

# RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS DE SALUD EN EL ESPACIO EUROPEO DE DATOS DE SALUD (EEDS)

---

## Autores

M.<sup>a</sup> Ángeles Egusquiza Balmaseda

Raquel Luquin Bergareche

María Jorqui Azofra

Javier Vidán Peña







## Disfrute gratuitamente **DURANTE UN AÑO** de los eBook y audiolibros de las obras de Editorial Colex\*

- Acceda a la página web de la editorial **www.colex.es**
- Identifíquese con su usuario y contraseña. En caso de no disponer de una cuenta regístrese.
- Acceda en el menú de usuario a la pestaña «Mis códigos» e introduzca el que aparece a continuación:

### RASCAR PARA VISUALIZAR EL CÓDIGO

- Una vez se valide el código, aparecerá una ventana de confirmación y su eBook y/o audiolibro estará disponible **durante 1 año desde su activación** en la pestaña «Mis libros» en el menú de usuario.

\* Los audiolibros están disponibles en las ediciones más recientes de nuestras obras. Se excluyen expresamente las colecciones «Códigos comentados», «Biblioteca digital» y los productos de [www.vademecumlegal.es](http://www.vademecumlegal.es).

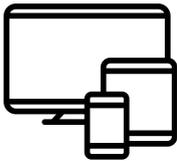
No se admitirá la devolución si el código promocional ha sido manipulado y/o utilizado.



**¡Gracias por confiar en nosotros!**

La obra que acaba de adquirir incluye de forma gratuita la versión electrónica. Acceda a nuestra página web para aprovechar todas las funcionalidades de las que dispone en nuestro lector.

## Funcionalidades eBook



**Acceso desde cualquier dispositivo con conexión a internet**



**Idéntica visualización a la edición de papel**



**Navegación intuitiva**



**Tamaño del texto adaptable**

Síguenos en:     

**RÉGIMEN JURÍDICO DE  
PROTECCIÓN DE DATOS DE  
SALUD EN EL ESPACIO EUROPEO  
DE DATOS DE SALUD (EEDS)**



# **RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS DE SALUD EN EL ESPACIO EUROPEO DE DATOS DE SALUD (EEDS)**

**M.<sup>a</sup> Ángeles Egusquiza Balmaseda**

*Catedrática de Derecho civil  
Universidad Pública de Navarra*

**Raquel Luquin Bergareche**

*Profesora Titular de Derecho civil  
Universidad Pública de Navarra*

**María Jorqui Azofra**

*Profesora de Derecho Civil  
Universidad Pública de Navarra*

**Javier Vidán Peña**

*Profesor Ayudante Doctor de Derecho Civil  
Universidad Pública de Navarra*



Esta publicación forma parte del proyecto de investigación «Contratación de Servicios de Telemedicina: Actualidad y Desafíos Jurídicos» (TED2021-129472B-00/MICINN) financiado por MCIN/AEI/10.13039/501100011033 y por la Unión Europea NextGeneration EU/PRTR.

Copyright © 2025

Queda prohibida, salvo excepción prevista en la ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (arts. 270 y sigs. del Código Penal). El Centro Español de Derechos Reprográficos ([www.cedro.org](http://www.cedro.org)) garantiza el respeto de los citados derechos.

Editorial Colex S.L. vela por la exactitud de los textos legales publicados. No obstante, advierte que la única normativa oficial se encuentra publicada en el BOE o Boletín Oficial correspondiente, siendo esta la única legalmente válida, y declinando cualquier responsabilidad por daños que puedan causarse debido a inexactitudes e incorrecciones en los mismos.

Editorial Colex S.L. habilitará a través de la web [www.colex.es](http://www.colex.es) un servicio online para acceder a las eventuales correcciones de erratas de cualquier libro perteneciente a nuestra editorial.

© M.<sup>a</sup> Ángeles Egusquiza Balmaseda

© Raquel Luquin Bergareche

© María Jorqui Azofra

© Javier Vidán Peña

© Editorial Colex, S.L.

