llevar a cabo una serie de tareas y obligaciones descritas en este reglamento. AseBio opina que las empresas y centros de investigación, como **Health Data User**, necesitan no tener que acudir a varios organismos en caso de necesitar diversos datasets de fuentes diferentes, y por eso proponemos al Ministerio de Sanidad que se pueda **acudir a una “ventanilla única”**, central o distribuida, para realizar las solicitudes de acceso al dato de salud.

Dado que el Ministerio y las Comunidades Autónomas son los organismos competentes para coordinar la gobernanza de un sistema multi-organismo de acceso a datos sanitarios, su papel resulta fundamental para asegurar un acceso ágil y seguro a la información. En este contexto, **AseBio se ofrece a aportar recomendaciones basadas en la experiencia de sus socios** en relación con los metadatos, abordando aspectos clave como la calidad técnica, la calidad clínica, la completitud y el formato, de modo que se garantice la comparabilidad de conjuntos de datos provenientes de distintos proveedores de datos cuando esto sea posible. Estas recomendaciones están siendo trabajadas ya por algunos proyectos que están desarrollando pautas de metadato y etiquetado de calidad, como lo está definiendo [TEHDAS2](#) o el proyecto [Quantum](#) con un enfoque ‘top-down’. Sin embargo, aquí proponemos un enfoque desde la experiencia práctica con Data Holders nacionales y la usabilidad real de los distintos conjuntos de datos (un enfoque ‘bottom-up), que complemente los esfuerzos europeos y refleje la realidad de las prácticas en nuestro territorio.

Además, **AseBio manifiesta su disposición a participar en fases tempranas de prueba** (“early testing”) de solicitudes de acceso a datos entre regiones (cross-regiones), incluyendo la posibilidad de involucrar a algunos **Health Data Holders** miembros. Este ejercicio permitiría contrastar el funcionamiento del mecanismo de “data permit” y evaluar la adecuación del metadato y el etiquetado asociados a la Calidad de los Datos (Quality of Data, QoD), especialmente al integrar información procedente de diferentes Comunidades Autónomas, cada una con sus propios sistemas, protocolos asistenciales y procesos de codificación.

Asimismo, es de sobra conocido que un dataset que represente a una misma subpoblación, cuando sea elaborado por distintas instituciones no será comparable a no ser que la elaboración comparta una metodología común. Por ello, y de cara a elaboración de guías para la **creación de datasets específicos por parte de los distintos dataholders**, AseBio se ofrece a colaborar con propuestas técnicas a través de la experiencia de sus miembros, con el objetivo de que estos sean comparables cuando se trate de cohortes con las mismas características clínicas.

2. Entorno de tratamiento seguro.

Según el reglamento EEDS, los HDAB son los organismos responsables de decidir sobre las solicitudes de acceso a los datos que reciben por parte de los Health Data User.

Los Health Data User pueden solicitar la autorización y expedición de un permiso de datos, o, simplemente pueden realizar la petición de datos de salud. Los HDAB proporcionarán acceso a los datos sanitarios electrónicos con arreglo a un permiso de datos únicamente a través de un entorno de tratamiento seguro (Secure Processing Environment; SPE) que esté sujeto a medidas técnicas y organizativas y a requisitos de seguridad e interoperabilidad. Ante una solicitud de descarga, se revisarán los datos sanitarios electrónicos incluidos en la misma para garantizar sólo la descarga de datos electrónicos no personales.

Desde el punto de vista de AseBio, este requerimiento, por sí mismo, no garantiza que las compañías de desarrollo **como las biotecnológicas puedan desarrollar o en su caso, validar un producto sanitario que estén desarrollando**. Debe tenerse en cuenta que los países que mejor den cabida a estas necesidades serán los que atraigan la mayor inversión y desarrollos biotecnológicos.

La validación de un producto sanitario requiere un escenario donde puedan trazar completamente el proceso de fabricación, incluyendo la validación: datos usados en entrenamiento, datos usados en validación, test... Lo cual supone contar con los datos disponibles a nivel local fruto de una descarga o un entorno que garantice su disponibilidad durante los años que establezca la regulación (por ejemplo, 5 años). Como se comentaba, la posibilidad de descarga viene de la mano de contar con una expedición de un permiso de datos, a lo cual no todas las compañías pueden acceder y en estos momentos no se especifica que los Entornos de Procesamiento Seguro vayan a contar con dichas funcionalidades.

