



**Máster en Dirección de Sistemas y TIC para la Salud y
en Digitalización Sanitaria**

TRABAJO FIN DE MÁSTER

**La adaptación del sector privado de asistencia
sanitaria al Reglamento del Espacio Europeo
de Datos de Salud (EEDS)**

**Adrian Gorricho
Alba Caballero
Nuria Cudolá
2025**

TRABAJO FIN DE MÁSTER

Título: LA ADAPTACIÓN DEL SECTOR PRIVADO DE ASISTENCIA SANITARIA
AL REGLAMENTO DEL ESPACIO EUROPEO DE DATOS DE SALUD (EEDS).

Autor: ADRIAN GORRICO, ALBA CABALLERO, NURIA CUDOLÁ

Tutor: DÑA. LUCÍA ESCAPA

Madrid, a 30 de Octubre de 2025



ALBA CABALLERO ECHEVERRÍA

Máster en Dirección de Sistemas y TIC para la Salud y en Digitalización Sanitaria



TRABAJO FIN DE MÁSTER

La adaptación del sector privado de asistencia sanitaria al Reglamento del Espacio Europeo de Datos de Salud (EEDS).

Índice

1. REFERENCIA DE CONTENIDOS DEL TEMARIO DEL MÁSTER UTILIZADOS	
2. INTRODUCCIÓN	1
2.1. Objetivos	1
2.2. Estructura	2
3. EL ESPACIO EUROPEO DE DATOS DE SALUD	3
3.1. Introducción al EEDS: Origen, Fundamentos, Principios y Objetivos	3
3.2. Marco Normativo: Reglamento EEDS (UE 2025/327), RGPD, Legislación Española y Otras Normativas Europeas Conexas	4
3.2.1. Reglamento (UE) 2025/327 sobre el EEDS	4
3.2.2. Reglamento General de Protección de Datos (RGPD)	5
3.2.3. Otras normativas relevantes a nivel estatal.	5
3.2.4. Otras normativas relevantes a nivel europeo.	6
3.2.5. Cuadro relacional del marco legislativo	7
3.3. Marco tecnológico: Requisitos funcionales y técnicos	8
3.3.1. Revisión Conceptual y Técnica: Interoperabilidad, Estándares (FHIR, SNOMED CT), Portales del Paciente, Consentimiento Dinámico	8
3.3.2. Revisión Conceptual y Técnica: Software como servicio (SaaS)	9
3.3.3. Requisitos Funcionales	10
3.3.4. Requisitos Técnicos	15
4. AVANCES EUROPEOS EN INTEROPERABILIDAD	19
4.1. <i>E-Health Network</i>	19
4.2. MyHealth@EU	19
4.2.1. Resumen de Paciente. <i>Patient Summary</i>	19
4.2.2. Receta electrónica. <i>ePrescriptions</i>	20
4.3. Estado Actual de Implementación: España y Comparativa Internacional	21
4.3.1. Situación en España	21
4.3.2. Comparativa internacional	21
5. EL ECOSISTEMA DE LA SANIDAD PRIVADA EN EL CONTEXTO DEL EEDS	23
5.1. La sanidad privada en España: una visión estructural	23
5.1.1. Modalidades de financiación	23
5.1.2. Tipos de prestadores en sanidad privada	24
5.2. Nivel de digitalización y capacidades actuales	24
5.2.1. El nodo de la sanidad privada: avances	25
5.2.2. Receta electrónica privada	26
5.2.3. Desafíos clave identificados	27
5.2.4. Gobernanza del dato sanitario en el ámbito privado	29
5.2.5. Casos de uso y ejemplos de integración digital en sanidad privada	30
5.2.6. Financiación e incentivos para la transformación digital	31
5.2.7. Diferencias capacidad de cumplimiento técnico	32
6. PROPUESTA DE SOLUCIÓN PARA LA IMPLEMENTACIÓN DEL EEDS EN LA SANIDAD PRIVADA	35
6.1. Solución propuesta: SaaS	35
6.1.1. Arquitectura Tecnológica Propuesta	35
6.2. Posible modelo de negocio	38
6.2.1. Propuesta de valor	38

6.2.2. Estrategia de acceso al mercado	39
6.2.3. Modelo de ingresos	40
6.2.4. Plan de inversión	40
6.2.5. Plan de acción en fases	40
6.3. DAFO Resumen	41
7. CONCLUSIONES	42
7.1. Grado de consecución de los objetivos planteados	42
7.2. Líneas futuras	43
Bibliografía	44

Índice de figuras

1.	Fechas más relevantes del Reglamento del EEDS	5
2.	Marco Normativo EEDS	7
3.	Relación de Empresas certificadas SERP	27
4.	Tabla comparativa: Grandes hospitales vs. pequeñas clínicas	33
5.	Esquema de comunicación de los sistemas de Historia Clínica Electrónica Interoperables	36
6.	Arquitectura tecnológica de la propuesta	36
7.	Plataforma Modular Interoperable	37
8.	Análisis DAFO	41

RESUMEN

El presente Trabajo Fin de Máster se ha centrado en el análisis de la adaptación del sector sanitario privado en España al Reglamento del Espacio Europeo de Datos de Salud (EEDS), aprobado por la Unión Europea en 2025. Este reglamento constituye un hito en la consolidación de un espacio común europeo de datos en el ámbito sanitario, cuyo propósito es garantizar la interoperabilidad, la seguridad y el acceso equitativo a la información clínica en toda la Unión. En particular, el EEDS persigue dos fines fundamentales: por un lado, facilitar la continuidad asistencial transfronteriza mediante el uso primario de los datos, y por otro, promover la investigación, la innovación y el diseño de políticas públicas basadas en evidencia a través del uso secundario de la información clínica, siendo el foco de este proyecto su implantación en lo relativo al uso primario.

El análisis realizado muestra que la sanidad privada en España, que representa un pilar complementario y estratégico al sistema público, se caracteriza por una notable heterogeneidad. En ella coexisten grandes grupos hospitalarios con elevada madurez digital, clínicas medianas con recursos limitados y pequeñas consultas o profesionales independientes con escasa capacidad tecnológica. Esta diversidad genera una clara brecha en cuanto a posibilidades de adaptación al EEDS, ya que mientras los grandes proveedores pueden asumir la inversión y los requisitos técnicos, los actores más pequeños corren el riesgo de quedar excluidos del nuevo ecosistema europeo de datos de salud.

A partir de este diagnóstico, se propone una solución basada en la creación de plataformas intermedias ofrecidas bajo un modelo de software como servicio (SaaS). Estas plataformas actúan como nodos de interoperabilidad, reducen los costes de integración y facilitan el cumplimiento de los estándares europeos, permitiendo que todos los prestadores, independientemente de su tamaño, puedan participar en el EEDS. Entre las funcionalidades contempladas se incluyen la identificación segura de pacientes y profesionales, la trazabilidad de accesos, la gestión de derechos de autoexclusión, el acceso a datos mediante portales y APIs, así como módulos específicos para la transformación y almacenamiento temporal de datos, o la interoperabilidad con los nodos nacionales y europeos.

PALABRAS CLAVE

Espacio Europeo de Datos de Salud (EEDS), Historia Clínica Electrónica (HCE) interoperable, Transformación Digital sanitaria, Sistemas de información hospitalaria, Sanidad Privada, proveedores de salud, Software sanitario, *Big Data* salud, interoperabilidad sanitaria, innovación en salud digital.

Lista de Acrónimos

AEPD	Agencia Española de Protección de Datos.
ATC	<i>Anatomical, Therapeutic, Chemical Classification System</i>
DGA	<i>Data Governance Act</i>
DICOM	<i>Digital Imaging and Communications in Medicine</i>
DSA	<i>Digital Services Act</i>
EEDS	Espacio Europeo de Datos de Salud
EHDS	<i>European Health Data Space</i>
HCE	Historia Clínica Electrónica.
HL7 FHIR	<i>Health Level Seven International Fast Healthcare Interoperability Resources</i>
IA	Inteligencia Artificial.
ICD	<i>International Classification of Diseases</i>
IDMP	Identificación de Productos Medicinales.
IoT	<i>Internet of Things</i>
LOINC	<i>Logical Observation Identifiers Names and Codes</i>
NIS2	<i>Network and Information Systems Directive 2</i>
UE	Unión Europea.
RGPD	Reglamento General de Protección de Datos.
SNOMED CT	<i>Systematized Nomenclature of Medicine - Clinical Terms</i>

1. REFERENCIA DE CONTENIDOS DEL TEMARIO DEL MÁSTER UTILIZADOS

Tema 2.5 - La seguridad TIC. Legislación aplicable. Aplicación del Reglamento General de Protección de Datos. El papel del Delegado de Protección de Datos. Auditorías. Metodologías /Herramientas de Seguridad MAGERIT. SGSI. PILAR.

Tema 2.7- Servicios al usuario final. Redes Sociales. Dispositivos en MOVILIDAD. Identidad digital, certificados electrónicos, firma electrónica.

Tema 3.1 - Los Sistemas de Información de Salud y Socio Sanitarios. Estrategia y Gobernanza. Espacio de Datos de Salud

Tema 3.2 - La aplicación de la normativa de Protección de datos en el sector Salud.

Tema 3.3 - La Interoperabilidad en al ámbito de la Salud.

Tema 3.4 - Las Infraestructuras TIC del sistema sanitario.

Tema 3.7 - Las TIC y la continuidad asistencial.

Tema 3.10 - Estrategias, infraestructuras y aplicaciones avanzadas basada en datos para la Investigación en Salud y Biomedicina. Comités de Ética

Tema 4.1 - Sistemas, servicios y aplicaciones institucionales: nodo SNS -HCDSNS, receta electrónica.

Tema 4.2 - Sistemas, servicios y aplicaciones departamentales hospitalarios.

Tema 4.5 - Sistemas, servicios y aplicaciones orientadas a la ciudadanía

Tema 4.6 Capacitación en TIC de profesionales y pacientes.

Tema 4.7 - Aplicaciones en asistencia sanitaria e investigación.

Tema 4.10 - Prospectiva y escenarios de futuro de la Salud Digital. Investigación e innovación en el Espacio de Datos de Salud

2. INTRODUCCIÓN

La transformación digital en el ámbito sanitario constituye uno de los principales retos y oportunidades de la Unión Europea en los próximos años. La reciente aprobación del Reglamento del Espacio Europeo de Datos de Salud (EEDS) (UE 2025/327) supone un hito en la creación de un ecosistema común que garantice el acceso, la interoperabilidad y el intercambio seguro de información clínica en toda Europa. Este marco normativo no solo persigue facilitar la asistencia transfronteriza y el empoderamiento del paciente como dueño de sus datos, sino también promover la investigación, la innovación y el desarrollo de políticas públicas basadas en evidencia.

En este contexto, la sanidad privada en España, que representa un pilar complementario al sistema público y concentra una parte significativa de la provisión de servicios, enfrenta el desafío de adaptarse a las exigencias del nuevo reglamento. La heterogeneidad de sus actores —grandes grupos hospitalarios, clínicas medianas y pequeñas, así como profesionales independientes— plantea diferentes capacidades de digitalización y recursos para cumplir con los requisitos técnicos, legales y organizativos que el EEDS establece.

El presente trabajo se centra en analizar cómo el sector privado de asistencia sanitaria puede abordar este proceso de adaptación. El proyecto aspira a contribuir con una visión estructurada y soluciones escalables que faciliten la transición hacia un modelo sanitario más digital, conectado y centrado en el paciente, en línea con los objetivos estratégicos de la Unión Europea en materia de salud digital.

2.1. Objetivos

El objetivo principal del proyecto es realizar una propuesta práctica para la adaptación del sector privado de asistencia sanitaria al Reglamento del Espacio Europeo de Datos de Salud **en su uso primario**. Dentro de esta propuesta, se definen los siguientes objetivos específicos:

- Identificar los diferentes tipos de prestadores de asistencia sanitaria en el ámbito de la sanidad privada en España: Grupos hospitalarios, profesionales independientes, agrupaciones profesionales, etc.
- Identificar los requerimientos, técnicos y funcionales, para la puesta a disposición de las categorías prioritarias específicas en el EEDS.
- Identificar los recursos disponibles para llevar a cabo la puesta a disposición de las categorías prioritarias específicas en el EEDS.
- Proponer una solución para que los prestadores sanitarios privados y/o soluciones existentes de Historia Clínica Electrónica (HCE) puedan poner a disposición sus HCE en el EEDS para uso primario y hacer disponibles sus datos para uso secundario a través de esta solución, cumpliendo los requisitos del reglamento.
- Definir la arquitectura tecnológica de la solución, requisitos a nivel de seguridad, RGPD y el modelo de negocio de la solución.

Para poder realizar esta propuesta, este trabajo se ha basado en un enfoque cualitativo, apoyado en el análisis documental y del diseño de soluciones tecnológicas de alto nivel. Se fundamenta en los siguientes ejes:

- **Marco teórico y normativo:** : Se analizan fuentes primarias (reglamentos y directivas de la Unión Europea (UE), normativa nacional aplicable), y secundarias (informes, estándares de interoperabilidad existentes) para comprender el marco del EEDS, la estructura de la sanidad privada en España actualmente y las implicaciones del marco en la misma.
- **Análisis y estudio de iniciativas existentes:** Desde la perspectiva de la interoperabilidad y los sistemas de información en salud, se estudian los requerimientos técnicos y funcionales del EEDS, y cómo estos interactúan con los sistemas actuales de historia clínica digital del sector

privado. Se revisan proyectos existentes para extraer buenas prácticas, dificultades detectadas y posibles modelos de integración para asegurar que los prestadores de servicios sanitarios privados pudieran poner a disposición sus datos al EEDS.

- **Diseño de la solución:** A partir del análisis anterior, se proponen soluciones de alto nivel, escalables y adaptadas al tamaño y capacidad de los distintos tipos de prestadores (grandes grupos, clínicas pequeñas y profesionales independientes).

2.2. Estructura

En esta sección se muestra una breve descripción del contenido de este documento, que se distribuye de acuerdo con la metodología escogida como sigue:

- **Capítulo 1:** Referencia de contenidos del temario del máster utilizados.
- **Capítulo 2:** Introducción. Presenta el proyecto desarrollado. Expone el ámbito en el que ha tenido lugar y los principales objetivos y resume la estructura seguida en esta memoria.
- **Capítulo 3:** El Espacio Europeo de Datos de Salud. Describe el contexto en el que tiene lugar el proyecto. Presenta el marco teórico y normativo y requisitos exigibles. Este capítulo pretende definir claramente a dónde queremos llegar.
- **Capítulo 4:** Avances Europeos en interoperabilidad. Presenta el análisis de las iniciativas europeas ya existentes en cuanto a la interoperabilidad. Este capítulo pretende completar el estado del arte actual en cuanto a la tecnología ya desarrollada y como aplica a la implantación completa del EEDS.
- **Capítulo 5:** El ecosistema de la sanidad privada en el contexto del EEDS. Presenta el análisis del estado de la sanidad privada actualmente, así como el nivel de interoperabilidad disponible de los sistemas de Historia Clínica Electrónica respecto al exigido por el EEDS y los recursos con los que se cuenta. Este capítulo pretende acotar de donde partimos.
- **Capítulo 6:** Propuesta de solución para la implementación del EEDS. Tras el análisis realizado en los puntos anteriores, describe a alto nivel una propuesta de plataforma de software que permita cumplir el reglamento a los centros privados sea cual sea su tamaño e introduce un posible modelo de negocio a seguir para implementar esta solución.
- **Capítulo 7:** Conclusiones y líneas futuras. Muestra las conclusiones, expone los objetivos alcanzados y las líneas futuras de trabajo a seguir.

3. EL ESPACIO EUROPEO DE DATOS DE SALUD

3.1. Introducción al EEDS: Origen, Fundamentos, Principios y Objetivos

El Espacio Europeo de Datos de Salud (EEDS, conocido en inglés como *European Health Data Space*, *EHDS*) es una iniciativa clave de la Unión Europea para crear un ecosistema común que permita el uso y el intercambio seguro de datos sanitarios electrónicos en toda Europa. La creación del Espacio Europeo de Datos de Salud (EEDS) se enmarca dentro de la Estrategia Europea de Datos [1], cuyo objetivo es aprovechar el potencial de los datos en distintos sectores estratégicos. En el ámbito sanitario, esta iniciativa busca garantizar un acceso seguro, interoperable y ético a la información de salud, tanto para su uso primario (asistencia) como secundario (investigación, innovación, política sanitaria) [2].

Su **origen** se encuentra en las lecciones aprendidas durante la pandemia de COVID-19, que evidenció los beneficios de compartir datos de salud a nivel internacional para tomar decisiones informadas y desarrollar nuevas terapias (por ejemplo, vacunas) en tiempo récord. Sin embargo, hasta ahora el intercambio de datos sanitarios ha estado limitado por reglas éticas y legales fragmentadas – en particular, por la aplicación dispar del Reglamento General de Protección de Datos (RGPD) en cada país.

El desarrollo del EEDS está anclado en **principios** éticos y valores europeos compartidos: equidad en el acceso a los datos, respeto a los derechos fundamentales (como la privacidad), transparencia en la toma de decisiones y no discriminación. Un principio central es empoderar al paciente como dueño de sus datos: cualquier ciudadano, sin importar en qué país de la UE se encuentre, debe poder acceder y controlar su información sanitaria de forma segura, gratuita y comprensible. Esto implica que el paciente pueda decidir quién accede a su historial clínico y pueda compartirlo fácilmente con profesionales de salud de otro estado miembro, superando barreras geográficas o lingüísticas. El EEDS promueve así un modelo centrado en el paciente (*person-centric*) que rompe con la lógica fragmentada actual, impulsando la interoperabilidad real entre sistemas nacionales de salud.

El EEDS persigue tres **objetivos** principales [1]:

- Capacitar a las personas para acceder y compartir sus datos de salud electrónicos más allá de fronteras cuando reciben asistencia sanitaria (uso primario de los datos).
- Facilitar la reutilización segura y confiable de los datos de salud con fines de investigación, innovación, formulación de políticas públicas o medidas regulatorias en salud (uso secundario de los datos).
- Fomentar un mercado único de sistemas de historia clínica electrónica (HCE), estableciendo estándares comunes de interoperabilidad que impulsen la innovación y el buen funcionamiento del mercado interior de tecnologías sanitarias.

En esencia, se busca aprovechar plenamente el potencial de los datos de salud en beneficio de pacientes, profesionales, investigadores, autoridades y empresas, mediante un intercambio y uso de datos seguro, protegido y confiable a escala europea.

Con estos objetivos, la Comisión Europea presentó en mayo de 2022 un borrador de reglamento para el EEDS como parte de la estrategia para una Unión Europea de la Salud más integrada. Tras amplias negociaciones, el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, fue finalmente aprobado el 11 de febrero de 2025 y publicado en el Diario Oficial de la UE el 5 de marzo de 2025, entrando en vigor el 26 de marzo de 2025. El Reglamento (UE) 2025/327 es el primer marco jurídico uniforme que garantizará el acceso, uso y compartición de datos de salud electrónicos en todos los Estados miembros, evitando la fragmentación donde cada país (o en el caso de España, cada comunidad autónoma) gestiona sus propios sistemas con distintas plataformas y normas. Sin embargo, este reglamento no es la única normativa que afecta al tratamiento de datos de salud, por lo que es necesario comprender el marco normativo en su conjunto.

3.2. Marco Normativo: Reglamento EEDS (UE 2025/327), RGPD, Legislación Española y Otras Normativas Europeas Conexas

El Marco Normativo del EEDS se compone de un reglamento europeo de aplicación directa, articulado con el RGPD como garante de la privacidad, complementado por la adecuación de las leyes nacionales (en España, LOPD GDD, Ley 41/2002, etc.) y en sinergia con un conjunto de normativas europeas horizontales (Inteligencia Artificial -IA-, datos, servicios digitales). Este andamiaje legal sienta las bases para un espacio común de datos de salud, donde todos los actores –públicos y privados– operen bajo reglas claras y homogéneas en toda la Unión.