Calle Costa Rica, número 5, 3.º B (local comercial)

A Coruña, 15004, A Coruña (Galicia)

[info@colex.es](mailto:info@colex.es)

[www.colex.es](http://www.colex.es)

I.S.B.N.: 979-13-7011-094-9

Depósito legal: C 650-2025

# SUMARIO

## CAPITULO I

### SERVICIOS DE TELEMEDICINA: PROTECCIÓN DE DATOS DE SALUD DEL PACIENTE Y USUARIO

*Javier Vidán Peña*

1. Introducción . . . . .	11
2. Derechos del paciente digital en relación a sus datos de salud. . . . .	18
2.1. Derecho de información para el tratamiento de datos de salud . . . . .	18
2.2. Derecho a la privacidad y confidencialidad de los datos de salud . . . . .	24
2.3. Cumplimiento de los principios y normas del RGPD y la LOPD . . . . .	29
2.4. Derechos de acceso, rectificación y supresión . . . . .	31
2.5. Derechos de las personas físicas sobre el uso primario de sus datos de salud electrónicos en el REEDS . . . . .	39
3. Telemonitorización de variables: gestión de datos mediante servicios en la nube . . . . .	42
4. Referencias normativas. . . . .	44
5. Referencias bibliográficas . . . . .	46

## CAPÍTULO II

### DERECHOS Y DISPOSICIONES RELATIVAS AL USO PRIMARIO DE LOS DATOS DE SALUD ELECTRÓNICOS PERSONALES

*María Jorqui Azofra*

1. Introducción . . . . .	49
2. Algunas breves consideraciones sobre los derechos de las personas físicas en relación con el uso primario de sus datos de salud electrónicos . . . . .	52
2.1. Derecho de acceso . . . . .	52
2.2. Derecho a introducir información en la propia HCE . . . . .	55
2.3. El derecho a la rectificación . . . . .	56
2.4. El derecho a la portabilidad . . . . .	57
2.5. Derecho a limitar el acceso . . . . .	62
2.6. Derecho a obtener información sobre el acceso a los datos . . . . .	63
2.7. Derecho de las personas físicas a la autoexclusión para el uso primario . . . . .	64

## SUMARIO

3. Breve referencia a la gobernanza para el uso primario . . . . .	65
4. ¿De qué modo y con respecto a qué datos ejercitar los mencionados derechos?: Revisión de algunas categorías conceptuales . . . . .	68
4.1. Los datos de salud electrónicos personales. . . . .	69
4.1.1. Datos personales . . . . .	71
4.1.2. Datos relativos a la salud. . . . .	76
4.1.3. Datos genéticos . . . . .	86
4.2. Las categorías prioritarias de datos de salud electrónicos . . . . .	86
5. Datos de salud tratados en formato electrónico en un sistema HCE. . . . .	89
6. MiSalud@UE: La infraestructura transfronteriza para el uso primario de datos de salud electrónicos personales . . . . .	97
7. Servicios e infraestructuras sanitarias digitales complementarias . . . . .	99
8. Algunas consideraciones sobre los sistemas HCE y aplicaciones de bienestar . . . . .	101
8.1. Los sistemas HCE . . . . .	101
8.2. Las aplicaciones de bienestar . . . . .	108
9. Conclusiones. . . . .	110
10. Bibliografía . . . . .	111