Desde AseBio, consideramos esencial encontrar una **solución unificada que sea estándar para todos los Health Data Users**, puesto que el panorama para el sector biotech será completamente distinto en el caso de que el Espacio Nacional de Datos Sanitarios (ENDS) permita el desarrollo de dispositivos basados en IA/datos o que la/los usen, o en caso de que no lo permita. En el primer escenario, el ecosistema florecerá en torno al ENDS, pero, por el contrario, si no lo permite, los desarrolladores seguirán llegando a acuerdos con instituciones sanitarias y no utilizarán el ENDS.

Para ello, nos ofrecemos a plantear y contrastar distintos modos de **garantizar dicha trazabilidad, incluyendo todos los aspectos técnicos necesarios** (persistencia, bloqueo, etc..), más allá de las recomendaciones del proyecto [SHAIPED](#). A modo informativo, el proyecto *SHAIPED* (*Supporting Health Data Access Bodies to establish AI pathways enabling Deployment of AI as medical device tools*), que sólo acaba de comenzar, tiene como objetivo facilitar el desarrollo, validación y despliegue de herramientas de **inteligencia artificial (IA) como dispositivos médicos** dentro del Espacio Europeo de Datos

de Salud (EHDS). Este proyecto trabaja para crear vías regulatorias claras, promover el uso seguro de datos sanitarios reales, y garantizar que las soluciones de IA cumplan con las normativas europeas como el **AI Act** y el **Reglamento de Dispositivos Médicos (MDR)**. De nuevo, este proyecto tiene un enfoque 'top-down', que proponemos complementar con otro 'bottom-up' desde nuestra experiencia como desarrolladores.

Nuestra propuesta tiene como objetivo que el Espacio Nacional de Datos Sanitarios tenga la capacidad de soportar el desarrollo/validación de productos biotecnológicos de manera proactiva en Europa y sea consistente en la regulación asociada. Consideramos de especial relevancia, y más allá de las iniciativas puestas en marcha que las pymes deben estar preparadas para marzo de 2029, lo cual implica una actitud proactiva para ser pioneros a nivel europeo. Además, los estados miembros que antes resuelvan estas lagunas serán los primeros en atraer a las compañías desarrolladoras.

3. Acceso al dato.

El acceso al dato podría causar un desequilibrio competitivo si se comparan empresas que tienen su sede en Europa y deben acogerse a este reglamento, y empresas con filiales en Europa, pero con central fuera de Europa, que no deban alinearse con él (puesto que los datos afectos al reglamento normalmente se encuentran bajo el control de las matrices, no de las filiales).

Con el objetivo de conocer y minimizar el caso de un posible desequilibrio competitivo de acceso al dato, **AseBio plantea la idea de introducir un mecanismo de control como que el acceso mutuo a los datos este bajo una aprobación de permiso de acceso.**

Para comprobar la magnitud de aplicación de esta medida, AseBio lanzó una encuesta a sus socios con el fin de conocer la cantidad de casos que podrían verse afectados y recabar la opinión y puntos de vista del ecosistema biotecnológico en torno a aspectos clave de acceso al dato.

De las entidades que respondieron a la encuesta, el **52% son empresas filiales en España**, mientras que el **48% tienen su matriz en el país**.

- Por un lado, y poniendo el foco en esas entidades que son filiales en España, el **86% de ellas tienen su matriz en la Unión Europea, mientras que el 14% tienen su matriz fuera de Europa**. Las entidades con matriz europea deberán acogerse al reglamento EHDS, al igual que el 48% de empresas con matriz en España, lo cual muestra indicios de un **desequilibrio competitivo bajo**.
- Por otro lado, y ahondando en el **14% restante de entidades con matriz no europea**, el **67% tienen interés en el acceso a los datos**, pero la mitad de **estos interesados** responden que la matriz **no estaría dispuesta a compartir los datos**.

4. Remuneración del Health Data Holder.

La gestión, preparación y otras acciones necesarias para compartir los datasets conllevan todo un proceso complejo que supone una carga de tiempo y recursos por parte del Health Data Holder. Por ello, **AseBio considera que el Health Data Holder privado debe tener derecho a una remuneración (tasa)** que incluya un margen por todo el proceso necesario, al igual que en otras actividades reguladas llevadas a cabo por agentes privados (por ejemplo, las redes eléctricas o de telecomunicaciones). Esta consideración se apoya en el hecho de que hay empresas que manejan una gran carga de información (por ejemplo, diagnóstico por imagen) y pueden llegar a recibir un volumen muy alto de peticiones.