3.2.1. Reglamento (UE) 2025/327 sobre el EEDS

El pilar normativo del Espacio Europeo de Datos de Salud es el mencionado Reglamento (UE) 2025/327 [3], de aplicación directa en todos los Estados miembros. Al ser un reglamento europeo, no requiere transposición nacional, lo que garantiza la unidad de criterios legales en toda la UE. El texto legal establece las condiciones y garantías para el tratamiento de datos de salud electrónicos tanto en el ámbito de la atención sanitaria (uso primario) como en la reutilización para fines secundarios. También modifica dos normas existentes: la Directiva 2011/24/UE (referente a derechos de los pacientes en la asistencia sanitaria transfronteriza) y el Reglamento (UE) 2024/2847 (relativo a redes y registros sanitarios específicos), para alinearlos con el nuevo marco del EEDS.

En concreto, el reglamento (UE) 2025/327 establece en su artículo 3 el derecho de las personas físicas a acceder de forma gratuita e inmediata a las categorías prioritarias específicas de datos de salud electrónicos personales (como la historia clínica resumida del paciente. Si bien respetando al mismo tiempo la necesaria viabilidad tecnológica, se trata de un derecho que debe aplicarse independientemente del Estado miembro en el que se traten los datos, el tipo de prestador de asistencia sanitaria, las fuentes de datos o el Estado miembro de afiliación de la persona física.

En sus artículos [6, 49, 68., 72 y 73], indica que el EEDS debe facilitar a las personas físicas la disponibilidad de sus datos en formato electrónico, además de garantizar un mejor control sobre el acceso e intercambio de los mismos.

Se establece también una obligación jurídica para los prestadores de servicios sanitarios, que son considerados "tenedores de datos de salud", de poner a disposición de los organismos responsables los datos para uso secundario.

Pese a que la entrada en vigor del reglamento fue 26 de marzo de 2025, las distintas obligaciones cuentan con fechas de aplicación progresivas. A partir del 26/03/2027, los prestadores de servicios sanitarios, tanto públicos como privados, deben estar en condiciones de cumplir con las diferentes obligaciones del Reglamento, en las fechas que se relacionan en el artículo 105 del mismo. Así, a partir del 26 de marzo de 2029, deben cumplir con las obligaciones relativas a las categorías prioritarias de historias clínicas resumidas de los pacientes, recetas electrónicas y dispensaciones electrónicas [136.a], y a las obligaciones respecto de los sistemas de historia clínica que traten datos de esas categorías. A partir del 26 de marzo de 2031, serán de aplicación las mismas obligaciones para las categorías prioritarias de estudios de diagnóstico por imagen e informes correspondientes a resultados de pruebas diagnósticas e informes de altas hospitalarias [137.b], así como para los sistemas de historia clínica que traten datos de esas categorías. El capítulo IV, uso secundario, será aplicable en general, a partir del 26 de marzo de 2029.

La Figura 1 ilustra las fechas más relevantes de entrada en vigor del reglamento.

A efectos de este Trabajo de Fin de Máster, se evalúan y tienen en cuenta las labores de adaptación del sector privado de asistencia sanitaria al reglamento en lo relativo a las llamadas **categorías prioritarias**, que incluyen: resúmenes clínicos de paciente, recetas electrónicas/dispensaciones, informes de laboratorio, informes de imagen médica, e informes de alta hospitalaria.

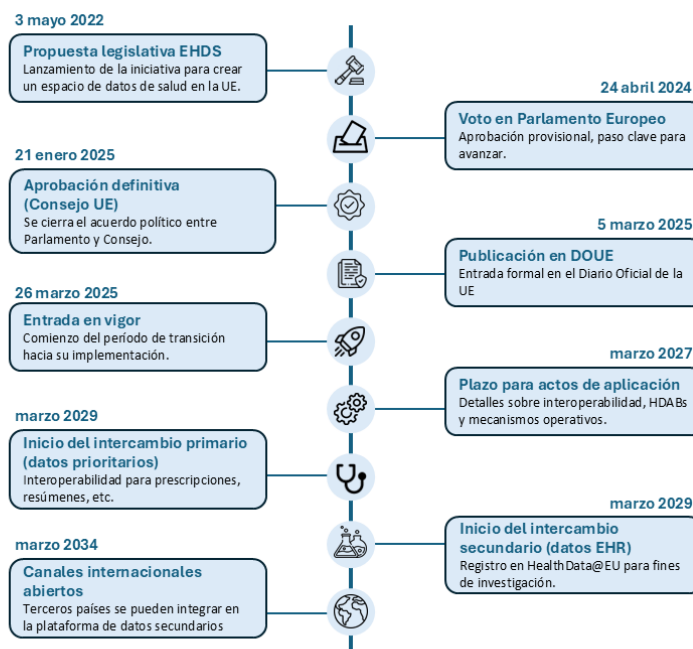


Figura 1: Fechas más relevantes del Reglamento del EEDS

3.2.2. Reglamento General de Protección de Datos (RGPD)

El Reglamento EEDS complementa y se alinea con el Reglamento General de Protección de Datos (UE) 2016/679 (RGPD) [4], que sigue siendo la piedra angular en materia de protección de datos personales en Europa. Dado que los datos de salud son considerados datos sensibles (categoría especial) por el RGPD, su tratamiento está generalmente prohibido salvo que se cumpla alguna excepción legal (por ejemplo, por razones de interés público en salud, fines de atención sanitaria, investigación científica, etc., tal como recoge el Art. 9 RGPD).

El EEDS actúa como una *ley specialis* para el ámbito sanitario, estableciendo un marco más detallado para esos tratamientos excepcionales permitidos. Por ejemplo, el Reglamento EEDS crea mecanismos de acceso y compartición de datos bajo controles estrictos, lo cual proporciona una base jurídica clara (en línea con el RGPD) para que hospitales, investigadores u otras entidades procesen datos de salud sin tener que recabar consentimiento en cada caso.

En cualquier caso, es importante destacar que todas las operaciones dentro del EEDS deben respetar los principios del RGPD (minimización, confidencialidad, integridad, legalidad, etc.) y garantizar los derechos ARCO (acceso, rectificación, supresión, oposición, etc.) de los ciudadanos. De hecho, el Reglamento enfatiza que la reutilización de datos deberá hacerse “respetando los derechos fundamentales y la protección de datos personales”, en plena consonancia con el RGPD.

En resumen, el EEDS no deroga ni debilita la protección de datos vigente, sino que proporciona un marco seguro y armonizado para aprovechar datos sanitarios dentro del espacio de confianza europeo, con salvaguardas legales sólidas.

3.2.3. Otras normativas relevantes a nivel estatal.

En el contexto nacional, España ya cuenta con normas que inciden en el manejo de datos de salud, las cuales deberán coordinarse con el EEDS:

- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD GDD)** [5]. Esta ley adapta el RGPD al ordenamien-

to español, incluyendo disposiciones sobre datos de salud. La LOPD GDD mantiene un enfoque garantista; de hecho, España ha sido identificada como uno de los países con interpretación más restrictiva del RGPD en materia sanitaria. Esto se manifiesta, por ejemplo, en criterios estrictos de la Agencia Española de Protección de Datos (AEPD) para la anonimización o el consentimiento informado en investigación. El EEDS podría ayudar a clarificar y flexibilizar algunos usos secundarios legítimos, ya que establece una gobernanza común que reducirá la incertidumbre jurídica actualmente percibida por las instituciones a la hora de compartir datos por temor a responsabilidad.

- **Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente**[6]. Es la norma básica de derechos del paciente en España, reconociendo el derecho de acceso del paciente a la información de su historia clínica (art. 18) y el deber de confidencialidad de los profesionales. Esta ley garantiza que el paciente puede solicitar y obtener copias de su historia clínica de cualquier centro, público o privado. Sin embargo, en la práctica este acceso ha sido tradicionalmente fragmentado (el ciudadano debe dirigirse a cada proveedor por separado). El EEDS viene a potenciar este derecho, al facilitar electrónicamente que el paciente acceda a todos sus datos de salud de forma unificada y transfronteriza. Asimismo, la ley 41/2002 exige que la historia clínica se lleve con criterios de unidad e integración dentro de cada centro sanitario; el EEDS expande este concepto al plano nacional y europeo, buscando la integración de historias clínicas entre distintos sistemas sanitarios, siempre con consentimiento o legitimación adecuada.
- **Otras normas sanitarias nacionales:** Cabe mencionar la Ley 14/2007 de Investigación Biomédica [7], que regula el uso de muestras biológicas y datos asociados en investigación. Dicha ley introdujo el concepto de consentimiento amplio para usos de investigación (el participante puede consentir que sus datos/muestras se usen en múltiples estudios futuros, sujeto a comités de ética), prefigurando ideas de consentimiento dinámico. También, la Ley 33/2011 General de Salud Pública [8] habilita tratamientos de datos con fines de vigilancia epidemiológica y salud pública. Todas estas disposiciones sectoriales deberán armonizarse con el nuevo marco del EEDS, que ofrece instrumentos adicionales (por ejemplo, los *Health Data Access Bodies* nacionales) para autorizar y supervisar dichos tratamientos con garantías éticas.

3.2.4. Otras normativas relevantes a nivel europeo.

El Espacio Europeo de Datos de Salud no surge en un vacío normativo, sino que forma parte de una estrategia más amplia de la UE en materia digital. Es fundamental la coordinación con otras regulaciones europeas para asegurar la coherencia y compatibilidad del marco general:

- **Reglamento de Inteligencia Artificial (Ley de IA de la UE, propuesta de 2021, próxima a adoptarse)**[9]. La IA aplicada a salud (por ejemplo, algoritmos de diagnóstico o medicina personalizada) requerirá grandes volúmenes de datos de calidad. El EEDS facilitará esos datos, mientras que la Ley de IA establecerá requisitos para que los sistemas de IA sean seguros, transparentes y no discriminatorios. Ambos marcos se refuerzan mutuamente: el EEDS provee datos fiables y gobernados éticamente, y la *IA Act* velará por un uso responsable de esos datos en algoritmos sanitarios.
- **Reglamento de Gobernanza de Datos (Reglamento (UE) 2022/868, *Data Governance Act*, DGA)** [10]. En vigor desde septiembre de 2023, crea mecanismos para facilitar la reutilización de ciertos datos de carácter público o sensible y establece la figura del “altruismo de datos” (donación voluntaria de datos para bien común). Los datos de salud son uno de los dominios de alto valor contemplados. El EEDS complementa al DGA proporcionando la infraestructura específica de salud donde esas prácticas de compartición altruista o intercambio seguro de datos pueden materializarse bajo condiciones uniformes.
- **Ley de Servicios Digitales (Reglamento (UE) 2022/2065, *Digital Services Act*, DSA)**[11]. Aunque está enfocada en plataformas en línea y servicios digitales en general, su espíritu de se-

guridad y confianza en entornos digitales también permea el ámbito sanitario. Por ejemplo, el DSA refuerza obligaciones de ciberseguridad y manejo de datos para grandes servicios digitales, lo cual es relevante si se emplean servicios en la nube o plataformas en el ecosistema del EEDS. De igual modo, el *Digital Markets Act* (Reglamento (UE) 2022/1925) busca evitar abusos de poder de mercado por parte de grandes empresas digitales, algo a tener en cuenta dado que los sistemas de historias clínicas electrónicas y aplicativos de salud suelen ser provistos por un puñado de empresas tecnológicas.

- **Otras iniciativas europeas:** La UE está desplegando normativa complementaria, como el Reglamento de Datos (propuesta de *Data Act*, centrada en acceso a datos de dispositivos y del IoT (*Internet of Things*), aplicable a partir de 2025) que podría incluir dispositivos médicos conectados; y la Ley Europea de Identidad Digital, crucial para que las identidades digitales de los ciudadanos permitan acceder a servicios (incluyendo los sanitarios) de forma segura en cualquier país.

Otra directiva a tener en cuenta es la Directiva 2022/2555, también conocida como NIS2 (*Network and Information Systems Directive 2*), que establece un marco jurídico unificado para garantizar la ciberseguridad en 18 sectores críticos de toda la UE (incluyendo a las entidades que prestan asistencia sanitaria y a las que fabrican medicamentos y productos sanitarios esenciales como entidades clave). También insta a los Estados miembros a definir estrategias nacionales de ciberseguridad y a colaborar con la UE para la reacción y la aplicación transfronterizas. Surge como respuesta al aumento en Europa de las amenazas cibernéticas y eleva el nivel común de ambición de la UE en materia de ciberseguridad, mediante un ámbito de aplicación más amplio, normas más claras y herramientas de supervisión más sólidas. Exige a los Estados miembros que mejoren sus capacidades en materia de ciberseguridad, al tiempo que introduce medidas de gestión de riesgos y requisitos de notificación para entidades de más sectores y establece normas de cooperación, intercambio de información, supervisión y aplicación de medidas de ciberseguridad[12].

3.2.5. Cuadro relacional del marco legislativo

Para facilitar la forma en la que los distintos reglamentos se relacionan puede consultarse la Figura 2.

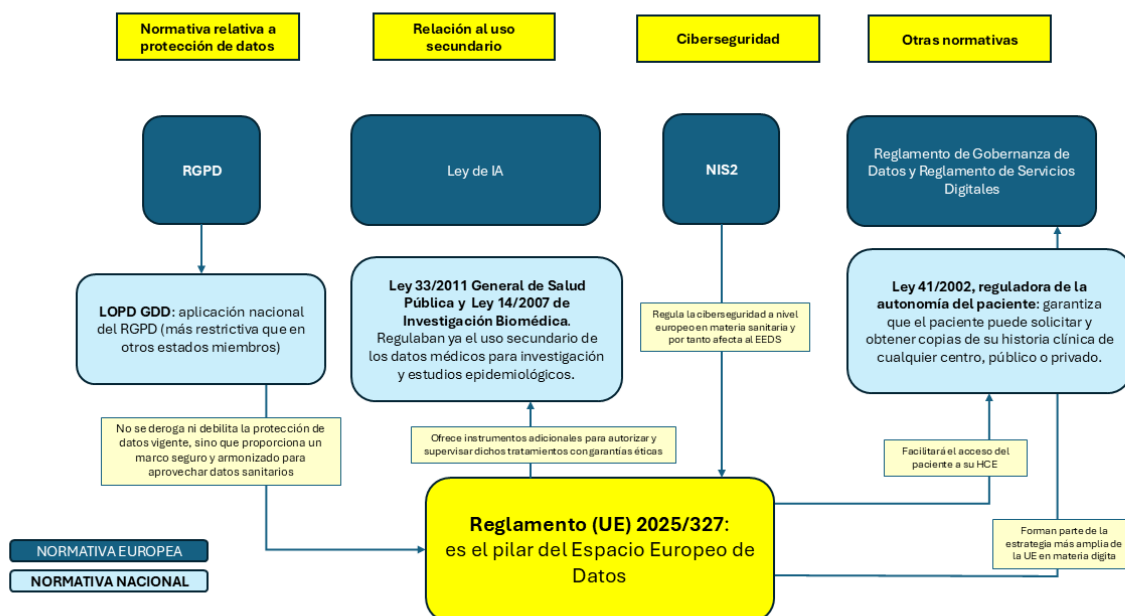


Figura 2: Marco Normativo EEDS

3.3. Marco tecnológico: Requisitos funcionales y técnicos

Todos reglamentos descritos anteriormente nos ofrecen la base legal para el EEDS pero, a su vez, incluyen pautas para su implementación (ya sea en forma de guías o por omisión al limitar ciertas soluciones técnicas). Para poder valorar correctamente las posibles soluciones para la adaptación del sector privado de asistencia sanitaria al Reglamento es necesario entender los conceptos bajo los que se sustentan estas soluciones, así como los requisitos funcionales y técnicos explícitamente descritos en el mismo.

3.3.1. Revisión Conceptual y Técnica: Interoperabilidad, Estándares (FHIR, SNOMED CT), Portales del Paciente, Consentimiento Dinámico

La realización práctica del Espacio Europeo de Datos de Salud exige abordar conceptos técnicos y organizativos clave más allá de conocer el marco normativo bajo el que se fundamenta. A continuación, se revisan los principales: la interoperabilidad y estándares que la hacen posible; las herramientas de acceso del paciente (portales) necesarias para garantizar sus derechos; y el enfoque emergente de consentimiento dinámico para la gestión de autorizaciones de uso de datos.

INTEROPERABILIDAD y ESTÁNDARES

La interoperabilidad es la capacidad de las aplicaciones y los sistemas para intercambiar y utilizar datos de forma cohesionada, segura y automática, independientemente de los límites geográficos, políticos u organizativos[13]. La interoperabilidad puede separarse a su vez en interoperabilidad organizativa (relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus actividades para colaborar con el objeto de alcanzar logros mutuamente acordados), técnica (relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad,) y semántica (relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación)[14]. La interoperabilidad es un pilar central del EEDS, dado que de nada sirve otorgar derechos de acceso o compartir datos si los formatos no son compatibles o comprensibles entre distintos sistemas nacionales. El Reglamento EEDS establece que los sistemas de historia clínica electrónica deberán cumplir requisitos armonizados de interoperabilidad técnica y semántica. En la práctica, esto significa adoptar estándares comunes en toda Europa. De entre los estándares existentes, destacamos por su relevancia para el EEDS:

- **HL7 FHIR (*Fast Healthcare Interoperability Resources*):** este estándar, creado por la organización de estándares sanitarios *Health Level Seven International* (HL7), se trata de un conjunto de normas y especificaciones para el intercambio seguro de datos sanitarios electrónicos. Está diseñado para ser flexible y adaptable, de modo que pueda utilizarse en una amplia gama de entornos y con diferentes sistemas de información sanitaria. El estándar describe los formatos y elementos de datos (conocidos como «recursos») y una interfaz de programación de aplicaciones (API) para el intercambio de HCE. FHIR permite “hablar el mismo idioma” a los sistemas de información de salud a nivel sintáctico[15].
- **Terminologías clínicas estandarizadas (SNOMED CT, LOINC, ICD, etc.):** La interoperabilidad semántica requiere no solo estructurar datos, sino usar vocabularios comunes para referirse a enfermedades, procedimientos, medicamentos, análisis, etc. El estándar de terminología clínica más amplio es SNOMED CT (*Systematized Nomenclature of Medicine - Clinical Terms*), un catálogo con más de 360.000 conceptos médicos[18]. Muchos países europeos (España incluida) ya tienen licencia de SNOMED CT y lo usan en ciertos sistemas (por ejemplo, para problemas de salud o alergias). Otra terminología clave es LOINC (*Logical Observation Identifiers Names and Codes*) empleada para codificar pruebas de laboratorio y resultados clínicos[20]. Asimismo, se mantienen estándares tradicionales como ICD-10/ICD-11 (*International Classifica-*

tion of Diseases) para diagnósticos [19] o ATC (*Anatomical, Therapeutic, Chemical Classification System*) para categorías de fármacos [17]. El EEDS promueve la adopción convergente de estas terminologías: por ejemplo, los *European Electronic Health Record Exchange Format* (EEHRxF) publicados por la Comisión recomiendan SNOMED CT y lo incorporan en los documentos clínicos europeos (como el resumen de paciente) para conceptos como alergias o vacunas. La elevada calidad semántica de los datos es esencial también para posibilitar algoritmos de inteligencia artificial y analítica avanzada sobre datos agregados de múltiples países.

- **Integración de imágenes médicas y otros formatos:** Además de datos alfanuméricos, la interoperabilidad abarca imágenes diagnósticas (radiografías, escáneres, etc.). Aquí el estándar predominante es DICOM (*Digital Imaging and Communications in Medicine*) para almacenar/transmitir imágenes y documentos asociados [16]. El EEDS prevé que imágenes médicas e informes radiológicos formen parte del segundo conjunto de datos prioritarios a intercambiar (hacia 2031). Ello requerirá robustecer redes de transferencia y visores universales compatibles. Del mismo modo, informes de laboratorio (que suelen generarse en PDF) deberán representarse también en formato estructurado (por ejemplo, utilizando FHIR con códigos LOINC para cada prueba).