## CAPÍTULO III

### CESIÓN ALTRUISTA DE DATOS EN EL ESPACIO EUROPEO DE DATOS DE SALUD

*M.ª Ángeles Egusquiza Balmaseda*

1. Contextualización . . . . .	117
2. Cesión altruista de datos de salud . . . . .	125
2.1.El <i>prius</i> del «altruismo»: la cesión de datos de salud como un valor tangible . . . . .	125
2.2. La noción legal de «cesión altruista» de datos de salud . . . . .	131
2.2.1. Consideraciones generales . . . . .	131
2.2.2. «Cesión altruista» y/o «donación» de datos de salud . . . . .	133
3. Elementos negociales de la «cesión altruista de datos»de salud en el EEDS . . . . .	143
3.1. Objeto de cesión: datos de salud electrónicos personales y no personales. . . . .	143
3.2. Aspectos subjetivos de la cesión «altruista» de datos de salud . . . . .	148
3.2.1. Una cuestión previa: interesado y titular o tenedor de los datos de salud electrónicos . . . . .	148
3.2.2. Cedente «altruista» de los datos de salud electrónicos: consentimiento y permiso. . . . .	150
3.2.3. Cesionarios de los datos de salud electrónicos para fines altruistas: su control . . . . .	157
3.2.3.1. Organizaciones de gestión de datos para fines altruista . . . . .	157
3.2.3.2. Inscripción en el Registro de organizaciones de gestión para fines altruistas . . . . .	169

## SUMARIO

4. Régimen jurídico para la cesión altruista de datos de salud electrónicos . . .	174
4.1. Deberes del cesionario altruista de datos de salud . . . . .	174
4.1.1. Deber de información: consentimiento o asentimiento informado y finalista . . . . .	175
4.1.2. Entorno de tratamiento seguro . . . . .	180
4.2. Forma de prestación del consentimiento y asentimiento por el cedente: el formulario europeo ¿sólo un medio de prueba? . . . . .	182
4.3. Revocación del consentimiento y de la autorización: consecuencias jurídicas . . . . .	185
5. Bibliografía . . . . .	193

## CAPITULO IV

### REUTILIZACIÓN O USO SECUNDARIO DE LOS DATOS PERSONALES DE SALUD

*Raquel Luquín Bergareche*

1. Reutilización de los datos de salud: contexto y caracterización en el marco del EEDS . . . . .	200
1.1 El valor de los «data» en los nuevos ecosistemas de salud digital y medicina personalizada . . . . .	200
1.2. El EEDS y su ecosistema regulatorio: del RGPD al REEDS . . . . .	201
2. Los datos de salud y su «tratamiento ulterior» en el RGPD: regla general, excepciones y bases jurídicas legitimadoras . . . . .	208
2.1. Datos de salud y genéticos de la persona como datos especialmente sensibles . . . . .	208
2.2. La regla general de prohibición de tratamiento de datos personales de salud . . . . .	210
2.3. Excepciones y bases jurídicas legitimadoras del uso ulterior de los datos de salud . . . . .	211
2.4. El consentimiento del interesado para un uso ulterior de sus datos de salud: algunas cuestiones . . . . .	213
2.4.1. El consentimiento en el RGPD . . . . .	213
2.4.2. El consentimiento como base legitimadora del tratamiento de datos de salud: vías de flexibilización . . . . .	215
2.4.3. Anonimización y seudonimización: necesarias, pero ¿suficientes? . . . . .	218
2.5. Configuración del interés público como base de legitimación . . . . .	220
3. La unificación de las bases jurídicas legitimadoras del tratamiento de datos de salud en la LOPDGDD . . . . .	221
4. El «uso secundario» de «datos de salud electrónicos» en el Reglamento (UE) 2025/327 del Parlamento europeo y del Consejo, de 11 de febrero de 2025, relativo al espacio europeo de datos de salud: la obligación legal de su puesta a disposición de los usuarios . . . . .	225
4.1. El EEDS como ecosistema . . . . .	225
4.1.1. Nuevos enfoques en el uso secundario de datos de salud . . . . .	225
4.1.2. Actores del EEDS: uso secundario . . . . .	227