La remuneración/tasa adoptada debe ser consecuente en función del alcance y la magnitud de la actividad desarrollada y de la magnitud o relevancia del tipo de dato. Por ello, es importante conocer que se define y reconoce como coste o tipos de costes, además de dimensionar éste. Para ello, debemos tener en cuenta que el coste de Intellectual Property Right (IPR) es diferente a una tasa de almacenamiento/preparación de datos, esto puede traducirse en costes de personal u otros. El interés común de esta definición debe residir en hacer lo que esté bien compensado.

Para ello, desde AseBio consideramos relevante poder dimensionar los costes que una empresa Health Personal Data puede tener. A continuación, se presenta una relación de costes directos e indirectos:

Costes Directos

COSTES DIRECTOS		
Actividad	Esfuerzo	Coste
Preparación y estructuración de los datos	<ul style="list-style-type: none"> Extracción, anonimización o pseudonimización del dato. Limpieza y organización de los datos de forma que puedan ser utilizados por terceros cumpliendo con los requisitos normativos y técnicos 	<ul style="list-style-type: none"> Costes de personal técnico. Licencias de software especializado. Coste de herramientas de transformación de datos.
Almacenamiento y procesamiento	<ul style="list-style-type: none"> Almacenamiento de los datos en infraestructuras seguras, interoperables y escalables 	<ul style="list-style-type: none"> Costes asociados a servidores físicos o servicios en la nube. Mantenimiento de bases de datos. Procesamiento para estructurar los datos conforme

		a estándares europeos (como HL7 FHIR).
Cumplimiento normativo y legal	<ul style="list-style-type: none"> Garantizar la conformidad con el RGPD, la legislación nacional y el propio reglamento EHDS 	<ul style="list-style-type: none"> Costes legales importantes Costes por contratación de un delegado de protección de datos (DPO). Costes de asesoría legal externa Costes por redacción de documentación de consentimiento o cláusulas contractuales
Gestión de accesos y solicitudes	<ul style="list-style-type: none"> La empresa debe contar con procesos, sistemas y personal para revisar y aprobar solicitudes de acceso a los datos 	<ul style="list-style-type: none"> Recursos administrativos Recursos técnicos Recursos jurídicos. Desarrollo de plataformas de control de acceso.
Derechos de propiedad intelectual (IPR)	<ul style="list-style-type: none"> Aunque los datos brutos pueden no tener IPR, si puede haber derechos asociados a su forma estructurada o al software utilizado para su tratamiento 	<ul style="list-style-type: none"> Costes de licencias, cesiones y protección de los desarrollos propios.
Seguridad y ciberprotección	<ul style="list-style-type: none"> La protección de datos sensibles requiere medidas tecnológicas robustas como cifrado, control de accesos, sistemas de detección de intrusos y auditorías de ciberseguridad. 	<ul style="list-style-type: none"> Estos elementos suponen un coste directo y recurrente
Supervisión técnico-científica	<ul style="list-style-type: none"> La validación del valor y aplicabilidad científica de los datos, y la elaboración de documentación técnica clara, también conlleva costes. 	<ul style="list-style-type: none"> Suelen implicar la participación de expertos, comités científicos o asesores técnicos.

Costes Indirectos

COSTES INDIRECTOS		
Actividad	Esfuerzo	Coste
Soporte técnico de terceros	<ul style="list-style-type: none"> Muchas empresas dependen de proveedores externos para mantener sus sistemas operativos, resolver incidencias o garantizar la interoperabilidad. 	<ul style="list-style-type: none"> Contratos de soporte, acuerdos de nivel de servicio (SLA) y asistencia técnica generan costes indirectos frecuentes.
Mantenimiento de sistemas	<ul style="list-style-type: none"> Los sistemas deben actualizarse regularmente para mantener la compatibilidad con estándares y normativas en evolución 	<ul style="list-style-type: none"> Renovaciones de licencias, migraciones a nuevas plataformas y ajustes técnicos, que pueden suponer inversiones no triviales.
Formación continua del personal	<ul style="list-style-type: none"> El personal debe mantenerse al día con nuevas regulaciones, estándares tecnológicos y buenas prácticas. 	<ul style="list-style-type: none"> Cursos de protección de datos, interoperabilidad, ética del dato o ciberseguridad son ejemplos de formación necesaria
Auditorías y revisiones externas	<ul style="list-style-type: none"> Es habitual que haya que someterse a auditorías de cumplimiento, tanto normativas como técnicas, realizadas por entidades externas 	<ul style="list-style-type: none"> Estas revisiones, necesarias para validar la calidad y seguridad del sistema, tienen un coste económico y de tiempo.
Coordinación y comunicación interna y externa	<ul style="list-style-type: none"> La gestión de datos en un entorno regulado requiere una estrecha colaboración entre equipos técnicos, legales y científicos, 	<ul style="list-style-type: none"> Todo este esfuerzo humano y organizativo conlleva costes indirectos.