PORTALES y CONSENTIMIENTO DINÁMICO

Desde el punto de vista técnico, un **portal del paciente** es la “cara amigable” de la interoperabilidad: consume los datos interoperables por detrás y los presenta de forma entendible. En el caso del EEDS, un portal para pacientes es una herramienta conectada a los sistemas de historia clínica que permite al paciente acceder a sus datos médicos (esto podría abarcar desde dar seguimiento a sus consultas, resultados de exámenes, facturación, recetas...). [21] Además de acceder a sus datos, el ciudadano podrá ejercer nuevos derechos digitales en salud, incluyendo la posibilidad de ver el historial de accesos, limitar o bloquear el acceso a ciertos datos sensibles y revocar en cualquier momento el consentimiento dado a terceros. Estas capacidades fortalecen la confianza en el sistema y aseguran un control real y no solo formal sobre la información personal.

En línea con el requisito de que el ciudadano pueda limitar o bloquear el acceso a ciertos datos, en el marco del EEDS surge con fuerza el concepto de **consentimiento dinámico** (*dynamic consent*) para la gestión del uso de datos de salud, especialmente en usos secundarios como investigación. Tradicionalmente, el consentimiento informado para uso de datos en investigación era estático: el paciente firmaba una autorización puntual, frecuentemente amplia, y los datos podrían usarse en adelante dentro de ese alcance. El consentimiento dinámico, por contraste, es un modelo participativo y flexible en el cual los individuos pueden dar, revocar o modificar su consentimiento de forma electrónica en cualquier momento. [22] Se apoya en herramientas tecnológicas (plataformas web, apps móviles...) que permiten al ciudadano visualizar qué datos suyos se están utilizando y para qué proyectos, y decidir en tiempo real si acepta nuevas utilidades o si desea retirarse de alguna previamente consentida. Este enfoque incrementa la transparencia y control del paciente, alineándose plenamente con los principios del EEDS de empoderamiento y confianza. En la práctica, implementar consentimiento dinámico implica varios retos: se necesita infraestructura para recopilar y gestionar las preferencias individuales, integrándolas con los flujos de datos.

OTROS

Otro ámbito técnico que tener presente es la **ciberseguridad**. La interoperabilidad debe lograrse sin sacrificar seguridad, aplicando estándares como cifrado de extremo a extremo, identificación digital (certificados electrónicos para profesionales, nodos seguros de intercambio) y cumplimiento de la normativa NIS2 de seguridad de redes.

3.3.2. Revisión Conceptual y Técnica: Software como servicio (SaaS)

Para poder ofrecer una propuesta, como es el objetivo de este proyecto, también es necesario plantear bajo que tecnología se puede sustentar la solución en sí misma (más allá de los estándares y condiciones

que debe cumplir). La propuesta de este trabajo se basa en un producto de tipo Software como Servicio.

El Software como servicio o SaaS (del inglés *Software as a Service*) es una modalidad de distribución de software basada en la nube, en la que las aplicaciones se proporcionan a los usuarios a través de Internet, generalmente mediante suscripción. A diferencia de los modelos tradicionales, donde el software se instala y mantiene localmente, el SaaS permite el acceso remoto a las aplicaciones, eliminando la necesidad de infraestructura interna y facilitando la gestión centralizada de actualizaciones y mantenimiento [23]. Las características principales del SaaS son [24], [25] :

- Acceso Remoto y Multidispositivo: Los usuarios pueden acceder a las aplicaciones desde cualquier dispositivo con conexión a Internet, sin necesidad de instalaciones locales.
- Modelo de Suscripción: El SaaS opera bajo un esquema de pago periódico, lo que permite a las organizaciones ajustar sus costos según el uso y evitar inversiones iniciales elevadas.
- Escalabilidad y Flexibilidad: Las soluciones SaaS ofrecen la posibilidad de adaptar los servicios contratados según las necesidades cambiantes de la empresa, facilitando la expansión o reducción de recursos.
- Mantenimiento y Actualizaciones Centralizadas: El proveedor del servicio se encarga de las actualizaciones y el mantenimiento del software, asegurando que todos los usuarios dispongan de la versión más reciente sin intervención local.
- Modelo Multitenencia: Una única instancia del software sirve a múltiples usuarios, lo que optimiza el uso de recursos y reduce costes.
- Seguridad y Cumplimiento: Los proveedores de SaaS implementan medidas de seguridad avanzadas y cumplen con normativas específicas para proteger los datos y garantizar la privacidad.

En el apartado 6.1 se detalla el modelo SaaS propuesto ahondando en la razón por la que estas características son relevantes para la adaptación del sector privado de asistencia sanitaria al Reglamento del EEDS.

3.3.3. Requisitos Funcionales

El Espacio Europeo de Datos de Salud define una serie de requerimientos funcionales que deben incorporar los sistemas de información sanitarios para alinearse con la nueva era de intercambio y aprovechamiento de datos. Estas funcionalidades obligatorias o recomendadas abarcan desde cómo interactúan los pacientes con sus datos (portales, consentimiento, transparencia) hasta cómo se integran los sistemas con las plataformas europeas y cómo se gestionan los datos para su uso secundario (aunque esta aplicación no es parte del objetivo del proyecto). A continuación, se analizan dichas capacidades, haciendo hincapié en su impacto en los flujos de trabajo clínicos y considerando diferencias en la implementación según el tamaño de las entidades.

Integración con MyHealth@EU y continuidad asistencial transfronteriza

Una de las funciones centrales del EEDS, en su vertiente de uso primario de datos, es habilitar la continuidad de la atención sanitaria a través de las fronteras. Para ello, todos los sistemas de historia clínica del sector deberán interoperar con la infraestructura MyHealth@EU, que es la red europea de servicios de eSalud para intercambio de datos asistenciales. Actualmente, MyHealth@EU soporta servicios como el Resumen del Paciente (*Patient Summary*) y la Receta Electrónica transfronteriza (eReceta), y se está ampliando a informes de laboratorio, imágenes médicas e informes de alta hospitalaria [26]. En el apartado 4.2 puede consultarse la información ampliada de la iniciativa MyHealth@EU así como de la eHealth Network (4.1).

El reglamento hace obligatoria la participación de los países en MyHealth@EU, lo que de facto obliga a que los hospitales y clínicas puedan enviar y recibir estos conjuntos de datos estándar a través del nodo nacional.

En términos funcionales, esto significa que un sistema HCE debe ser capaz de, por ejemplo, generar automáticamente un Resumen de Paciente en formato europeo cuando llega un solicitante externo válido (un médico en otro Estado) o cuando el propio paciente lo pide. Dicho resumen contendrá información clínica básica (alergias, medicación actual, diagnósticos relevantes, procedimientos recientes) estructurada según las guías europeas. Del mismo modo, el sistema debe poder consumir un resumen extranjero: por ejemplo, si un paciente alemán acude a una clínica española, esta debería poder importar su *Patient Summary* emitido en Alemania para que los facultativos lo consulten en su propio idioma o formato local. Para lograrlo, los proveedores privados necesitan implementar módulos de interoperabilidad que manejan estos flujos: llamadas a servicios web del Punto Nacional de Contacto, conversión de formatos cuando sea necesario, y presentación al usuario clínico de forma integrada en su pantalla, casi como si se tratara de una parte más de la historia.

Otro caso de uso es la eReceta transfronteriza: si un médico en Países Bajos prescribe electrónicamente un fármaco a un paciente francés, y este acude a una farmacia en España, el sistema español debe poder recuperar la prescripción desde MyHealth@EU y tratarla como si fuera una receta local para dispensar el medicamento. Funcionalmente, esto requiere que los sistemas de farmacia o prescripción reconozcan los datos estándares (por ejemplo, identificadores de medicamento posiblemente basados en estándares como IDMP -Identificación de Productos Medicinales- o códigos nacionales mapeados) y gestionen los estados de dispensación devolviendo la información a la red.

Para asegurar el éxito de esta integración, los sistemas privados tendrán que superar diferencias idiomáticas y de flujos de trabajo. Podrían ser necesarias herramientas de traducción automática de términos clínicos o al menos la visualización bilingüe (mostrar el término codificado y su etiqueta en el idioma local). Asimismo, habrá que capacitar a los profesionales en el uso de estas funciones: por ejemplo, saber que en el módulo del HCE hay una sección “Documentos Europeos” donde pueden buscar información previa de un paciente extranjero. En cuanto al flujo de trabajo, idealmente la consulta de datos de MyHealth@EU debería integrarse de forma fluida: quizás dispararse automáticamente al ingresar un paciente nuevo, o con un botón accesible en la interfaz del médico, evitando pasos manuales engorrosos.

El EEDS también exige retroalimentación y calidad: si la información recibida es incompleta o errónea, deben existir mecanismos para solicitar correcciones. De hecho, el paciente tiene derecho a pedir la rectificación de errores en sus datos; esto conlleva que, si un hospital detecta un error en datos originados en otro país, se coordine un procedimiento para subsanarlo a través de los canales de MyHealth@EU o bilaterales. Funcionalmente, este nivel de coordinación es complejo, pero esencial para la confianza en el sistema.

Generación de informes clínicos y portabilidad de datos

Un requerimiento funcional importante es que los sistemas de información puedan producir e intercambiar informes clínicos estandarizados de las principales categorías definidas en el EEDS. Como ya se mencionó, las categorías prioritarias incluyen: resúmenes clínicos de paciente, recetas electrónicas/-dispensaciones, informes de laboratorio, informes de imagen médica, e informes de alta hospitalaria. Las HCE del sector privado deben estar preparadas para generar estos documentos en el formato correcto cuando sea necesario compartirlos, y también para incorporarlos cuando se reciben de otros. Esto implica, por ejemplo, que una clínica privada que hasta ahora entregaba informes de alta en PDF no estructurado, evolucione para generar un informe de alta estructurado con campos codificados (diagnóstico de alta en SNOMED CT o ICD, procedimientos realizados, recomendaciones, etc.) siguiendo la plantilla común europea.

La portabilidad de los datos está estrechamente relacionada: el reglamento busca que los ciudadanos puedan mover sus datos de un proveedor a otro sin obstáculos (*data portability*, consagrada también en el RGPD). Por ello, se recomienda que los sistemas ofrezcan funciones de exportación e importación de datos clínicos en formatos estándar interoperables. Un caso de uso sería un paciente que decide cambiar de proveedor sanitario privado: tendría derecho a llevarse su historial en un formato electrónico

consolidado (por ejemplo, un conjunto de documentos FHIR o un archivo consolidado tipo CDA/XML) e importarlo en la nueva clínica, evitando pérdidas de información. Funcionalmente, las aplicaciones deben permitir al usuario (paciente o profesional autorizado) extraer esos datos con un par de clics, quizás descargando un fichero o mediante transferencias seguras entre sistemas. Esto va más allá del simple PDF; se trata de datos estructurados que otra máquina puede interpretar. Para las entidades, supone un esfuerzo de mapeo de datos internos a estándares externos, pero es crucial para romper los históricos bloqueos de proveedor y fomentar un mercado más competitivo de servicios sanitarios.

La generación automatizada de informes es otra capacidad esperada. Aprovechando los datos estructurados en las HCE, el sistema debería ayudar a los clínicos a confeccionar documentos requeridos por EEDS sin duplicar trabajo. Por ejemplo, al dar de alta a un paciente, el HCE podría compilar automáticamente la información relevante (motivo de ingreso, procedimientos, medicación administrada, citas de seguimiento) en el formato de informe de alta europeo, listo para revisión y firma por el médico. Esto no solo ahorra tiempo, sino que mejora la consistencia y la inclusión de todos los campos obligatorios para intercambiar ese informe con otros centros si fuese necesario. De igual modo, al terminar una consulta, el sistema podría ofrecer generar un resumen de episodio que el paciente se lleve o comparta digitalmente.

Acceso del paciente, portales personales y control de consentimiento

El EEDS coloca al paciente en el centro del ecosistema digital, otorgándole derechos efectivos de acceso y control sobre sus datos de salud. En la práctica, esto se traduce en que los sistemas de información (historias clínicas electrónicas, aplicaciones de salud, etc.) deben proveer funcionalidades de portal del paciente o medios equivalentes donde cada ciudadano pueda ejercer esos derechos de forma fácil y segura. Por ejemplo, todo paciente deberá poder acceder electrónicamente y de forma gratuita a una copia de sus datos de salud en formato legible y, cuando aplique, en formato estructurado estándar. Esto incluye documentos clínicos como informes de alta, resultados de pruebas, imágenes diagnósticas, etc., idealmente ofrecidos en un formato europeo común para facilitar su portabilidad. El reglamento contempla el desarrollo de un formato europeo de historia clínica electrónica (*Electronic Health Record Exchange Format, EEHRxF*) que normaliza la presentación de datos básicos del paciente. Por tanto, los sistemas privados deberán adaptarse para generar y exportar dichos documentos (por ejemplo, un resumen de historia clínica) siguiendo ese formato común.

Junto con el derecho de acceso, el paciente tiene el derecho a gestionar el consentimiento y las restricciones sobre sus datos. Esto impone a los sistemas la obligación de implementar funcionalidades específicas para la gestión del consentimiento. Un paciente podrá decidir que los datos sensibles de su historia no sean accesibles o revocar el acceso una vez otorgado. Para habilitar esto, las HCE deben permitir marcar segmentos de la información con distintos niveles de privacidad y respetar esas preferencias en el intercambio. Igualmente, los pacientes tendrán opciones de *opt-out* global en ciertos contextos: el reglamento prevé que puedan excluirse del intercambio transfronterizo de datos asistenciales si así lo desean, lo cual los sistemas nacionales tendrían que contemplar (por ejemplo, un ajuste en el perfil del paciente que, si está activo, evitará que su información se envíe a MyHealth@EU). Estas decisiones deben ser reversibles y auditables.

Para gestionar todo lo anterior, es imprescindible ofrecer una interfaz al ciudadano: los llamados portales de paciente (o *Personal Health Portals*). En algunos países, estos portales serán de ámbito nacional o regional (como el portal de salud del Sistema Nacional de Salud en España) y las entidades privadas se integrarán con ellos; en otros casos, cada proveedor puede ofrecer el suyo. En cualquiera de los modelos, la funcionalidad mínima debe incluir: visualización de la historia clínica (con secciones como medicación, alergias, vacunas, informes, etc.), descarga de documentos en formatos estándar (ya sea PDF o formatos estructurados tipo FHIR), opciones para otorgar o revocar consentimientos de acceso, y un registro de accesos donde el paciente vea quién consultó sus datos y cuándo. Además, en línea con la accesibilidad universal, estos portales han de ser fáciles de usar, seguros y estar disponibles en múltiples idiomas de la UE para no crear brechas digitales.

Un aspecto novedoso es la integración con la identidad digital europea (eID, *electronic identification* por sus siglas en inglés) en el proceso de autenticación del paciente. El uso de los wallets de identidad digital permitirá que el ciudadano acceda a su portal de salud utilizando credenciales unificadas y de alta seguridad (por ejemplo, con autenticación de doble factor respaldada por la infraestructura eIDAS). Asimismo, el monedero digital podría almacenar atributos o credenciales de salud del usuario (por ejemplo, certificados de vacunación, o una prueba de ser profesional sanitario) que faciliten ciertos trámites. Desde la perspectiva funcional, esto significa que los portales y sistemas de salud deben ser capaces de reconocer y aceptar identidades digitales emitidas en cualquier Estado miembro, evitando que el paciente deba crear cuentas separadas en cada país. Esta interoperabilidad de identidad reducirá barreras de acceso: un ciudadano europeo podrá autenticarse en servicios sanitarios en otro Estado con la misma facilidad que en su país de origen.

Desde la perspectiva del ciudadano, la implementación del EEDS supone un avance sin precedentes en el ejercicio de sus derechos digitales en salud. Más allá del acceso básico a sus datos, el paciente tendrá herramientas activas para ver quién ha accedido a su información, con qué fin, y en qué momento.

Este nivel de granularidad en el control exige una interfaz intuitiva, multilingüe y accesible, así como campañas de alfabetización digital para asegurar su uso efectivo. Pero también refuerza la autonomía del paciente, su privacidad y su capacidad de decidir sobre su salud de forma informada. El empoderamiento digital del ciudadano se convierte así en uno de los pilares éticos del EEDS, alineado con la Carta de Derechos Fundamentales de la UE y la visión de una salud digital centrada en la persona.

Historial de accesos y transparencia para el paciente

De la mano con el avance para los pacientes en la gestión del consentimiento y las restricciones sobre sus datos, la transparencia en el uso de los datos es uno de los ejes del EEDS, por lo que funcionalmente los sistemas deben habilitar que el paciente “vea y entienda” cómo se utilizan sus datos en el ecosistema. Para ello, como se mencionó, es obligatoria la disponibilidad de un historial de accesos consultable por el ciudadano. Este historial debe listar las cesiones de datos realizadas a terceros y posiblemente las reutilizaciones en proyectos. Es decir, el ciudadano debe poder saber, por ejemplo que “Dr. X del Hospital Y accedió a su informe de alta el 5/4/2026”) y que “sus datos anonimizados fueron utilizados en el estudio Z el 10/9/2027”. Lograr esto requerirá que todos los accesos queden registrados con metadatos adecuados (fecha, usuario, institución, finalidad) y que esos registros fluyan de vuelta al portal del paciente. Para las entidades privadas, será un reto técnico consolidar en un solo lugar accesos que podrían ocurrir a través de múltiples canales (una consulta directa en la clínica, una descarga vía MyHealth@EU por parte de un médico externo, o una extracción por el organismo de acceso para investigación). Funcionalmente, puede suponer integrar los logs locales con sistemas nacionales de auditoría.

El valor práctico de esta transparencia es empoderar al ciudadano y fomentar la confianza. Un paciente informado sobre quién usa sus datos puede detectar accesos indebidos (y reclamar si algo no concuerda) y sentirse más seguro al compartir información sensible sabiendo que podrá rastrear su uso. Desde el punto de vista de las clínicas y hospitales, deberán ajustar sus políticas y procedimientos internos: cada acceso de un profesional debe obedecer a una razón legítima y quedar documentado. Es posible que internamente deban reforzar la formación al personal sobre esta trazabilidad y las sanciones asociadas a accesos inapropiados. En términos de experiencia de usuario, también habrá que presentar la información de forma comprensible, evitando tecnicismos, y quizás ofrecer notificaciones proactivas (por ejemplo, un aviso al paciente en su móvil cuando alguien accede a su historial desde otro centro).

Soporte para inteligencia artificial y toma de decisiones clínicas

El acceso a grandes volúmenes de datos sanitarios de calidad que promueve el EEDS abre la puerta a nuevas aplicaciones de inteligencia artificial en salud. Aunque el reglamento EEDS en sí se centra en datos, se complementa con otras iniciativas europeas (como la propuesta de Reglamento de IA) que incidirán en cómo las herramientas de IA se integran en entornos clínicos. Por ello, es previsible

que los sistemas de información sanitarios necesiten estar preparados para incorporar algoritmos de soporte a la decisión clínica y otras aplicaciones basadas en IA de forma segura y transparente.

Desde un punto de vista funcional, esto implica que las HCE deben contar con mecanismos de integración de aplicaciones externas (**plug-ins**, APIs estandarizadas) para que módulos de IA puedan acceder a datos clínicos relevantes, procesarlos y devolver sugerencias o predicciones al profesional en tiempo real. Un ejemplo sería un módulo de alerta precoz de sepsis que analice en segundo plano los datos del paciente (signos vitales, resultados de laboratorio) y emita una advertencia en el interfaz del médico si detecta un patrón de riesgo. Para permitir esto, el sistema principal tiene que exponer los datos mediante servicios (idealmente FHIR, que incluso define recursos para decisiones clínicas) y mostrar los resultados de la IA en su flujo de trabajo (por ejemplo, en la pantalla de resultados del paciente).

El EEDS, al armonizar datos y códigos, facilita que las soluciones de IA desarrolladas en un país funcionen en otro, puesto que los datos de entrada estarán estandarizados. Sin embargo, también impone que cualquier uso de IA respete los derechos del paciente y la ética. Es decir, las decisiones asistidas por algoritmos no pueden ser opacas: habrá que proveer explicaciones comprensibles al clínico de cómo se llegó a cierta recomendación (lo que entronca con el futuro Reglamento de IA, que clasificará muchos sistemas de IA en salud como de “alto riesgo” y exigirá trazabilidad y supervisión humana). Funcionalmente, puede ser necesario que los sistemas muestren junto a la sugerencia un resumen de las bases de la IA (por ejemplo, “alerta generada por un algoritmo entrenado con 1 millón de casos, con un 90 % de sensibilidad para detectar sepsis, principales variables: fiebre, taquicardia, leucocitosis”).

Otra aplicación es la medicina personalizada: con grandes bases de datos interoperables, un médico podría, desde su HCE, lanzar consultas poblacionales (*cohort queries*) para encontrar pacientes similares y ver qué tratamientos recibieron, apoyado por IA. Esto difumina la línea entre uso primario y secundario, pero funcionalmente los sistemas podrían ofrecer asistentes inteligentes que, en una consulta, permitan comparar el caso actual con “estadísticas” derivadas de datos anonimizados de la red (por ejemplo, “este tumor raro tiene un 70 % de respuesta a la terapia X según datos europeos”). Para llegar a ese punto, primero se necesita la consolidación de la infraestructura de datos; el EEDS es el habilitador, y las aplicaciones de IA serán la capa de valor añadido que explotará esa base. Los hospitales grandes seguramente lideren la introducción de IA debido a sus recursos (y ya existen iniciativas pilotos en ese sentido), mientras que las clínicas pequeñas podrían beneficiarse consumiendo esas herramientas como servicios en la nube sin tener que desarrollarlas.

Anonimización, seudonimización y reutilización de datos de salud

Pese a no ser el foco de este Trabajo de Fin de Máster, en el ámbito del uso secundario de datos, los sistemas de información deben incorporar funcionalidades para proteger la identidad de las personas cuando sus datos se reutilicen con fines de investigación u otros fines secundarios. El EEDS establece que, por defecto, los datos personales solo se compartan para estos fines en formato seudonimizado (es decir, reemplazando identificadores directos por códigos) o anonimizado si es posible. Por tanto, los proveedores de datos de salud (hospitales, clínicas, laboratorios, etc.) necesitan herramientas para realizar estos procesos de forma fiable conforme al RGPD y a técnicas reconocidas.

En este sentido, también es importante la documentación de la calidad y origen de los datos. El EEDS contempla catálogos nacionales donde los titulares de datos (*data holders*) describan qué conjuntos de datos tienen disponibles. Las entidades privadas deberán cooperar con estos catálogos proporcionando metadatos de sus registros.

Desde el punto de vista del flujo de trabajo clínico, estas exigencias introducen nuevos procesos: por ejemplo, comités de ética o de investigación del hospital evaluando las solicitudes de datos antes de aprobar que el sistema libere la información; personal de TI dedicado a preparar las extracciones; y la necesidad de asegurarse de que la anonimización es suficientemente sólida (por ejemplo, evitar que la combinación de ciertos datos raros vuelva identificable a un paciente, lo que podría requerir intervención manual de expertos en protección de datos). Todo ello añade una capa de trabajo colaborativo

entre departamentos clínicos, jurídicos y técnicos de las instituciones sanitarias.

3.3.4. Requisitos Técnicos

El Espacio Europeo de Datos de Salud (EEDS) establece un marco tecnológico unificado para el intercambio seguro y eficiente de información sanitaria en toda la UE. En el ámbito técnico, el reglamento impone una serie de especificaciones y estándares que deben cumplir los sistemas de historia clínica electrónica (HCE) y otras aplicaciones de salud digital, con el objetivo de garantizar la interoperabilidad semántica y sintáctica, la seguridad de los datos y el respeto a la privacidad en todos los Estados miembros. A continuación, se detallan estos requerimientos técnicos, incluyendo las diferencias en la capacidad de adaptación entre grandes grupos hospitalarios y pequeñas clínicas.

Estándares tecnológicos e interoperabilidad

Un pilar fundamental del EEDS es la adopción de estándares internacionales de datos de salud ampliamente reconocidos. Para lograr una interoperabilidad sintáctica (es decir, compatibilidad en formatos y estructuras de datos), la Comisión Europea ha respaldado el uso de formatos como HL7 CDA (*Clinical Document Architecture*) y, de forma destacada, HL7 FHIR para el intercambio de información clínica estructurada. Estos estándares definen cómo se organizan y transmiten los datos (por ejemplo, un informe médico o el historial farmacoterapéutico), de modo que cualquier sistema compatible pueda interpretarlos correctamente sin importar el proveedor o la tecnología subyacente. Asimismo, se fomenta la utilización de perfiles de interoperabilidad IHE (*Integrating the Healthcare Enterprise*) como XDS/XCA para facilitar el intercambio de documentos clínicos entre diferentes instituciones y países.

En el ámbito de la imagen médica, el EEDS refuerza el empleo de DICOM como formato estándar para almacenar y transferir imágenes diagnósticas (radiografías, TAC, resonancias, etc.) junto con sus informes asociados. DICOM, combinado con perfiles IHE Radiology, permite que, por ejemplo, una resonancia realizada en un hospital de un país pueda ser visualizada y entendida en otro centro europeo sin pérdida de información ni necesidad de conversión manual.

Como ya se ha comentado, lograr la interoperabilidad total no solo implica compartir datos estructurados, sino entender su significado de forma homogénea en distintos contextos lingüísticos y clínicos. Esto requiere interoperabilidad semántica, que el EEDS impulsa mediante la adopción de terminologías y códigos normalizados a nivel europeo. En particular, se promueve el uso de SNOMED CT como ontología de referencia para diagnósticos, procedimientos y hallazgos clínicos. Organismos europeos especializados han recomendado a la Comisión y a los Estados Miembros desplegar progresivamente SNOMED CT como vocabulario clínico común, dada su amplitud y detalle para codificar conceptos médicos. Igualmente, para el intercambio de resultados de laboratorio y otros datos observacionales, se emplea la terminología LOINC, ampliamente utilizada en Europa para estandarizar las pruebas de laboratorio y sus resultados. De hecho, la experiencia en uso de SNOMED CT y LOINC es ya considerable en muchos países europeos, sentando las bases para su adopción extensiva bajo el EEDS.

Gracias a estos estándares semánticos, cuando un profesional acceda a la historia resumida de un paciente procedente de otro país, los diagnósticos estarán codificados en un lenguaje clínico común (p. ej., un código SNOMED CT para "diabetes mellitus tipo 2") y los análisis de laboratorio usarán códigos LOINC universales. Esto evita ambigüedades y asegura que el "significado" de la información médica se conserve más allá de las barreras idiomáticas o de formato. Cabe destacar que el reglamento también prevé la incorporación de otros estándares complementarios según el tipo de datos: por ejemplo, ICD-10/ICD-11 para clasificaciones de enfermedades (utilizados sobre todo con fines estadísticos y de facturación) o IDMP (*Identification of Medicinal Products*) para la identificación armonizada de medicamentos en recetas electrónicas. En conjunto, el cumplimiento de estas especificaciones técnicas garantiza que los datos de salud puedan fluir entre sistemas heterogéneos de distintos países con plena coherencia interpretativa.

Infraestructura y entornos seguros de procesamiento de datos

El EEDS no se limita a definir estándares de datos, sino que exige condiciones de infraestructura que aseguren la conectividad y la seguridad en las transacciones. En primer lugar, cada Estado miembro debe disponer de nodos de conexión a la red MyHealth@EU (para uso primario de datos) y a la futura red HealthData@EU (para uso secundario), con las cuales los sistemas privados deberán interoperar.

Esto implica que hospitales y clínicas tendrán que conectarse, directa o indirectamente, a infraestructuras nacionales de intercambio que enlazan con la red europea. En la práctica, los proveedores de atención sanitaria deberán integrar sus HCE con el Punto Nacional de Contacto eHealth de su país, encargado de gestionar los mensajes transfronterizos (como solicitudes de historial o envío de informes) dentro de MyHealth@EU. Esta conexión exige disponer de APIs y servicios web seguros que empaqueten la información clínica en formatos estándar (ej. un resumen de paciente en formato europeo) y la transmitan cifrada a través de la red común.

Para el uso secundario de datos (investigación, salud pública, política sanitaria), el reglamento prevé la creación de entornos federados de análisis. Cada país establecerá uno o varios Organismos de Acceso a Datos de Salud (*Health Data Access Bodies, HDAB*) que actuarán como intermediarios, ofreciendo plataformas seguras de procesamiento donde los datos de salud (previamente anonimizados o seudonimizados) pueden ser analizados por investigadores autorizados. Desde un punto de vista técnico, estos entornos son auténticas infraestructuras de alto nivel: combinan centros de datos con alta capacidad de cómputo, herramientas de análisis (incluyendo posibilidades de *machine learning* sobre datos federados) y estrictos controles de acceso. Un requerimiento clave es que los datos personales nunca salgan de estos entornos seguros: los análisis se realizan in situ y solo se extraen resultados agregados, evitando así riesgos de filtración. La arquitectura del EEDS permite, por ejemplo, que un investigador en un Estado miembro solicite acceder a datos de pacientes ubicados en otros países; los datos permanecen en sus países de origen pero son consultados de forma remota en un entorno seguro, cumpliendo con todos los estándares de privacidad y seguridad. Esto requiere infraestructura en la nube o centros de datos nacionales interconectados, protocolos de federación de consultas y mecanismos comunes de autenticación y autorización entre los distintos nodos de HealthData@EU.

Otro elemento técnico fundamental es la necesidad de alta disponibilidad y resiliencia de las redes. Dado que la continuidad asistencial podría depender de acceder a datos alojados en otro país en tiempo real, las conexiones y servidores deben garantizar tiempos de respuesta rápidos, redundancia ante fallos y compatibilidad con distintas escalas de volúmenes de datos. Esto se enmarca en las exigencias de la Directiva de seguridad de redes y sistemas de información (Directiva NIS2) citada por el propio reglamento EEDS.

Seguridad, cifrado y trazabilidad de los datos

La protección de la confidencialidad e integridad de los datos de salud es un principio rector del EEDS. En términos técnicos, esto se traduce en requisitos de cifrado robusto, controles de acceso estrictos y trazabilidad completa de las operaciones. El reglamento enfatiza la necesidad de aplicar “los estándares más estrictos en materia de privacidad y ciberseguridad” en todas las plataformas del espacio de datos sanitarios. Por consiguiente, los datos deben viajar cifrados de extremo a extremo en cada intercambio transfronterizo (usando protocolos seguros como TLS para comunicaciones web, VPN cifradas entre nodos, etc.), y también deben almacenarse cifrados en reposo en los repositorios y servidores que formen parte del espacio. La gestión de claves criptográficas y certificados digitales confiables (por ejemplo, certificados X.509 emitidos por autoridades reconocidas a nivel de la UE) será esencial para asegurar que solo los entes autorizados puedan descifrar la información.

La trazabilidad es otro requerimiento crítico: todo acceso, consulta o modificación de datos de salud en el EEDS debe quedar registrado. Esto implica que los sistemas de información mantengan logs de auditoría detallados que incluyan quién accedió a qué datos, en qué fecha y con qué propósito. El paciente, por su parte, tendrá el derecho a consultar el historial de accesos a sus datos de salud electrónicos, como explícitamente recoge el reglamento. Por ejemplo, si distintos profesionales sanitarios

de varios hospitales han consultado la historia clínica de un ciudadano, este debe poder ver esa lista de accesos a través de un portal seguro, añadiendo transparencia al sistema. En la práctica, los HCE y repositorios deberán implementar módulos de auditoría capaces de almacenar millones de eventos de acceso, conservarlos durante los periodos legales estipulados y presentarlos de forma comprensible al usuario final.

Otra dimensión de la trazabilidad es el seguimiento del propósito de uso. Para los usos secundarios, cualquier petición de datos deberá asociarse a un fin autorizado (investigación específica, elaboración de política sanitaria, etc.), y los sistemas deberán etiquetar las sesiones de análisis con esa finalidad. De ese modo, los organismos de acceso a datos pueden monitorizar que no se realicen usos indebidos. Por reglamento, está prohibido utilizar los datos de salud para fines no permitidos, como decisiones que perjudiquen a individuos o mercadotecnia directa, y este cumplimiento debe ser vigilado técnicamente. Los entornos seguros incorporarán restricciones que impidan, por ejemplo, extraer información que identifique a una persona concreta o combinar conjuntos de datos de forma no autorizada, reforzando así las garantías éticas.

En términos de autenticación y control de acceso, los sistemas participantes en el EEDS deberán implementar mecanismos robustos de identificación de usuarios: autenticación multifactor para profesionales sanitarios, certificados electrónicos que acrediten a instituciones, y en general un modelo de gestión de identidades federado. Aquí enlaza el papel de la identificación única: idealmente, cada paciente debería poder ser identificado de forma unívoca a escala europea. El EEDS aprovecha los avances en la Identidad Digital Europea (eID) para autenticar a los ciudadanos cuando acceden o comparten sus datos a través de servicios en línea. La iniciativa del monedero digital europeo (*EU Digital Identity Wallet*) proporcionará a cada persona credenciales electrónicas verificables, facilitando que un paciente se identifique de forma fiable en cualquier país de la UE. Por ejemplo, un paciente español de viaje en Alemania podría usar su identificación digital europea para autenticarse en el hospital alemán y dar acceso a su historial, sin necesidad de trámites adicionales. Desde la perspectiva técnica, esto requiere que los sistemas HCE sean compatibles con los estándares eIDAS de identificación electrónica, permitiendo la integración con servicios de autenticación federada. Además, la identificación única se extiende a profesionales y organizaciones: certificados o IDs únicos a nivel europeo permitirán reconocer a un médico foráneo en los sistemas locales, registrando que “el Dr. X (identificador europeo Y) accedió al registro”, lo que redundará en confianza y trazabilidad.

Certificación de sistemas y cumplimiento normativo

Con el fin de asegurar que todos estos requisitos técnicos se implementen correctamente, el EEDS introduce un marco de certificación obligatoria para los sistemas electrónicos de salud. Los fabricantes y desarrolladores de software de HCE deberán certificar sus productos conforme a criterios europeos de interoperabilidad y seguridad antes de comercializarlos en el mercado de la UE. En la práctica, esto significa que los sistemas de información sanitaria (ya sean grandes suites hospitalarias o aplicaciones de historia clínica para clínicas pequeñas) tendrán que superar evaluaciones de conformidad realizadas por organismos designados, similares a como los productos sanitarios requieren marcaje CE. El reglamento establece un esquema integral de cumplimiento previo y posterior a la comercialización: antes de salir al mercado, el software debe demostrar que cumple con los estándares técnicos comunes y medidas de seguridad; una vez en uso, estará sujeto a vigilancia y posibles auditorías para verificar que mantenga el cumplimiento y actualice sus funcionalidades según evolucione la normativa. Este marco pretende eliminar las brechas de calidad entre sistemas, garantizando que “sean de alta calidad, seguros y plenamente interoperables en todo el mercado de la UE”.

Los criterios exactos de certificación abarcan aspectos como: soporte nativo de los formatos EEHRxF en las categorías de datos prioritarias, integración de terminologías clínicas normalizadas, capacidad de exportar e importar datos en formato estructurado, presencia de funcionalidades de consentimiento y acceso del paciente, mecanismos de seguridad (cifrado, autenticación, registro de accesos) y rendimiento adecuado en entornos de intercambio masivo. De hecho, la propia norma anticipa el desarrollo de actos de ejecución con especificaciones detalladas antes de 2027, que concretarán perfiles técnicos, estándares

específicos y procesos de evaluación de la conformidad. A partir de 2029, comenzarán a ser exigibles funcionalidades concretas para un primer grupo de tipos de datos (resúmenes de paciente, recetas electrónicas, etc.), y hacia 2031 se ampliará a un segundo grupo (imágenes médicas, resultados de laboratorio, informes de alta). Esto marca una hoja de ruta escalonada en la que los proveedores tecnológicos deberán adaptar sus productos progresivamente.

Desde la óptica de las entidades sanitarias, la certificación ofrece una garantía: al adquirir o utilizar un sistema con “etiqueta EEDS”, pueden confiar en que cumplirá con los requisitos mínimos para conectarse al espacio europeo de datos. Además, se espera que surja un registro europeo de soluciones homologadas, que dé visibilidad a qué aplicaciones y HCE están certificados, fomentando la transparencia y competencia en el mercado.

4. AVANCES EUROPEOS EN INTEROPERABILIDAD

A pesar de que el Reglamento EEDS apenas ha entrado en vigor en 2025, muchos países de la UE ya venían preparándose y desarrollando infraestructuras digitales de salud en la última década. Dentro de estos desarrollos, es relevante destacar la red eHealth Network y la plataforma MyHealth@EU.

4.1. *E-Health Network*

El eHealth Network es una red de cooperación voluntaria entre los Estados miembros de la Unión Europea, regulada por la Directiva 2011/24/UE sobre los derechos de los pacientes en la asistencia sanitaria transfronteriza. Está compuesta por las autoridades nacionales responsables de la salud digital en cada Estado miembro de la Unión Europea y por la Comisión Europea, que actúa como secretaria. Su finalidad es servir como foro de coordinación en el ámbito de la salud electrónica, promoviendo el desarrollo de marcos comunes que faciliten la interoperabilidad de los sistemas digitales sanitarios en toda la Unión[27].

El eHealth Network trabaja en el desarrollo de normas y orientaciones que permiten el intercambio electrónico seguro de información sanitaria entre países. Es decir, define los marcos comunes, estándares y directrices para la interoperabilidad de la salud digital entre los Estados miembros de la UE. Esto incluye aspectos técnicos (formatos de datos, protocolos de intercambio) y legales (protección de datos, consentimiento del paciente). De esta manera, contribuye a garantizar que un ciudadano europeo pueda acceder a sus propios datos de salud y utilizarlos en otro Estado miembro, respetando siempre la normativa sobre protección de datos personales.

4.2. MyHealth@EU

MyHealth@EU (antes conocido como *eHealth Digital Service Infrastructure, eHDSI*) es una plataforma e iniciativa piloto que implementa la interoperabilidad transfronteriza de datos de salud siguiendo los estándares acordados por el eHealth Network [28]. Es un ejemplo práctico de cómo los ciudadanos europeos pueden acceder a sus resúmenes de paciente (*Patient Summary*) o recetas electrónicas (*ePrescription*) en otro país miembro.

En otras palabras, MyHealth@EU es la aplicación concreta de las normas y protocolos que el eHealth Network desarrolla. La red define el “qué” y “cómo” de la interoperabilidad, y MyHealth@EU se encarga de materializarlo a nivel técnico y operativo.

Como se ha comentado en los Requisitos Funcionales 3.3.3, bajo el Reglamento del EEDS, la participación en la infraestructura MyHealth@EU será obligatoria para los Estados miembros de la UE en lo relativo al uso primario de los datos de salud para la asistencia sanitaria (es decir, MyHealth@EU pasa de ser voluntario a mandato legal).

Teniendo en cuenta todo lo anterior, podríamos decir que el Reglamento del EEDS regula legalmente el espacio de datos sanitarios europeo, MyHealth@EU es la infraestructura que permite la interoperabilidad y el intercambio transfronterizo, y eHealth Network es el órgano normativo que diseña los estándares, especificaciones y guías para que esos servicios puedan funcionar de modo seguro, eficaz y coordinado.

Dentro de la infraestructura de MyHealth@EU son especialmente relevantes el Resumen de Paciente (*Patient Summary*) y la Receta electrónica (*eReceta*).

4.2.1. Resumen de Paciente. *Patient Summary*

El Patient Summary (o “Resumen del Paciente”) es un documento clínico breve pero esencial, formado por un conjunto estandarizado de datos de salud que pueden incluir alergias, medicamentos actuales, historial de enfermedades, intervenciones quirúrgicas previas, vacunas, etc. Su objetivo es permitir que profesionales sanitarios de otro Estado miembro de la UE puedan atender al paciente

de forma segura, especialmente en casos de urgencia, atención no programada o cuando hay barreras lingüísticas.

Se crea a partir de la información disponible en el historial clínico electrónico del paciente (Electronic Health Record, EHR) y se transmite mediante la infraestructura de MyHealth@EU cuando es necesario, siempre con el consentimiento del paciente. En concreto, el eHealth Network ha adoptado directrices específicas para la definición del conjunto mínimo de datos (dataset) del *Patient Summary*. Estas directrices más recientes se recogen en las *Guidelines on Patient Summary, Release 3.4* (noviembre 2024), donde se especifica que el documento para intercambio debe usar formatos y perfiles acordados (por ejemplo, CDA de HL7) y vocabularios codificados con sistemas de terminología estándares.