	además de interlocución con terceros como autoridades sanitarias o usuarios de datos	
Ineficiencias operativas y riesgos	<ul style="list-style-type: none"> • A menudo se generan costes por ineficiencias, errores humanos, duplicación de tareas o retrasos en la entrega de datos. 	<ul style="list-style-type: none"> - También hay un coste potencial en términos de riesgo reputacional o pérdida de ventaja competitiva si los datos compartidos tienen valor estratégico.

III. Guía de Buenas Prácticas.

El Reglamento EEDS traerá consigo la **implementación de una gran variedad de novedades** que deberán ser acogidas e implantadas en muchas instituciones y empresas, conllevando la **adopción de nuevos protocolos de trabajo**. Por ello, desde AseBio, como asociación nacional de bioempresas, que también agrupa por ejemplo a institutos de investigación biomédica, lanzamos al Ministerio una **propuesta de elaboración de una guía de buenas prácticas** que sirva de acompañamiento y ayuda a las instituciones públicas y al tejido empresarial, para lo cual **ponemos a disposición nuestra experiencia y colaboración para una redacción conjunta**.

La **motivación de esta propuesta** nace de la **necesidad de abordar los siguientes puntos considerados de interés por el sector biotecnológico**:

1. **Categorías mínimas de datos sanitarios electrónicos que deben poner a disposición de los titulares de datos.**
 - Informar a los Health Data Holder que las imágenes médicas y patológicas forman parte de las categorías prioritarias de datos sanitarios electrónicos para su uso secundario tiene un potencial significativo. En general, difundir a los Health Data Holder sus obligaciones de cara a una adecuada gestión de los datos para que estos sean realmente útiles.
 - Definir y describir las tipologías incluidas en las categorías de datos sanitarios.
 - Transparencia en el uso de los datos.
Recomendación de que los conjuntos de datos preparados por los usuarios, que cuentan con un acceso mediante un permiso de

datos, se devuelvan a los titulares originales de los datos. Esta devolución debe incluir una descripción detallada de los flujos de trabajo de preparación implementados en un formato reutilizable. De este modo, los titulares de los datos pueden garantizar que las metodologías y los procesos aplicados a los datos sean transparentes y que otros investigadores puedan reproducirlos o utilizarlos como base, fomentando así un ecosistema de datos más colaborativo y fiable.

- Considerar la inclusión de los catálogos de los biobancos dentro de los datos ómicos y regular los procesos de petición, secuenciación y cesión de los datos resultantes.

2. Derechos de propiedad intelectual y secretos comerciales.

- Posibilidad de introducir un periodo de tiempo entre la generación de los datos y la obligación de compartirlos.
- Poner a disposición de las entidades modelos de contrato para proteger la propiedad intelectual en función de la tipología del dato.
- Proporcionar recomendaciones de pautas para guiar a los Data Holder en acuerdo IPR según sus necesidades.

3. Obligaciones de los organismos de acceso a los datos sanitarios respecto de las personas físicas // Derecho a no participar en el tratamiento de datos sanitarios electrónicos personales para uso secundario.

- Añadir cálculo de estadísticas e información antes y después del proceso de exclusión voluntaria, con el fin de presentar el impacto de ésta de una forma comprensible.

4. Minimización de datos y limitación de la finalidad.

- Pautas para una buena justificación del uso de datos en casos de big data/ predictivos/ exploratorios donde puede ser necesario el acceso a conjuntos grandes de datos que inicialmente no se consideran relevantes.

5. Entorno de tratamiento seguro.

- Pautas para establecer un tratamiento seguro de datos en infraestructura propia con el fin de utilizar pipelines propios de entrenamiento.
- Compartir prácticas y experiencias previas del entorno AseBio para empresas interesadas en el establecimiento de un entorno de

tratamiento seguro y óptimo, y que sea específico como puede ser tratamiento de dato clínico.

- Permitir a las propias empresas especializadas certificarse como un entorno de tratamiento seguro y dar las guías necesarias para ello.
- Guías de elaboración de datasets, de modo que se facilite la comparabilidad de cohortes equivalentes.