El estándar ISO 27269:2021 (Health informatics — International Patient Summary, IPS) se toma como referencia en estas directrices para formalizar el contenido del resumen del paciente en un contexto internacional. Los campos incluidos están definidos como parte de un dataset básico (obligatorio) y un dataset extendido (recomendado cuando sea posible).

Algunos ejemplos de campos que pertenecen al dataset básico incluyen:

- Identificación administrativa del paciente (ID nacional de salud, país).
- Datos demográficos (nombre, fecha de nacimiento, sexo).
- Alergias e intolerancias.
- Medicamentos actuales (incluyendo dosis, frecuencia).
- Historia clínica relevante (antecedentes clínicos/cirugías).
- Inmunizaciones/vacunas.
- Diagnósticos clínicos significativos.

El dataset extendido puede abarcar detalles adicionales, como valores de laboratorio recientes, resultados de pruebas o potencialmente enlaces a documentos clínicos completos.

Para asegurar interoperabilidad semántica, los elementos del resumen del paciente deben codificarse usando sistemas estándar como SNOMED CT, LOINC, ICD-10, entre otros, y deben respetar los catálogos de valores controlados definidos por el eHealth Network.

4.2.2. Receta electrónica. *ePrescriptions*

El término eReceta o *ePrescriptions* (prescripciones electrónicas) refiere al sistema mediante el cual las recetas médicas se emiten y gestionan en formato digital, en lugar de papel. El servicio transfronterizo permite que un ciudadano de la UE pueda obtener medicamentos en una farmacia de otro Estado miembro utilizando una receta electrónica emitida en su país de origen. La eDispensation se refiere al acto de dispensar esos medicamentos en la farmacia del país de destino.

El intercambio electrónico de *ePrescriptions* también requiere estándares comunes (técnicos, semánticos, seguridad, protección de datos), que son definidos por la eHealth Network, y se implementan vía MyHealth@EU. En concreto, en el esquema de MyHealth@EU, el servicio de *ePrescription/eDispensation* opera mediante perfiles CDA HL7, y forma parte de los servicios definidos por la API de NCP (*National Contact Points*). El Business View de MyHealth@EU indica que ePrescription / eDispensation ya están “in operation” usando HL7 CDA.

Se requiere que los datos clínicos de la receta estén codificados con sistemas estándares — por ejemplo, en el ámbito de medicamentos se contempla la adopción gradual de ISO IDMP para una codificación más rigurosa y armonizada entre países. Finalmente, como parte de la interoperabilidad, los valores (por ejemplo, el nombre del medicamento, dosis, forma farmacéutica) deben ajustarse

a catálogos de valores europeos o nacionales para asegurar que los sistemas de destino interpreten correctamente los mismos conceptos.

4.3. Estado Actual de Implementación: España y Comparativa Internacional

A continuación se revisa la situación actual en cuanto a la implementación de los componentes clave del EEDS, tanto en España como en otros países relevantes, para comparar niveles de avance.

4.3.1. Situación en España

España cuenta con un Sistema Nacional de Salud descentralizado en 17 comunidades autónomas, pero con importantes desarrollos para la integración digital. En el ámbito del uso primario de datos, desde 2018 está operativa la Historia Clínica Digital del SNS (HCDSNS) y la Receta Electrónica interoperable, que conectan los sistemas de las distintas comunidades. Gracias a ello, a nivel interno existe conexión entre las historias clínicas autonómicas: un profesional en cualquier Servicio de Salud regional puede consultar un resumen clínico o dispensar una receta emitida en otra región. Además, España participa en la infraestructura MyHealth@EU.

España se encuentra entre los 15 países pioneros que para inicios de 2025 soportan el intercambio de al menos un servicio de salud digital transfronterizo. No obstante, todavía queda camino para la plena implantación: muchos servicios (como intercambio de imágenes, informes de laboratorio, etc.) están en fase piloto y la conexión del sector privado es el gran reto pendiente. España tiene más de 150.000 centros sanitarios privados (clínicas, laboratorios, etc.) cuyos datos no están aún integrados.

España llega por tanto al EEDS bien posicionada en infraestructura pública (interoperabilidad intranacional y conexión a MyHealth@EU) pero con tareas pendientes en integración del sector privado y gobernanza del dato para investigación.

4.3.2. Comparativa internacional

Francia.

Francia es uno de los países que más ha avanzado en la digitalización de la salud, impulsado por una fuerte estrategia estatal. En 2022 lanzó *Mon Espace Santé*, un portal de salud personal para todos los ciudadanos franceses que funciona como historia clínica electrónica unificada. Cada usuario dispone de un espacio seguro donde se almacenan sus informes médicos, resultados, medicamentos, etc., y puede compartirlos con profesionales de su elección. Este sistema –desarrollado con estándares nacionales pero alineado a los europeos– tiene similitudes con la visión del EEDS de dar control al paciente sobre sus datos. Francia también implementó el intercambio transfronterizo: fue de los primeros en activar la eReceta y el Resumen de Paciente con otros países.

Alemania.

Alemania históricamente fue rezagada en digitalización sanitaria, pero en los últimos años ha acelerado el paso con importantes reformas legislativas. En 2021 introdujo la electrónica *Patientenakte* (ePA) –el expediente electrónico del paciente– de uso voluntario. La adopción inicial fue baja, por lo que el gobierno decidió cambiar a un modelo opt-out: a partir de 15 de enero de 2025, todas las personas aseguradas en el sistema público alemán tendrán automáticamente una ePA creada, salvo que rechacen explícitamente. Esto supone un salto cualitativo: se espera que la gran mayoría de 73 millones de asegurados tengan su historial digital activo en 2025, accesible para los profesionales que los atiendan. La ePA alemana permitirá almacenar informes, medicación, resultados y compartirlos entre distintos proveedores, avanzando en la interoperabilidad interna.

En cuanto al intercambio transfronterizo, Alemania trabaja para conectarse a MyHealth@EU; su infraestructura nacional (*gematik*) está adaptando estándares para poder enviar/recibir recetas electrónicas y resúmenes de pacientes con otros países en 2025.

En resumen, Alemania ha pasado de rezagada a tener un plan claro de digitalización acelerada con plazos concretos (opt-out de ePA en 2025, etc.), aunque aún debe afianzar la adopción por parte de profesionales y pacientes, así como la integración con esquemas europeos.

Italia.

Italia desarrolla desde hace años el *Fascicolo Sanitario Elettronico* (FSE), un expediente sanitario electrónico para cada ciudadano. Aunque concebido a nivel nacional en 2015, su implementación efectiva ha dependido de cada región, generando avances desiguales. Algunas regiones (Lombardía, Emilia-Romagna) tienen FSE muy completos y usados, mientras otras están rezagadas. En 2020–2021, impulsada por fondos de recuperación, Italia relanzó el FSE con estándares unificados HL7 FHIR y obligando a las regiones a cargar en él ciertos documentos clínicos (resúmenes de alta, informes, etc.).

Italia también participa en proyectos piloto de MyHealth@EU: por ejemplo, durante 2023 empezó a probar la entrega de ePrescrizioni en farmacias de otros países y el acceso a Sommario Paziente desde el extranjero. Se espera que en 2025 Italia se conecte formalmente a la red europea.

Finlandia.

Finlandia es ampliamente reconocida como pionera en salud digital en Europa, hasta el punto de que su modelo sirvió de inspiración para elementos del EEDS. Desde 2010 opera Kanta, la plataforma nacional de historias clínicas electrónicas y datos de salud finlandesa. Kanta funciona como un repositorio central donde todas las organizaciones sanitarias (públicas y privadas) cargan la información de sus pacientes, de modo que los datos están disponibles de forma unificada para asistencia en cualquier punto del país. Kanta incluye servicios como recetas electrónicas (Finlandia fue la primera en intercambiarlas transfronterizamente en la UE a partir de 2019), resúmenes médicos, imágenes, etc., accesibles también por pacientes a través de un portal ciudadano. En cuanto a interoperabilidad semántica, Finlandia adoptó temprano estándares internacionales (p.ej. SNOMED CT forma parte de sus terminologías desde 2014) y promueve la calidad de datos mediante validaciones automatizadas en los registros nacionales.

No es exagerado afirmar que Finlandia “vive” ya en gran medida el EEDS: sus ciudadanos ejercen los derechos que el EEDS promueve (acceder a sus datos, compartirlos digitalmente), sus profesionales tienen uno de los sistemas más interoperables a disposición, y sus investigadores disponen de un marco legal ejemplar para reutilizar datos protegiendo la privacidad.

Países Bajos.

Los Países Bajos han tomado un camino singular, con fuerte involucramiento del sector privado en la interoperabilidad. Tras un intento fallido en 2011 de implementar un EHR nacional centralizado (vetado por preocupaciones de privacidad), Holanda optó por un enfoque descentralizado basado en estándares abiertos y acuerdos voluntarios. Se creó la iniciativa MedMij, un estándar nacional para intercambio de datos de salud que permite a múltiples proveedores desarrollar portales personales de salud (PGO) interoperables. Cientos de clínicas y aseguradoras adoptan MedMij para que los pacientes puedan reunir sus datos de distintos proveedores en la app o portal de su preferencia. Este modelo de ecosistema competitivo, regulado por estándares, ha logrado cierto éxito: ya existe una decena de aplicaciones certificadas que permiten a pacientes holandeses descargar informes de hospitales, resultados de laboratorio, medicación, etc., en formato estructurado FHIR. En paralelo, para datos secundarios,

En lo legislativo, en 2022 se aprobó la Ley de Intercambio Electrónico de Datos en Salud (Wegiz), que hace obligatoria la interoperabilidad para ciertos tipos de datos clínicos y otorga al Ministerio facultad para imponer estándares. Esta ley nacional encaja con los objetivos del EEDS de “hacer obligatorio el intercambio de categorías prioritarias de datos” para 2029. Los Países Bajos se espera que se unan a MyHealth@EU en 2025, lo que permitirá conectar su red MedMij a la infraestructura europea.

5. EL ECOSISTEMA DE LA SANIDAD PRIVADA EN EL CONTEXTO DEL EEDS

Teniendo presente el objetivo en lo respectivo al EEDS, el capítulo 3 de este proyecto se dedica al mapeo del ecosistema de la sanidad privada en España, un pilar clave del sistema sanitario mixto nacional. Comprender su estructura, nivel de digitalización, desafíos y grado de preparación es esencial para garantizar su integración armónica en el nuevo marco digital europeo. En un entorno en el que el dato se convierte en un activo estratégico, tanto el sector público como el privado deben avanzar en paralelo y con garantías de interoperabilidad y equidad.

La sanidad privada no solo representa una parte significativa del gasto y actividad sanitaria, sino que también es innovadora en muchos procesos asistenciales y organizativos. Sin embargo, la integración en el EEDS implica superar barreras técnicas, jurídicas y organizativas, además de armonizar principios como la gobernanza de los datos, la portabilidad de la información y la protección de los derechos de los pacientes.

5.1. La sanidad privada en España: una visión estructural

La sanidad privada constituye uno de los pilares fundamentales del modelo sanitario mixto español, coexistiendo y complementando al sistema público en la provisión de servicios asistenciales. Su relevancia no es solo cuantitativa, sino también cualitativa: aporta una oferta diversificada, flexible, tecnológicamente avanzada y, en muchos casos, más ágil en su respuesta a las necesidades de los pacientes.

En términos de volumen, la sanidad privada representa aproximadamente el 28 % del gasto sanitario total en España. Este sector está compuesto por más de 431 hospitales (56 % del total del país) y cerca de 12,6 millones de personas están cubiertas por algún tipo de seguro de salud privado (26 % de la población). Además, corresponde a casi 50.000 camas, un 31 % del total nacional y durante el año 2024 supuso más del 40 % de las intervenciones quirúrgicas y el 33 % de las urgencias. La sanidad privada desempeña un papel crucial en la atención hospitalaria, diagnóstica y ambulatoria, y también en la prestación de servicios complementarios, como la salud mental, rehabilitación o atención domiciliaria[29].

Para comprender su complejidad, es necesario analizar tanto los mecanismos de financiación como los diferentes tipos de proveedores que operan en este ámbito:

5.1.1. Modalidades de financiación

- Sanidad asegurada: Usuarios que acceden a servicios mediante pólizas privadas de seguros médicos. Representa alrededor del 24 % del gasto sanitario privado.
- Asistencia directa o pago de bolsillo: Es la modalidad mayoritaria (73 %) y comprende todos aquellos servicios médicos que el usuario paga directamente sin intermediación aseguradora.
- Sanidad concertada: Instituciones privadas que prestan servicios financiados con fondos públicos mediante convenios. Es muy común en comunidades como Cataluña, donde el modelo mixto se ha institucionalizado.
- Mutualismo administrativo: Sistema por el cual los funcionarios públicos pueden elegir entre la sanidad pública y seguros privados concertados (MUFACE, ISFAS, MUGEJU).
- Mutuas colaboradoras con la Seguridad Social: Entidades privadas que gestionan riesgos laborales, prestaciones económicas y asistenciales derivadas de accidentes de trabajo o enfermedades profesionales.

5.1.2. Tipos de prestadores en sanidad privada

- Grupos hospitalarios privados: Redes que gestionan múltiples hospitales, como Quirónsalud, Vithas o HM Hospitales. Tienen gran capacidad de inversión y operan con estándares tecnológicos avanzados.
- Centros monográficos y clínicas especializadas: Ofrecen atención en áreas específicas como fertilidad, dermatología, oncología o cirugía plástica. Suelen ser independientes o formar parte de redes temáticas.
- Profesionales sanitarios independientes: Consultas médicas individuales o de pequeño tamaño, gestionadas directamente por los profesionales. Son altamente representativos en el ámbito urbano y periurbano.
- Agrupaciones profesionales y cooperativas médicas: Modelos de gestión colectiva donde los profesionales comparten infraestructuras y costes, manteniendo autonomía clínica.
- Centros sociosanitarios y de cuidados continuados: Instituciones que cubren servicios de rehabilitación, atención a la cronicidad, cuidados paliativos o atención a personas mayores.
- Entidades religiosas o benéficas: Prestadores históricos del sector sanitario que ofrecen servicios, en muchos casos, sin ánimo de lucro o con una vocación social clara.
- Empresas proveedoras de servicios diagnósticos y de laboratorio: Laboratorios, centros de imagen médica, análisis clínicos o genética, esenciales para la cadena asistencial.

Este mapa de actores demuestra que la sanidad privada en España no es un bloque homogéneo, sino un ecosistema con múltiples capas y niveles de complejidad. Esta heterogeneidad plantea desafíos adicionales para la digitalización e integración con el Espacio Europeo de Datos de Salud, ya que las capacidades tecnológicas, los intereses institucionales y la estructura de gobernanza varían ampliamente entre los diferentes tipos de proveedores.

El reconocimiento de esta diversidad es un paso esencial para diseñar políticas públicas, incentivos regulatorios y estrategias de interoperabilidad que no excluyan a los pequeños operadores ni dependan únicamente de los grandes grupos empresariales. Una integración justa y eficaz del sector privado en el EEDS debe reflejar esta pluralidad, garantizar estándares mínimos de calidad y asegurar que el paciente pueda ejercer sus derechos con independencia del prestador que elija.

5.2. Nivel de digitalización y capacidades actuales

El nivel de digitalización de la sanidad privada en España ha evolucionado significativamente en los últimos años, impulsado tanto por la demanda de servicios más accesibles y personalizados como por la necesidad de adaptarse a un entorno competitivo donde la innovación tecnológica actúa como diferenciador clave. Sin embargo, este progreso no ha sido homogéneo, y persisten grandes disparidades entre distintos tipos de proveedores.

Los grandes grupos hospitalarios, por su dimensión y capacidad inversora, han liderado esta transformación. Disponen de historias clínicas electrónicas (HCE) interoperables dentro de su red, sistemas avanzados de gestión hospitalaria, plataformas de imagen médica (PACS), soluciones de inteligencia artificial aplicadas al diagnóstico, y herramientas de monitorización remota de pacientes. También han incorporado servicios de telemedicina y acceso digital a resultados e informes clínicos a través de portales para pacientes, reforzando el empoderamiento ciudadano y la continuidad asistencial.

Según el Observatorio de Digitalización de la Sanidad Privada (Fundación IDIS, 2025) [30]:

- El 76 % de los hospitales privados ya tiene interoperabilidad entre centros propios o aseguradoras.
- El 86 % ofrece servicios digitales al paciente (citás, resultados, teleconsulta).

- El 100 % de los operadores relevantes ha integrado la telemedicina, especialmente en atención primaria y pediatría.
- El uso de inteligencia artificial y analítica de datos está en expansión, con pilotos en diagnóstico, gestión de recursos y logística hospitalaria.

No obstante, fuera del entorno de los grandes grupos, muchos centros medianos y pequeños, así como profesionales independientes, presentan una situación más dispar. En estos casos, es común encontrar soluciones tecnológicas más limitadas, con historias clínicas parcialmente digitalizadas, escasa integración entre módulos asistenciales y administrativos, y mayores dificultades para cumplir con los requisitos de interoperabilidad con plataformas externas. Las barreras no son solo tecnológicas, sino también económicas y organizativas, ya que el coste de implementar infraestructuras modernas o adaptarse a estándares europeos (como HL7-FHIR o OpenEHR) puede ser prohibitivo sin apoyo institucional o subvenciones específicas.

La madurez digital en el sector privado también se ve reflejada en la capacidad de análisis del dato. Algunos centros han empezado a aplicar big data y machine learning en sus procesos, especialmente en áreas como oncología, imagen médica o medicina personalizada. Sin embargo, la adopción masiva de estas tecnologías sigue siendo incipiente. Además, la gobernanza del dato, la trazabilidad, la anonimización y la protección de la privacidad continúan siendo aspectos críticos a reforzar.

Un reto común a todo el sistema privado es la escasa conexión estructural con el sistema público de salud. A pesar de que algunos centros concertados mantienen ciertos vínculos operativos, la comparación de información entre ambos ámbitos es limitada, lo que obstaculiza la continuidad asistencial, la movilidad del paciente y la eficiencia global del sistema.

Por tanto, el diagnóstico actual del nivel de digitalización en la sanidad privada española puede resumirse en los siguientes puntos clave:

- Alto desarrollo tecnológico en grandes grupos y redes hospitalarias.
- Amplia adopción de herramientas de telemedicina y portales de salud.
- Desconexión operativa con el sistema público y con nodos de datos nacionales/europeos.
- Baja estandarización técnica y necesidad de formación en interoperabilidad y ciberseguridad.

En este contexto, el Espacio Europeo de Datos de Salud representa una gran oportunidad para impulsar la homogeneización y modernización del sector privado. La participación en programas piloto, la incorporación de estándares comunes y la habilitación de nodos interoperables puede permitir que incluso los actores más pequeños accedan a nuevas oportunidades asistenciales, científicas y de colaboración internacional, siempre que se articulen mecanismos de apoyo adecuados.

5.2.1. El nodo de la sanidad privada: avances

La creación de un nodo de datos específico para la sanidad privada es uno de los avances más relevantes en la preparación del sector para su integración en el Espacio Europeo de Datos de Salud (EEDS). Esta iniciativa, liderada por la Fundación IDIS en colaboración con distintas entidades tecnológicas, busca habilitar una infraestructura digital segura, interoperable y centrada en el paciente que permita el acceso, la portabilidad y el uso ético de los datos sanitarios generados en el entorno privado.

El nodo privado se articula en torno a la plataforma Mi Historia Clínica (MiHC), una solución tecnológica que permite a los ciudadanos acceder a sus datos clínicos, almacenarlos, compartirlos con otros profesionales y ejercer control sobre el uso de esa información. Actualmente, más de 400.000 personas utilizan esta herramienta, que se ha concebido desde sus inicios para cumplir con los requisitos regulatorios del EEDS, el Reglamento General de Protección de Datos (RGPD) y las normas de interoperabilidad.

Uno de los aspectos clave del nodo privado es que actúa como interfaz entre múltiples entidades asistenciales que, de otro modo, operarían de forma aislada. La arquitectura modular y abierta de MiHC permite integrar centros con diferentes niveles de digitalización, ofreciendo servicios escalables de acceso, custodia, auditoría, anonimización y gobernanza del dato. Esto resulta fundamental para reducir la brecha tecnológica entre grandes grupos hospitalarios y pequeños centros o consultas independientes.

El nodo también se concibe como un entorno habilitador para el uso secundario de los datos. En este sentido, se están diseñando mecanismos que permitan compartir información anonimizada para fines de investigación clínica, desarrollo de inteligencia artificial, mejora de procesos asistenciales y generación de conocimiento en salud pública. Esta apertura al uso secundario es clave en el marco europeo, donde el EEDS tiene un doble propósito: mejorar la atención a través del uso primario de datos, y promover el aprovechamiento del dato para innovación.

La preparación del nodo para la interoperabilidad con MyHealth@EU es otro de los avances destacados. Esto incluye la adaptación a estándares europeos de exportación e importación de datos (como el *Patient Summary*), la habilitación de consentimientos portables y el establecimiento de mecanismos de certificación compatibles con la arquitectura común europea. Todo ello sitúa al nodo de sanidad privada como una infraestructura pionera en Europa.

Entre los principales logros alcanzados hasta ahora, se destacan:

- Creación de un repositorio federado con control del paciente sobre el acceso a sus datos.
- Desarrollo de servicios de identificación, trazabilidad, seguridad y anonimización.
- Conexión con más de 50 entidades privadas que ya generan datos estructurados e interoperables.
- Puesta en marcha de pilotos clínicos que validan el uso secundario del dato en entornos reales.

Sin embargo, también existen desafíos. La sostenibilidad financiera del nodo, la necesidad de formación de profesionales en gestión del dato, y la generación de confianza entre los ciudadanos son elementos que deben abordarse de manera estructurada. Asimismo, se requiere un marco de gobernanza claro que defina las responsabilidades de cada actor implicado, los criterios de acceso y uso de los datos, y los mecanismos de auditoría y rendición de cuentas.

5.2.2. Receta electrónica privada

De acuerdo al art. 14.4 del RD 1718/2010, “se establecerá por los consejos generales de las organizaciones colegiales corporativas de médicos, odontólogos, podólogos, enfermeros y farmacéuticos en coordinación con las Administraciones sanitarias, el procedimiento de homologación del sistema de receta privada electrónica que posibilite su interoperabilidad, preservando el derecho del paciente a la protección de los datos de su historia clínica” [32], los Consejos Generales de Dentistas, Farmacéuticos, Médicos y Podólogos en coordinación con las Administraciones sanitarias, han desarrollado el sistema de receta electrónica privada (SREP).

El SREP es un instrumento que permite interoperar a todos los agentes que actúan en el ciclo de prescripción – dispensación de los medicamentos en el ámbito de la asistencia sanitaria privada; es decir, que permite a los profesionales de la salud del ámbito privado (médicos, dentistas y podólogos) prescribir medicamentos y productos sanitarios mediante recetas emitidas en soporte electrónico desde cualquier sistema de prescripción homologado, para que pueda ser dispensado por cualquier farmacéutico habilitado en cualquier oficina de farmacia de España [33],

El SREP organiza agentes y plataformas interoperables garantizando que las recetas electrónicas sean emitidas por profesionales autorizados por medio de cualquiera de los sistemas de prescripción homologados, siendo almacenadas y gestionadas en repositorios homologados. Desde allí, las recetas pueden ser dispensadas en cualquier farmacia del territorio nacional -desde sus softwares de gestión,

también homologados- cuando sean presentadas en las condiciones legalmente establecidas, asegurando el acceso universal, la confidencialidad de los datos del paciente y la seguridad del tratamiento.

En ese sentido, sólo las recetas electrónicas privadas emitidas de acuerdo con este sistema cumplen con los requisitos legales establecidos en la normativa vigente; estando diseñado dicho sistema para que las recetas electrónicas homologadas en el SREP garanticen la trazabilidad, la privacidad y la seguridad tanto para los pacientes como para los profesionales sanitarios.

Es difícil identificar el volumen de prestadores de salud privada que están haciendo uso de estos sistemas de prescripción. Si atendemos a las empresas certificadas, vemos que los grandes grupos hospitalarios como HM Hospitales, Quirón Salud y Sanitas han certificado sus propios sistemas de eReceta, pero también observamos la homologación de plataformas que permiten la subscripción de servicios a sus sistemas para todo tipo de prestadores sanitarios con diferentes planes de suscripción, como REMPE, DOCLINE o REDSYS y diferentes niveles de integración con los subscriptores. La Figura 3 muestra la relación de Empresas certificadas [31].

EMPRESA	CERTIFICACIÓN	RENOVACIÓN
CLÍNICA UNIVERSIDAD NAVARRA	2023	2025
DELONIA SOFTWARE S.L	2022	2024
DOCLINE	2021	2025
DPS (REMPE)	2020	2025
HM HOSPITALES	2021	2025
MEDIGEST	2021	2025
QUIRON SALUD	2021	2025
REDSYS	2021	2025
SANITAS	2021	2025
FREMAP	2025	NA

Figura 3: Relación de Empresas certificadas SERP

MEDIGEST ha homologado un modulo de eReceta que pone a disposición dentro de su software de gestión médica, AXON local o AXON Cloud.

Según datos de 2022, en dos años de funcionamiento de la eReceta Privada se dió cobertura a 9,2 millones de pacientes y se la facilitó la dispensación electrónica de más de un millón de medicamentos [34]. Si citamos las webs de algunas de las empresas homologadas, por ejemplo Docline, anuncia realizar más de 9.500 recetas mensuales desde su sistema [35].

Esta prescripción y dispensación de receta electrónica es una de las categorías prioritarias identificada en el reglamento para uso primario y determinada su aplicación para el 26/03/2029.

5.2.3. Desafíos clave identificados

La integración de la sanidad privada en el Espacio Europeo de Datos de Salud (EEDS) no está exenta de retos. Aunque existen avances significativos en digitalización e interoperabilidad, el sector se enfrenta a una serie de obstáculos estructurales, tecnológicos, económicos y regulatorios que deben abordarse de manera coordinada. Identificar estos desafíos es el primer paso para establecer estrategias que faciliten una participación plena y efectiva del sector privado en el ecosistema digital europeo.

Uno de los principales retos es la fragmentación de los sistemas de información. Aunque los grandes grupos hospitalarios suelen contar con infraestructuras tecnológicas avanzadas y homogéneas, muchos centros de menor tamaño emplean sistemas dispares que no permiten una comunicación fluida ni el intercambio estructurado de información. Esta heterogeneidad tecnológica dificulta la interoperabilidad interna y externa, y representa una barrera para la integración con plataformas nacionales y europeas.

A ello se suma la falta de un identificador único de paciente a nivel estatal. Actualmente, no existe un sistema unificado que permita vincular de manera segura y precisa los datos de un mismo individuo cuando accede a servicios en diferentes centros del sistema privado, o entre el ámbito privado y público. Esta ausencia compromete la trazabilidad de la información, la calidad del dato y, en consecuencia, la continuidad asistencial.

Otro obstáculo relevante es la desigualdad en capacidades técnicas y económicas entre los distintos actores del sector privado. Mientras algunos operadores disponen de recursos suficientes para acometer las inversiones necesarias en infraestructuras digitales, otros —especialmente clínicas pequeñas, consultas independientes o centros en áreas rurales— tienen mayores dificultades para acceder a las soluciones tecnológicas exigidas por el EEDS. Esta brecha digital amenaza con dejar fuera a parte del sistema privado de salud.

La falta de estándares técnicos comunes también se presenta como un desafío crítico. Aunque existen recomendaciones claras a nivel europeo (como el uso de HL7 FHIR o perfiles IHE para la interoperabilidad), su adopción en el sector privado no ha sido homogénea. Esta falta de estandarización limita la posibilidad de compartir datos de forma segura y eficiente, lo que se traduce en ineficiencias y en una menor calidad del servicio al paciente. Desde el punto de vista normativo, persisten incertidumbres regulatorias sobre cómo se aplicará de forma concreta el Reglamento del EEDS en el ámbito privado, qué requisitos técnicos y legales deberán cumplir los nodos privados, y qué mecanismos se establecerán para asegurar la equidad y el acceso universal al dato sanitario.

A nivel organizativo, uno de los retos más señalados es la ausencia de una gobernanza compartida del dato. Mientras que en el sistema público se están articulando oficinas del dato y autoridades de acceso, el sector privado carece aún de estructuras institucionalizadas que asuman estas funciones de manera reconocida y coordinada. Esto obstaculiza la definición de reglas comunes de acceso, anonimización, auditoría o uso secundario de la información clínica.

Otro aspecto crítico es la confianza de los pacientes. La cesión de datos sanitarios, incluso de forma anonimizada, sigue generando dudas en buena parte de la ciudadanía. Esta desconfianza puede incrementarse cuando se trata de entidades privadas, especialmente si no existe una comunicación clara, garantías sólidas de protección de la privacidad y mecanismos efectivos de control por parte del usuario.

Por último, cabe señalar la necesidad urgente de capacitación del capital humano. Muchos profesionales del sector no están formados en competencias digitales, protección de datos ni uso de herramientas interoperables. La falta de estos conocimientos puede ralentizar la adopción de nuevas tecnologías y limitar el aprovechamiento del potencial del EEDS.

En conjunto, los desafíos identificados se resumen en:

- Fragmentación tecnológica y heterogeneidad de sistemas.
- Falta de un identificador único de paciente.
- Brecha digital entre grandes y pequeños operadores.
- Ausencia de estándares técnicos homogéneos.
- Incertidumbres regulatorias.
- Carencia de estructuras de gobernanza del dato en el ámbito privado.
- Desconfianza social en el uso del dato sanitario.
- Necesidad de formación profesional en competencias digitales.

Superar estos retos requiere una estrategia integral que combine incentivos económicos, acompañamiento técnico, cooperación público-privada, regulación clara y participación activa de todos los actores implicados. Solo así podrá garantizarse que el sector privado no quede rezagado, sino que

contribuya de forma efectiva y responsable al desarrollo de un espacio europeo de datos de salud centrado en el ciudadano.

5.2.4. Gobernanza del dato sanitario en el ámbito privado

La gobernanza del dato sanitario es uno de los pilares sobre los que se construye el Espacio Europeo de Datos de Salud (EEDS). Este concepto implica mucho más que la gestión técnica de la información: abarca aspectos éticos, jurídicos, organizativos y tecnológicos que definen cómo se recogen, almacenan, usan, comparten y protegen los datos clínicos. En el ámbito privado, la necesidad de una gobernanza sólida y transparente se vuelve aún más crucial, ya que debe garantizar la confianza del paciente, la calidad del dato y la alineación con las políticas europeas.

En el sector privado español, la gobernanza del dato ha evolucionado de forma desigual. Mientras que algunos grandes grupos sanitarios han desarrollado políticas internas avanzadas, estructuras de seguridad de la información y mecanismos de auditoría, en muchas pequeñas entidades todavía predomina un enfoque operativo y fragmentado. Esta disparidad genera una brecha no solo tecnológica, sino también normativa y organizativa, que complica la integración de todos los actores en un ecosistema de datos compartidos. Uno de los elementos centrales de la gobernanza es la definición de roles y responsabilidades. El Reglamento General de Protección de Datos (RGPD) establece con claridad las figuras del responsable y el encargado del tratamiento, así como los derechos del interesado. Sin embargo, en muchos centros privados, especialmente en consultas individuales, estas funciones no están adecuadamente estructuradas ni diferenciadas, lo que incrementa los riesgos de incumplimiento y vulnerabilidad ante ciberataques.

Asimismo, la trazabilidad del dato y la gestión de consentimientos son aspectos clave. En un entorno interoperable como el EEDS, donde los datos pueden circular entre diferentes jurisdicciones y usos, es imprescindible garantizar que el paciente sepa en todo momento quién accede a su información, con qué fin y durante cuánto tiempo. Esto requiere herramientas tecnológicas robustas —como registros de acceso, plataformas de consentimiento dinámico y sistemas de auditoría— y una cultura organizativa que priorice la protección de derechos.

Otro componente crítico es la anonimización y pseudonimización de los datos cuando se destinan a usos secundarios (investigación, innovación, política sanitaria). Aunque el sector privado genera gran cantidad de datos valiosos, su uso ético y seguro requiere metodologías estandarizadas, herramientas de transformación del dato y normas claras sobre su acceso por terceros.

En cuanto a las estructuras de gobernanza compartida, el sector privado aún no dispone de mecanismos institucionales que agrupen a los distintos actores en órganos comunes de decisión o supervisión del dato sanitario. A diferencia del sistema público, que está desarrollando Oficinas del Dato, el ámbito privado necesita avanzar hacia modelos de gobernanza colaborativa que aseguren la transparencia, la equidad en el acceso y la coherencia con las políticas nacionales y europeas.

Existen, sin embargo, iniciativas prometedoras. La Fundación IDIS ha impulsado la creación de un nodo privado federado con control ciudadano sobre sus datos. Esta plataforma incorpora principios de gobernanza del dato como la autonomía del paciente, la interoperabilidad técnica, la custodia responsable de la información y la trazabilidad del acceso. Aunque aún en fase de desarrollo, constituye un modelo referencial para avanzar en esta materia.

Por tanto, los desafíos en gobernanza del dato en el ámbito privado pueden resumirse en:

- Necesidad de profesionalizar la gestión del dato clínico en todas las organizaciones.
- Establecimiento de estructuras formales de responsabilidad, auditoría y control.
- Adopción de herramientas tecnológicas que garanticen el consentimiento, la trazabilidad y la privacidad.
- Construcción de una gobernanza compartida entre actores del ecosistema privado.

- Armonización con las directrices del EEDS y del marco normativo europeo.

El desarrollo de una gobernanza eficaz no solo es una obligación regulatoria, sino una condición imprescindible para generar confianza social, atraer inversión en innovación y consolidar un modelo de sanidad privada alineado con los valores del espacio digital europeo centrado en la persona.

5.2.5. Casos de uso y ejemplos de integración digital en sanidad privada

Entre los casos de uso más relevantes del EEDS para pequeños proveedores de salud destacan aquellos orientados a facilitar su integración tecnológica en el ecosistema europeo mediante soluciones escalables y accesibles. En particular, el modelo SaaS (Software as a Service) se perfila como una vía prioritaria para clínicas independientes, centros rurales y pequeños proveedores ambulatorios que no disponen de recursos para desarrollar infraestructuras propias. Estas soluciones permiten conectarse al nodo nacional de interoperabilidad, garantizar el cumplimiento normativo europeo (por ejemplo, estándares FHIR y SNOMED CT), y participar en el uso secundario de datos (investigación, políticas públicas) sin asumir cargas técnicas internas.

Casos concretos pueden incluir:

- Un centro médico rural que accede a la historia clínica electrónica de un paciente atendido previamente en otro Estado miembro.
- Una clínica privada que ofrece al paciente una app interoperable donde este puede gestionar sus consentimientos y revisar el historial de accesos.
- Un proveedor de radiología que comparte imágenes médicas a través de un nodo interoperable con hospitales europeos que tratan al paciente.
- La participación de pequeños centros en estudios multicéntricos de investigación mediante entornos seguros federados provistos por plataformas SaaS.

Estos escenarios potencian la equidad en el acceso a la innovación digital y la interoperabilidad para actores del sistema que tradicionalmente han quedado fuera de los grandes despliegues tecnológicos.

La integración digital de la sanidad privada en el Espacio Europeo de Datos de Salud (EEDS) no es solo una aspiración teórica. Ya existen casos reales que demuestran el potencial del sector para participar activamente en este nuevo ecosistema. Estas experiencias permiten identificar buenas prácticas, lecciones aprendidas y elementos replicables que pueden servir de guía para otras entidades en su proceso de transformación.

Uno de los ejemplos más significativos en España es la plataforma Mi Historia Clínica, impulsada por la Fundación IDIS. Se trata de un nodo digital de salud que permite a los pacientes acceder a su información clínica de forma centralizada, segura e interoperable, independientemente del proveedor sanitario que haya generado el dato. Esta herramienta fue diseñada para cumplir con los estándares europeos en portabilidad de datos, trazabilidad de accesos y protección de la privacidad del paciente.

Actualmente, Mi Historia Clínica conecta a más de cincuenta entidades privadas, incluyendo grandes grupos hospitalarios, clínicas especializadas y centros ambulatorios. Su diseño modular facilita que tanto organizaciones con alta capacidad tecnológica como otras más pequeñas puedan incorporarse de forma progresiva. Este modelo demuestra que es posible construir una red federada de datos sanitarios bajo gobernanza privada, centrada en el ciudadano y alineada con los principios del EEDS.

También es destacable el despliegue de servicios de telemedicina por parte de aseguradoras y grupos hospitalarios privados. Durante la pandemia de COVID-19, muchas entidades desarrollaron plataformas para consultas virtuales, emisión de recetas electrónicas y seguimiento remoto de pacientes. Estas herramientas, integradas con los sistemas de historia clínica digital, se han consolidado como una opción habitual de atención sanitaria no presencial.

En lo que respecta a la digitalización de procesos clínicos y administrativos, algunos hospitales privados han alcanzado una interoperabilidad total entre sus servicios. Esto abarca desde la solicitud electrónica de pruebas diagnósticas hasta la gestión farmacológica y la elaboración de informes clínicos estructurados, todo ello compatible con los estándares europeos como HL7 FHIR.

En el ámbito de la inteligencia artificial, varias entidades están explorando proyectos que utilizan algoritmos para la detección precoz de enfermedades, análisis de imágenes médicas o predicción de eventos clínicos adversos. Aunque muchos de estos proyectos se encuentran aún en fase piloto, su evolución apunta a un uso más intensivo y ético del dato en beneficio del paciente y de la eficiencia del sistema.

Además, algunas comunidades autónomas han puesto en marcha iniciativas que permiten a determinados centros privados compartir información relevante con los sistemas públicos de salud mediante protocolos específicos. Estas primeras integraciones representan un paso hacia una mayor colaboración estructurada entre ambos sectores.

En el campo de la investigación y la salud poblacional, algunas entidades privadas ya participan en proyectos de análisis de grandes volúmenes de datos anonimizados. Estos datos se utilizan para mejorar la planificación sanitaria, detectar patrones epidemiológicos y evaluar el impacto de tratamientos médicos en la población.

Todos estos ejemplos confirman que el sector privado no solo está preparado para integrarse en el EEDS, sino que ya ha comenzado a construir los elementos clave para lograrlo. La clave ahora está en extender estas prácticas, asegurar su interoperabilidad y consolidar una cultura organizativa centrada en el valor del dato clínico.

Para garantizar que estas iniciativas se consoliden y multipliquen, será fundamental contar con marcos normativos adecuados, acceso a financiación, confianza por parte de los pacientes y una voluntad real de colaboración entre todos los actores implicados. La transformación digital de la sanidad privada es una realidad en marcha que puede aportar valor estratégico al conjunto del sistema sanitario europeo.

El uso de inteligencia artificial en el entorno del EEDS introduce nuevos riesgos éticos y clínicos que deben ser abordados desde el diseño del sistema. Uno de los más relevantes es la posibilidad de que los algoritmos perpetúen o amplifiquen sesgos estructurales presentes en los datos de origen: desigualdades por género, raza, territorio o nivel socioeconómico pueden ser reproducidas en sistemas de apoyo a la decisión clínica sin una supervisión adecuada.

Además, la automatización excesiva de procesos clínicos puede derivar en una medicalización algorítmica, en la que las decisiones sanitarias se tomen sin suficiente juicio humano ni contexto individual. Esto pone en riesgo la calidad asistencial y el principio de autonomía del paciente.

Para evitar estos escenarios, el despliegue de IA en el marco del EEDS debe ir acompañado de:

- Supervisión humana significativa en todo el ciclo de uso de algoritmos clínicos.
- Auditorías éticas y técnicas para detectar y corregir sesgos.
- Transparencia en los criterios de decisión algorítmica.
- Evaluación independiente del impacto de la IA sobre los resultados en salud y la equidad.

Solo así se puede garantizar que la inteligencia artificial actúe como un instrumento de mejora, y no como una fuente adicional de exclusión o error clínico.

5.2.6. Financiación e incentivos para la transformación digital

La transformación digital del sistema sanitario en España requiere inversiones constantes y planificadas. En el sector privado, esta evolución depende en gran medida de recursos propios, ya que las

entidades no reciben financiación pública estructurada como sucede con el sistema sanitario público. Esto hace especialmente necesario establecer mecanismos específicos de financiación e incentivos que permitan su integración plena en el Espacio Europeo de Datos de Salud (EEDS).

Uno de los principales obstáculos que enfrenta la sanidad privada es el acceso limitado a los fondos europeos destinados a la digitalización del sistema de salud. A pesar de que iniciativas como el Plan de Recuperación, Transformación y Resiliencia (PRTR) contemplan recursos para la modernización tecnológica del sector, en la práctica estos fondos se han destinado casi exclusivamente al ámbito público. Esta exclusión genera un riesgo real de que muchas entidades privadas, especialmente las de menor tamaño o ubicadas en entornos rurales, queden fuera de esta ola de transformación.

Ante esta situación, se hace imprescindible desarrollar líneas de financiación público-privada que faciliten el acceso de los operadores privados a recursos para la digitalización, interoperabilidad, seguridad de la información e integración en los nodos de datos nacionales y europeos. Estas líneas pueden articularse mediante convocatorias específicas, incentivos fiscales, préstamos blandos o fórmulas de colaboración entre sectores.

Además, deben diseñarse incentivos regulatorios que reconozcan y premien a las entidades que implementen buenas prácticas en el tratamiento del dato, la interoperabilidad y la participación activa en el EEDS. Por ejemplo, podría establecerse un sistema europeo de certificación que acredite el cumplimiento de los estándares técnicos, organizativos y de seguridad, otorgando ventajas competitivas a los centros acreditados.

El uso secundario del dato sanitario también ofrece oportunidades significativas. La participación de entidades privadas en iniciativas de investigación, análisis de resultados o desarrollo de soluciones tecnológicas puede incentivarse mediante modelos de retorno justos y transparentes. Esto implica establecer mecanismos de compensación adecuados que respeten la privacidad del paciente y promuevan el uso responsable del dato con fines científicos y de innovación.

Asimismo, la Fundación IDIS ha destacado la necesidad de reconocer el dato sanitario como un activo estratégico. Esto requiere un enfoque regulatorio que no solo proteja la información, sino que habilite su uso ético, controlado y eficiente en beneficio del conjunto del sistema sanitario y de los propios ciudadanos. La política pública debe combinar control con estímulo para aprovechar plenamente el potencial transformador del dato.

Finalmente, asegurar la sostenibilidad económica de las plataformas digitales privadas, como los nodos de datos federados impulsados por el propio sector, exige planificación. No es viable que su mantenimiento dependa únicamente de las aportaciones de los centros participantes. Será necesario articular modelos financieros que integren apoyo institucional, fondos europeos y alianzas estratégicas para garantizar su continuidad operativa.

En resumen, los elementos clave para una financiación efectiva de la transformación digital en la sanidad privada son: el acceso equitativo a fondos nacionales y europeos; la existencia de incentivos fiscales y regulatorios; la creación de modelos de compensación por uso secundario del dato; el reconocimiento del dato como activo estratégico; y la planificación de estructuras económicas sostenibles para las infraestructuras digitales comunes.

Sin estas condiciones, existe el riesgo de una transformación desigual, en la que parte del ecosistema sanitario privado quede rezagado, comprometiendo la cohesión, la eficiencia y la interoperabilidad del sistema de salud en su conjunto dentro del EEDS.

5.2.7. Diferencias capacidad de cumplimiento técnico

Como se ha comentado desde un inicio, la implantación de los requerimientos técnicos no afecta por igual a todas las entidades. Grandes grupos hospitalarios suelen disponer de departamentos de TI robustos, mayor presupuesto y sistemas de información más avanzados, lo que les posiciona mejor para acometer las adaptaciones necesarias. Muchas de estas instituciones ya utilizan estándares como

HL7 o DICOM en sus entornos internos, y es posible que participen en proyectos piloto o pruebas de concepto a nivel nacional/europeo. Por tanto, es previsible que lideren la adopción temprana del EEDS, integrándose con los nodos nacionales e incorporando las actualizaciones de software certificadas. No obstante, también enfrentan desafíos: al tener volúmenes de datos masivos y sistemas legados complejos, la interoperabilidad plena puede requerir migraciones de datos, actualizaciones costosas de infraestructura y reforzar la ciberseguridad en cada punto de acceso. La gestión del cambio a esta escala implicará planificar cuidadosamente las transiciones para no interrumpir la atención sanitaria.

En contraste, las pequeñas clínicas y consultorios (por ejemplo, una clínica independiente con unos pocos facultativos o un centro de especialidades ambulatorias) pueden tener más dificultades para cumplir con todos los requisitos técnicos. A menudo utilizan soluciones informáticas sencillas o software de gestión clínica proporcionado por terceros, sin equipos dedicados de informática médica. La exigencia de conectarse al nodo interoperable nacional, utilizar formatos estándar o habilitar portales de paciente puede sobrepasar sus capacidades iniciales. Conscientes de ello, los legisladores han introducido cierta flexibilidad para microentidades: las organizaciones sanitarias muy pequeñas (menos de 10 empleados y menos de 2 millones de euros de facturación anual) podrían quedar temporalmente exentas de algunas obligaciones de cumplimiento del EEDS, si bien los Estados miembros tienen la potestad de revocar esa exención en su territorio. Este margen busca no asfixiar a los micro-proveedores, aunque a medio plazo se espera que todos los actores se integren en la red.

En la Figura 4 se detalla la diferenciación en cuanto a nivel de madurez de los distintos centros privados.

Aspecto	Grandes hospitales y corporaciones	Pequeñas clínicas y consultorios
Infraestructura TI	Sistemas avanzados y centralizados (HCE integradas, nubes privadas), listos para interoperabilidad.	Sistemas básicos o heterogéneos (software de gestión simple, registros locales), con menor grado de digitalización.
Personal	Equipos dedicados de TI, datos y seguridad; personal habituado a herramientas digitales complejas.	Escaso o nulo personal técnico; profesionales sanitarios deben autogestionar tecnología, a menudo con brecha de formación.
Capacidad financiera	Presupuestos elevados para inversión en TIC; pueden desplegar soluciones a gran escala con costes asumibles.	Recursos limitados; la inversión en nuevas plataformas supone un gran esfuerzo relativo y coste hundido sin retorno inmediato.
Experiencia en datos	Participación en proyectos previos de interoperabilidad; cultura del dato más asentada.	Poca experiencia en intercambio de datos más allá del entorno inmediato; enfoque tradicional en procesos en papel o sistemas aislados.
Soporte externo	Menor dependencia; pueden desarrollar soluciones a medida o colaborar con grandes proveedores tecnológicos.	Alta dependencia de proveedores externos de software; requerirán soluciones llave en mano o apoyo de asociaciones sectoriales.

Figura 4: Tabla comparativa: Grandes hospitales vs. pequeñas clínicas

Estas diferencias se traducen en una brecha técnica estructural que debe abordarse con medidas de política pública y diseño tecnológico.

Uno de los enfoques más prometedores es el uso de soluciones SaaS o plataformas cloud preconfiguradas y certificadas. Esto permitiría que clínicas con pocos recursos “se enchufen” a servicios ya interoperables sin necesidad de desarrollar sistemas propios. Por ejemplo, un centro rural podría contratar un software clínico en la nube homologado para EEDS, que incluya módulos de consentimiento, trazabilidad, y conexión directa al nodo nacional.

6. PROPUESTA DE SOLUCIÓN PARA LA IMPLEMENTACIÓN DEL EEDS EN LA SANIDAD PRIVADA

6.1. Solución propuesta: SaaS

La implementación efectiva del Espacio Europeo de Datos de Salud (EEDS) exige no solo el cumplimiento normativo y técnico, sino también soluciones prácticas adaptadas a la realidad diversa de los centros sanitarios. Las propuestas para hacer operativa la implementación del EEDS, tanto en grandes hospitales como en otros centros más pequeños, deben tener en cuenta las diferentes capacidades, barreras y oportunidades de cada tipo de centro.

6.1.1. Arquitectura Tecnológica Propuesta

Como vimos anteriormente el EEDS establece una serie de requerimientos técnicos a cumplir por todos los prestadores de servicios:

- Interoperar con la Plataforma centralizada de interoperabilidad para la salud digital MyHealth@UE, con altos niveles de seguridad y rendimiento (art. 23). Los prestadores sanitarios privados deberán compartir su información clínica a través del nodo nacional, garantizando la seguridad, la conectividad y el rendimiento en las transacciones, máxime cuando la continuidad asistencial puede depender de los datos a compartir.
- Garantizar la interoperabilidad sintáctica y semántica La información compartida tiene que ser perfectamente interpretable por el receptor y de forma automática, esto implica compartir la información en un formato concreto, interoperabilidad sintáctica y utilizando estándares internacionales de terminología que permitan entender el significado de lo compartido de forma homogénea, interoperabilidad semántica. (art.15)
- Obligación para los sistemas de HCE de incorporar los componentes armonizados de programa informático de HCE, el de interoperabilidad y el de registro (art. 25) y certificarlos para su uso.

En España el Ministerio de Sanidad es usuario de esta infraestructura proporcionando el nodo nacional de conexión para compartir los datos de Historia Clínica y Receta Electrónica cumpliendo la directiva 2011/24/UE referente a derechos de los pacientes en la asistencia transfronteriza. Las CCAA disponen cada una de un nodo autonómico que se conecta al nodo del ministerio para compartir la información sanitaria entre comunidades, proyecto HCDSNS y con europa.

Entre los prestadores de asistencia privados la fundación IDIS, promovió un proyecto de HCE de la sanidad privada, poniendo a disposición de sus “socios” una plataforma a través de la que compartir información sanitaria (5.2.1 Mi Historia Clínica).

A partir del 26/03/2029 todos los prestadores de salud privados deberán poder compartir los datos de salud referentes a la HC Resumida y la receta y la dispensación electrónica utilizando la infraestructura comunitaria.

Proponemos crear plataformas intermedias que actúen como componentes armonizados de HCE tal y como define el reglamento y que puedan ponerse a disposición de los fabricantes de sistemas HCE en modelo As a Service.

Estas plataformas se encargarán de conectar con el o los nodos que disponga el ministerio de sanidad para el intercambio de información sanitaria, tanto a nivel nacional como con europa o podrían ser nodos de conexión autorizados por el ministerio para la conexión de los prestadores sanitarios privados.

La plataforma debe contemplar dos tipos de conexiones, las de los sistemas de HCE de los prestadores a los que da servicio y las que provengan de otros prestadores de atención sanitaria, nacionales privados o públicos y supranacionales, privados o públicos. Por sencillez hacemos la suposición de que a nivel

nacional todas las conexiones se realizarán a través del nodo del ministerio, pero podría plantearse autorizar estos sistemas por CCAA.

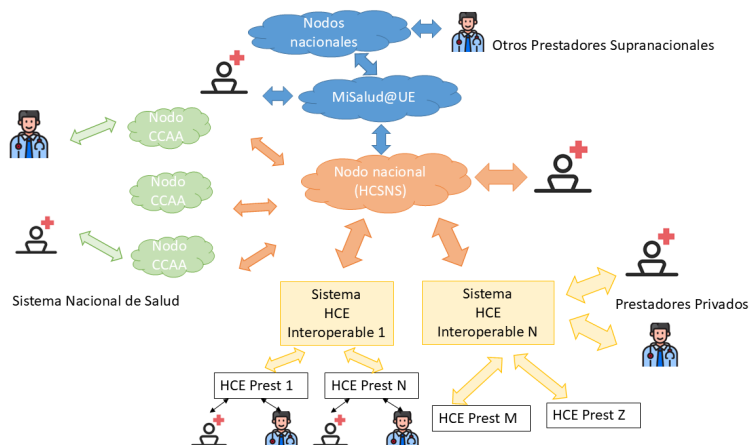


Figura 5: Esquema de comunicación de los sistemas de Historia Clínica Electrónica Interoperables

Estas plataformas pueden definirse como meros transportadores de la información de un lado a otro, como transportadores y “traductores” de la información o incluso persistir la información de los prestadores para la interoperabilidad si estos así lo desean. Este planteamiento permitiría reducir el número de conexiones con los nodos de interoperabilidad ya existentes, reduciendo la variabilidad y permitiendo mantener las exigencias a nivel de seguridad y rendimiento. También obliga a los prestadores sanitarios privados a suscribir servicios con un intermediario, pero les permite disponer de economías de escala, ya que como hemos analizado previamente los prestadores de pequeño tamaño podrían encontrarse con la imposibilidad de asumir los costes de las infraestructuras necesarias para garantizar los requerimientos técnicos del EEDS.

La arquitectura tecnológica de la plataforma (Figura 6) seguirá un modelo en capas, con alta disponibilidad y la posibilidad de interconexión con la infraestructura del nodo nacional cumpliendo todos los requisitos de seguridad y rendimiento.

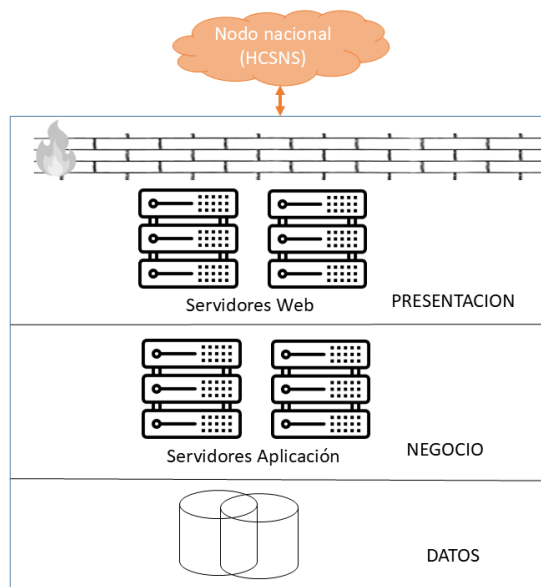


Figura 6: Arquitectura tecnológica de la propuesta

La solución propuesta tiene que dar respuesta a los requisitos funcionales que plantea el reglamento y proponemos hacerlo de forma modular:

- Identificación segura de usuarios: pacientes y profesionales. Cuando el usuario sea el peticionario de información, la plataforma debe garantizar su identificación correcta y en el caso de profesionales que el acceso a la información solicitada es justificada y pertinente.
- Trazabilidad de accesos. La plataforma se encargará de almacenar y proporcionar como servicio los datos de acceso a la información clínica en el formato que se detalle en las actuaciones de la comisión.
- Derecho de autoexclusión. La plataforma permitirá la gestión de la autoexclusión del paciente, permitiendo que pueda activarla o desactivarla en cualquier momento.
- Acceso a datos de paciente. La plataforma ofrecerá la posibilidad de un portal para el paciente o el consumo de servicios a través de una API que permita integrar los datos en portales corporativos (B2B).
- Acceso a datos por profesionales. La plataforma ofrecerá la posibilidad de un portal para el prestador de asistencia o el consumo de servicios a través de una API que permita integrar los datos en portales corporativos (B2B).

La plataforma podrá contener otros módulos que permitan cumplir con los requisitos del reglamento a los fabricantes de software si así lo requieren, por ejemplo:

- Módulo de Transformación de datos. Permitirá recibir los datos clínicos en un formato no interoperable y transformarlos al formato que se defina en las actuaciones de la comisión.
- Módulo de almacenamiento. Permitirá persistir determinados datos para evitar las comunicaciones continuas con los sistemas del prestador de servicio y mejorar el rendimiento de la comunicación con los nodos nacional y europeo. En ningún caso almacenará ninguna información recibida del nodo nacional, solo la que debe aportar como HCe origen de los datos.
- Módulo de Interoperabilidad. El que se encargue de la comunicación con el nodo nacional.
- Módulo de anonimización/pseudoanonimización de datos, para poder proveer los datos para su uso secundario.
- Módulo de IA, para incluir algoritmos de IA que añadan funcionalidad a la plataforma
- Módulo de alertas, para generar alertas para los profesionales y también para los pacientes, que se integrará en los portales de accesos y con el módulo de Servicios de interoperabilidad.
- Otros ...

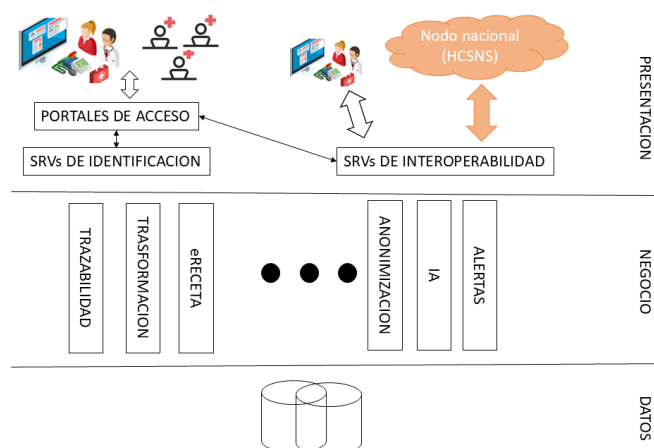


Figura 7: Plataforma Modular Interoperable

6.2. Posible modelo de negocio

6.2.1. Propuesta de valor

El modelo de negocio se articula como una plataforma SaaS modular y escalable, diseñada para que cada proveedor sanitario, desde una clínica rural hasta un gran grupo hospitalario, pueda subir, acceder y explotar datos en el EEDS sin fricciones técnicas ni riesgos regulatorios. Todos los niveles de servicio cumplen con estándares de seguridad y normativas europeas (como FHIR y SNOMED CT), garantizando la confidencialidad y la interoperabilidad.

La propuesta de valor se centra en cubrir las necesidades de pymes y clínicas independientes —como odontología o estomatología— que no cuentan con recursos para grandes desarrollos, pero que deberán cumplir con las nuevas obligaciones (incluyendo imagen médica a partir de 2029), porque se considera que este es el segmento de negocio que más se puede interesar por la solución. A este segmento se le ofrece un acceso simplificado al EEDS y un servicio integral que combina infraestructura tecnológica y una capa de gestión digital especializada, que asegura el cumplimiento normativo continuo. Sin embargo, la solución se organiza en tres planes adaptados al tamaño y necesidades del cliente para abarcar todos los posibles proveedores tecnológicos:

Plan “Connect”: Pensado para pequeños proveedores (clínicas independientes, centros rurales, consultas ambulatorias). Permite:

- Subida de datos: mediante el *Módulo de Transformación de Datos* y el *Módulo de Interoperabilidad*, que conectan con su software actual para volcar datos al EEDS de forma sencilla y estandarizada.
- Acceso a datos: acceso directo a los datos ya disponibles en el EEDS, a través del *Portal de Paciente* y el *Portal de Profesionales Sanitarios*, favoreciendo una visión integral del paciente.
- Cumplimentación de estándares: cumplimiento automático de estándares de seguridad y normativos europeos gracias al *Módulo de Identificación Segura* y al *Módulo de Trazabilidad de Accesos*, que garantizan seguridad, trazabilidad y autenticación mediante certificado electrónico.
- Cuadros de mando: cuadros de mando preconfigurados con analítica descriptiva básica, soportados por el *Módulo de Almacenamiento Temporal y Analítica Descriptiva*.

Plan “Boost”: Enfocado en proveedores medianos (hospitales privados, aseguradoras regionales). Incluye todo lo anterior y añade:

- Analítica inteligente: analítica personalizada y segmentación avanzada de pacientes, mediante el *Módulo de Inteligencia Artificial y Alertas*.
- Integraciones de bases de datos: con el *Módulo de Interoperabilidad* y el *Módulo de Transformación de Datos*, facilitando la consolidación de múltiples fuentes internas y externas.
- Personalización de bases de datos: generados desde el *Módulo de Almacenamiento Temporal* y adaptados a la gestión clínica y operativa.
- Acceso a investigaciones federadas: habilitado a través del *Módulo de Anonimización/Pseudo-anonimización*, que permite la participación en proyectos multicéntricos en entornos seguros..

Plan “Scale”: Diseñado para grandes grupos hospitalarios y aseguradoras con mayor madurez digital. Ofrece:

- Motor de IA: a través del *Módulo de Inteligencia Artificial y Alertas*, con algoritmos de predicción, prevención y estratificación de riesgos.
- Interoperabilidad Pro+: mediante el *Módulo de Interoperabilidad* con conexiones avanzadas a HCE, apps de pacientes y sistemas de terceros.

- Herramientas de decisión: soporte a decisiones clínicas y estratégicas basado en datos en tiempo real integradas con el *Módulo de Portal de Profesionales Sanitarios* y el *Módulo de Inteligencia Artificial*.

Además, en todos los niveles se integra la capa de gestión digital especializada, que asegura la conexión permanente con el nodo del Ministerio, el cumplimiento normativo, la trazabilidad y el acceso seguro de cualquier ciudadano europeo a su historia clínica.

La propuesta de valor, por tanto, no se limita a la tecnología, sino que ofrece un servicio integral de cumplimiento y digitalización, que democratiza la adaptación al EEDS y aporta valor añadido a todo tipo de proveedores sanitarios privados.

6.2.2. Estrategia de acceso al mercado

La estrategia de acceso al mercado se ha diseñado para equilibrar visibilidad institucional, credibilidad técnica y capilaridad comercial. Se articula en torno a cinco ejes complementarios:

Enfoque en clientes objetivo prioritarios La solución se dirigirá en primer lugar a pymes sanitarias que no forman parte de grandes grupos hospitalarios, como clínicas de odontología, estomatología y consultas especializadas. Estos actores carecen de capacidad para desarrollar sus propios sistemas y, sin embargo, deberán cumplir las obligaciones del EEDS, incluida la incorporación de imagen médica a partir de 2029.

Colaboración con colegios profesionales y mutuas Una vía fundamental para acelerar la adopción será establecer alianzas estratégicas con colegios profesionales sanitarios, pequeñas aseguradoras y mutuas. Estos agentes actúan como agregadores naturales de cientos de profesionales sanitarios y pequeñas clínicas, y permiten escalar rápidamente el acceso a colectivos enteros. De este modo, se reduce el coste comercial y se multiplica la capilaridad de la solución.

Generación de confianza mediante pilotos y casos de éxito Se mantendrá la estrategia de desarrollar proyectos piloto gratuitos de entre tres y seis meses con tres perfiles representativos:

- Una clínica privada de tamaño medio en entorno urbano.
- Un hospital comarcal en zona rural o semiurbana.
- Una aseguradora interesada en la explotación de datos para el manejo de pacientes crónicos.

En estos pilotos se incluirá el acompañamiento formativo y la capa de gestión digital especializada, destacando que la solución no solo proporciona tecnología, sino también un servicio integral que asegura el cumplimiento del reglamento. Los resultados se difundirán como casos de éxito a través de artículos, vídeos e infografías en medios especializados (Redacción Médica, Diario Médico) y en hubs de innovación relevantes.

Visibilidad institucional y digital Se reforzará la notoriedad mediante la participación activa en congresos de referencia como el Barcelona Health Hub Summit, Healthnology, South Summit o el Congreso Nacional de Hospitales y Gestión Sanitaria (SEDISA). A ello se sumarán mesas redondas y webinars en colaboración con asociaciones como ASPE, la Asociación Salud Digital y SEIS. En paralelo, se desplegará una estrategia digital multicanal basada en:

- Campañas de content marketing dirigidas a decisores (CIOs, gerentes, directores médicos).
- Refuerzo del posicionamiento SEO con palabras clave específicas como EEDS España, interoperabilidad clínica, SaaS sanitario, gestión digital en salud.
- Alianzas con plataformas de innovación como Kunsen, EIT Health Spain e ITEMAS.

Certificaciones y cumplimiento normativo La fiabilidad de la herramienta se sustentará en la obtención de certificaciones de calidad y seguridad como:

- ISO 27001 (gestión de seguridad de la información).
- ISO 13485 (en caso de que se considere producto sanitario).
- ENS en nivel medio-alto, obligatorio en España para sistemas que gestionan datos de salud.
- Evaluación continua de adecuación al GDPR y a los estándares europeos de interoperabilidad (FHIR, SNOMED CT).

En conjunto, la estrategia de acceso al mercado no solo busca dar a conocer la herramienta, sino también construir confianza y legitimidad en el ecosistema sanitario privado, poniendo el foco en quienes más necesitan apoyo: las pequeñas clínicas y consultas que sin esta solución tendrían enormes barreras de entrada al EEDS.

6.2.3. Modelo de ingresos

El modelo de negocio se fundamenta en un esquema de suscripción anual diferenciada por niveles. La modalidad Conect (básica) se sitúa en un rango de 5.000 a 10.000 euros anuales, mientras que la versión Boost (avanzada) oscila entre los 25.000 y 40.000 euros. Por su parte, la modalidad Scale (enterprise) supera los 75.000 euros anuales. Además de estas suscripciones, se contempla la generación de ingresos adicionales a través de nuevas integraciones o adaptaciones específicas que puedan requerir los clientes.

6.2.4. Plan de inversión

- **Acciones comerciales y de marketing:** El despliegue inicial de la estrategia de comercialización implica una inversión estimada de 75.000 euros durante el primer año. Esta cifra se distribuye en 30.000 euros destinados a patrocinios y participación en congresos, 15.000 euros para el desarrollo de contenidos (vídeos, infografías y casos de éxito), 20.000 euros para la realización de pruebas piloto —incluyendo el despliegue, soporte y evaluación—, y 10.000 euros para acciones digitales, entre ellas SEO, newsletters y webinars.
- **Recursos humanos:** El éxito de la estrategia requiere la incorporación de perfiles especializados. Se prevé la contratación de un responsable de desarrollo de negocio a tiempo completo, encargado de la relación con hospitales, aseguradoras y asociaciones; un jefe de cuentas, también a tiempo completo, con responsabilidad sobre el acompañamiento en los pilotos, la formación a usuarios y el soporte postventa; y un profesional de marketing y comunicación a media jornada, centrado en la generación de contenido y en la relación con hubs y prensa sectorial. El coste total estimado de recursos humanos asciende a 110.000 euros anuales.

6.2.5. Plan de acción en fases

El plan de despliegue propuesto se estructura en tres fases.

- **Fase 1 (0–6 meses):** Durante este periodo se priorizará la obtención de certificaciones críticas, como el ENS y la ISO 27001. Paralelamente, se identificarán y formalizarán los acuerdos con los tres pilotos seleccionados, al tiempo que se desarrollarán las primeras acciones de difusión en congresos de referencia como el BHH Summit y Healthnology.
- **Fase 2 (6–12 meses):** En esta etapa se evaluarán los resultados de los pilotos y se elaborarán casos de éxito para su difusión. Asimismo, se lanzará la estrategia digital con especial énfasis en campañas SEO y se intensificará la presencia en congresos de alcance nacional, como los organizados por SEDISA o ASPE.
- **Fase 3 (12–18 meses):** Finalmente, se buscará consolidar el escalado de la solución hacia un mayor número de hospitales y aseguradoras, establecer alianzas estratégicas con hubs y sociedades médicas, y afianzar el modelo de ingresos basado en las suscripciones.

La estrategia propuesta combina visibilidad en foros clave, validación mediante pilotos representativos, y una base sólida de certificaciones que garantizan la seguridad y confianza del mercado. Con una inversión inicial de aprox. 185.000 € el primer año (75K marketing + 110K RRHH), se sientan las bases para construir una posición de liderazgo en el acceso al dato sanitario en España.

El modelo de negocio planteado permite democratizar el acceso a la explotación del dato sanitario, superando las barreras económicas y tecnológicas que impiden a los pequeños proveedores sumarse al EEDS. Su enfoque SaaS modular, la estrategia escalonada de acceso al mercado y la viabilidad económica lo convierten en una propuesta sólida para impulsar la equidad, la innovación y la sostenibilidad en el sistema de salud.

6.3. DAFO Resumen

Además del planteamiento de la solución técnica y el modelo de negocio, se ha realizado un análisis de las Fortalezas, Debilidades, Oportunidades y Amenazas, que puede consultarse en la Figura 8.



Figura 8: Análisis DAFO

7. CONCLUSIONES

La investigación realizada permite concluir que la implementación del Espacio Europeo de Datos de Salud constituye una oportunidad sin precedentes para avanzar hacia un modelo sanitario digital, seguro y centrado en el paciente. En el caso de la sanidad privada, la adaptación al reglamento implica retos significativos relacionados con la interoperabilidad, la gobernanza del dato y la capacidad de inversión en infraestructuras tecnológicas. No obstante, la propuesta desarrollada en este trabajo demuestra que es posible ofrecer soluciones compartidas que permitan la integración de todos los actores en el EEDS, evitando la exclusión de los prestadores con menor madurez digital y promoviendo un ecosistema sanitario más equitativo y cohesionado.

El enfoque planteado, basado en plataformas SaaS modulares, se revela como una alternativa viable para democratizar el acceso al EEDS y garantizar el cumplimiento normativo. Su carácter escalable facilita la adaptación de la solución a distintos perfiles de prestadores, mientras que la incorporación de estándares internacionales de interoperabilidad y seguridad refuerza la confianza tanto de profesionales como de pacientes. Asimismo, la validación a través de proyectos piloto y la obtención de certificaciones internacionales se identifican como factores críticos para generar credibilidad en el mercado y acelerar la adopción de la solución.

7.1. Grado de consecución de los objetivos planteados

En relación con los objetivos definidos al inicio del trabajo, se puede afirmar que estos han sido alcanzados en un grado significativo, aportando una visión estructurada y aplicable a la adaptación de la sanidad privada al Reglamento del EEDS.

En primer lugar, se ha realizado una identificación detallada de los diferentes tipos de prestadores de asistencia sanitaria en el ámbito privado en España, incluyendo grandes grupos hospitalarios, clínicas de tamaño medio, consultas independientes y agrupaciones profesionales. Este análisis ha permitido reconocer la heterogeneidad del sector y poner de relieve la existencia de importantes diferencias en su grado de digitalización y en los recursos disponibles para afrontar la transición hacia el EEDS.

En segundo lugar, se han identificado los requerimientos técnicos y funcionales exigidos por el reglamento para la puesta a disposición de las categorías prioritarias de datos, como la historia clínica resumida, las recetas electrónicas, los informes de laboratorio, las pruebas de imagen y los informes de alta hospitalaria. En este sentido, el estudio ha analizado los estándares de interoperabilidad necesarios (FHIR, SNOMED CT, LOINC, DICOM), así como los requisitos asociados a los derechos de los pacientes, la trazabilidad de accesos y la gestión de consentimientos.

En tercer lugar, se han examinado los recursos disponibles para llevar a cabo la adaptación, tanto desde el punto de vista tecnológico como organizativo. Se han identificado las iniciativas ya en marcha en España (como el nodo nacional y los nodos autonómicos de interoperabilidad, así como proyectos impulsados por fundaciones y asociaciones del sector privado), además de destacar las limitaciones económicas y de personal especializado que afectan a los prestadores de menor tamaño.

En cuarto lugar, el trabajo ha cumplido el objetivo de proponer una solución viable para que los prestadores sanitarios privados puedan poner a disposición sus sistemas de historia clínica electrónica en el EEDS para uso primario, y habilitar la explotación de datos para fines secundarios en condiciones de seguridad y cumplimiento normativo. La solución planteada, basada en plataformas intermedias modulares ofrecidas en un modelo SaaS, responde a las necesidades de flexibilidad, escalabilidad y reducción de costes, lo que la hace especialmente adecuada para la diversidad de actores que conforman el sector privado.

Finalmente, se ha logrado definir una arquitectura tecnológica de la solución, en la que se detallan los componentes funcionales y técnicos necesarios para cumplir con los requisitos del reglamento, tanto en materia de seguridad como en el marco del RGPD. Asimismo, se ha diseñado un modelo de negocio escalonado que asegura la sostenibilidad de la propuesta y que permite adaptar los servicios a las

diferentes realidades del sector. Este modelo integra desde planes básicos de acceso al EEDS hasta servicios avanzados de inteligencia artificial y analítica para grandes grupos hospitalarios, demostrando la aplicabilidad práctica de la solución en distintos niveles de madurez digital.

El trabajo ha logrado alcanzar los objetivos planteados, aportando una propuesta coherente, viable y alineada con los principios del EEDS. No obstante, se reconoce que la validación empírica mediante pilotos y la evaluación del impacto real en los flujos asistenciales y en la eficiencia operativa constituyen pasos necesarios en el futuro para consolidar la aplicabilidad de la solución en contextos reales.

7.2. Líneas futuras

De cara a las líneas de trabajo futuras, se identifican diversas áreas de desarrollo prioritario:

- Resulta necesario profundizar en casos de uso concretos vinculados con las categorías de datos que progresivamente deberán integrarse en el EEDS, tales como los informes de laboratorio, las imágenes médicas o los informes de alta hospitalaria.
- Se debe avanzar en la definición de modelos de gobernanza que distribuyan de manera clara y justa las responsabilidades entre proveedores privados, intermediarios tecnológicos y nodos nacionales, garantizando así un marco sólido de confianza y transparencia.
- Es preciso explorar con mayor detalle el potencial del uso secundario de los datos y como podría extenderse esta solución para cumplir con esta parte del reglamento, que no era objeto de este proyecto.
- La ciberseguridad se configura como un eje transversal en todo el proceso. La correcta aplicación de la Directiva NIS2 y la integración con los sistemas de identidad digital europea (eIDAS) resultan esenciales para reforzar la protección de la información clínica y salvaguardar los derechos fundamentales de los pacientes.

Bibliografía

- [1] Dirección General de Salud y Seguridad Alimentaria. “Reglamento Relativo al Espacio Europeo de Datos de Salud (EEDS).” Public Health, 28 Mar. 2025, health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_es.
- [2] Salud Digital. “Ministerio de Sanidad - Áreas - Espacio Europeo de Datos de Salud.” Sanidad.gob.es, 2025, www.sanidad.gob.es/areas/saludDigital/espacioEuropeoDS/home.htm.
- [3] EUR-Lex. “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, (Texto Pertinente a Efectos Del EEE).” Europa.eu, <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32025R0327>.
- [4] EUR-Lex. “Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo, de 27 de Abril de 2016, Relativo a La Protección de Las Personas Físicas En Lo Que Respecta al Tratamiento de Datos Personales Y a La Libre Circulación de Estos Datos Y Por El Que Se Deroga La Directiva 95/46/CE (Reglamento General de Protección de Datos) (Texto Pertinente a Efectos Del EEE).” Europa.eu, 2016, <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>.
- [5] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, Wwww.boe.es, [Wwww.boe.es, 6Dec.2018, www.boe.es/buscar/act.php?id=BOE-A-2018-16673](https://www.boe.es/boe/6Dec.2018).
- [6] Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, Wwww.boe.es, 2018, www.boe.es/buscar/act.php?id=BOE-A-2002-22188.
- [7] Ley 14/2007, de 3 de julio, de Investigación biomédica, Wwww.boe.es, 2011, www.boe.es/buscar/doc.php?id=BOE-A-2007-12945.
- [8] Ley 33/2011, de 4 de octubre, General de Salud Pública. Wwww.boe.es, 2024, www.boe.es/eli/es/1/2011/10/04/33s.
- [9] Ley 33/2011, de 4 de octubre, General de Salud Pública. “Boletín Oficial Del Estado.” Wwww.boe.es, 2024, www.boe.es/eli/es/1/2011/10/04/33s.
- [10] Unión Europea. “Reglamento (UE) 2022/868 Del Parlamento Europeo Y Del Consejo de 30 de Mayo de 2022 Relativo a La Gobernanza Europea de Datos Y Por El Que Se Modifica El Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).” Wwww.boe.es, 2022, www.boe.es/buscar/doc.php?id=DOUE-L-2022-80835.
- [11] Unión Europea. Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) Wwww.boe.es, 2022, <https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81573>.
- [12] European Commission. “Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) — Shaping Europe’s Digital Future.” Digital-Strategy.ec.europa.eu, 14 Sept. 2023, digital-strategy.ec.europa.eu/en/policies/nis2-directive.
- [13] “¿Qué Es La Interoperabilidad? - Explicación Sobre La Interoperabilidad En La Asistencia Sanitaria - AWS.” Amazon Web Services, Inc., aws.amazon.com/es/what-is/interoperability/.
- [14] CNIS. “Glosario Interoperabilidad .” Cnis.es, 2025, www.cnis.es/glosario-interoperabilidad/.
- [15] HL7. “Summary - FHIR V4.0.1.” Wwww.hl7.org, www.hl7.org/fhir/summary.html.

- [16] “About DICOM- Overview.” DICOM, www.dicomstandard.org/about-home.
- [17] “ATCDDD - Structure and Principles.” Atcddd.fhi.no, atcddd.fhi.no/atc/structure_and_principles/.
- [18] SNOMED International. “What Is SNOMED CT.” SNOMED International, 2025, www.snomed.org/what-is-snomed-ct.
- [19] World Health Organization. “International Classification of Diseases (ICD).” Wwww.who.int, 2022, www.who.int/standards/classifications/classification-of-diseases.
- [20] LOINC. “About LOINC.” LOINC, 2025, loinc.org/about/.
- [21] “Portales Para Pacientes - Una Herramienta En Línea Para Su Salud: MedlinePlus Enciclopedia Médica.” Medlineplus.gov, 2023, medlineplus.gov/spanish/ency/patientinstructions/000880.htm.
- [22] Fundación ISYS. “Uso Secundario de Los Datos Clínicos.” Fundacionisys.org, 2025, www.fundacionisys.org/es/blogs/profesional/profesional/999-uso-secundario-de-los-datos-clinicos.
- [23] Microsoft. “What Is SaaS? Software as a Service — Microsoft Azure.” Azure.microsoft.com, 2023, azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas.
- [24] Hernández, Miguel. “Saas or Software as a Service: What It Is, Characteristics and Examples.” Telefónica, 17 June 2025, ww.telefonica.com/en/communication-room/blog/saas-what-it-is/.
- [25] “What Are the Characteristics of SaaS? - Tencent Cloud.” Tencentcloud.com, 2025, www.tencentcloud.com/techpedia/102553. Accessed 28 Sept. 2025.
- [26] European Commission. “Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) — Shaping Europe’s Digital Future.” Digital-Strategy.ec.europa.eu, 14 Sept. 2023, digital-strategy.ec.europa.eu/en/policies/nis2-directive.
- [27] “EHealth Network.” Public Health, 28 Mar. 2025, health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/eu-cooperation/ehealth-network_en.
- [28] “Electronic Cross-Border Health Services.” Public Health, 5 Mar. 2025, health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en.
- [29] Pinillos, Berta. “La Sanidad Privada Realiza El 40 % de Las Intervenciones Quirúrgicas En España.” EFE Salud, 24 Apr. 2025, efesalud.com/sanidad-privada-espana-informe-observatorio-fundacion-idis-2025/.
- [30] Fundación IDIS. “Observatorio de Digitalización En La Sanidad Privada: Madurez Digital Y Casos de Éxito.” Fundación IDIS, 2025, www.fundacionidis.com/informes/otros-informes/informe-observatorio-de-digitalizacion-en-la-sanidad-privada-madurez-digital-y-casos-de-e.
- [31] “En Soporte Electrónico.” CGCOM, 2019, www.cgcom.es/servicios/receta-medica-privada/en-soporte-electronico.
- [32] BOE-A-2011-1013 Real Decreto 1718/2010, de 17 de Diciembre, Sobre Receta Médica Y Órdenes de Dispensación. Wwww.boe.es, www.boe.es/buscar/act.php?id=BOE-A-2011-1013.
- [33] “¿Qué Es SREP?” E-Recetaprivada.com, 2025, e-recetaprivada.com/que-es-srep/. Accessed 21 Sept. 2025.

- [34] Consejo General de Dentistas de España. “Una Nueva Web Reúne Toda La Información Sobre El Sistema de Receta Electrónica Privada - Consejo General de Dentistas de España.” 29 June 2022, consejodentistas.es/una-nueva-web-reune-toda-la-informacion-sobre-el-sistema-de-receta-electronica-privada/.
- [35] “Hospital Digital Y Telemedicina B2B — Docline.” Docline, 23 Sept. 2025, docline.com/receta-electronica/.