## SUMARIO

4.2. La Unión Europea de la Salud: delimitación de categorías de «datos de salud electrónicos» y «fines del tratamiento para uso secundario» en el REEDS .....	230
4.2.1. ¿Armonización a la vista en materia de salud en la UE? .....	230
4.2.2. Categorías de datos de salud electrónicos para uso secundario .....	231
4.2.3. Derechos de propiedad intelectual e industrial y secretos comerciales .....	233
4.2.4. Usos secundarios permitidos .....	234
4.2.5. Usos secundarios prohibidos .....	236
4.2.6. Minimización de datos y adecuación o limitación a los fines .....	237
4.3. Marco jurídico regulador del uso secundario de datos de salud electrónicos .....	237
4.3.1. «Organismos de acceso» a los datos de salud: funciones y obligaciones .....	237
4.3.2. Obligaciones de los tenedores de datos de salud .....	243
4.3.3. Usuarios de datos de salud: obligaciones .....	243
4.3.4. Cobro de tasas .....	244
4.4. Procedimiento .....	245
4.4.1. Solicitud de acceso a datos de salud .....	245
4.4.2. Permiso de datos de salud .....	246
4.4.3. Petición de datos de salud .....	250
4.4.4. Modelos para apoyar el acceso a datos de salud electrónicos para uso secundario .....	250
4.5. El derecho de autoexclusión del tratamiento de datos de salud electrónicos personales para uso secundario .....	250
4.6. Procedimiento simplificado para el acceso a los datos de salud electrónicos de un tenedor fiable .....	253
4.7. Entorno de tratamiento seguro .....	254
5. DatosSalud@UE Infraestructura transfronteriza para el uso secundario .....	255
6. Solicitudes de acceso a datos de salud y peticiones de datos de salud por terceros países .....	258
7. Reclamaciones .....	259
8. Referencias normativas .....	259
9. Bibliografía .....	260

# CAPITULO I

---

## **SERVICIOS DE TELEMEDICINA: PROTECCIÓN DE DATOS DE SALUD DEL PACIENTE Y USUARIO<sup>1</sup>**

**Javier Vidán Peña**

*Profesor Ayudante Doctor de Derecho Civil  
Universidad Pública de Navarra*

**Sumario:** 1. Introducción. 2. Derechos del paciente digital en relación a sus datos de salud. 2.1. Derecho de información para el tratamiento de datos de salud. 2.2. Derecho a la privacidad y confidencialidad de los datos de salud. 2.3. Cumplimiento de los principios y normas del RGPD y la LOPD. 2.4. Derechos de acceso, rectificación y supresión. 2.5. Derechos de las personas físicas sobre el uso primario de sus datos de salud electrónicos en el REEDS. 3. Telemonitorización de variables: gestión de datos mediante servicios en la nube. 4. Referencias normativas. 5. Referencias bibliográficas.

### **1. Introducción**

El Reglamento General de Protección de Datos 216/679 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 (en adelante, RGPD)<sup>2</sup> define en su art. 4.1) los «datos personales» como «toda información sobre una persona física identificada o identificable (“el interesado”)». Persona física identificable es toda persona cuya identidad pueda hallarse, ya sea directa o indirectamente,

---

1 El presente trabajo es parte del proyecto de Investigación «Contratación de Servicios de Telemedicina: Actualidad y Desafíos Jurídicos (TED2021-129472B-00/MICINN «Next Generation EU»/PRTR)

2 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 (RGPD) publicado en el «DOUE» núm. 119, de 4 de mayo de 2016:  
Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>

mediante un identificador. La propia norma pone como ejemplo de identificadores el nombre, el DNI, datos de localización, un identificador en línea o uno o varios rasgos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de la persona. Es decir, cualquier información que, directa o indirectamente, pueda servir para identificar al interesado en cuanto titular de la misma será susceptible de ser considerada como dato personal<sup>3</sup>.

Dentro de los datos personales, el art. 9 RGDPR recoge una categoría que requiere de una especial protección: aquellos «(...) que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida u orientación sexual de una persona física». El tratamiento de estos datos queda prohibido, salvo que el interesado dé su consentimiento explícito<sup>4</sup> o cuando concurra alguna de las circunstancias que recoge el apartado 2 del citado precepto<sup>5</sup>. No será necesario que el médico o el centro sanitario solicite el consentimiento a los pacientes, por ejemplo, cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social (art. 9.2.h); si el tratamiento de datos se efectúa por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios o la inspección de reclamaciones de los ciudadanos (art. 9.2.i); o cuando el tratamiento es necesario para fines de archivo en interés público, investigación científica o histórica o fines estadísticos.

Por su propia naturaleza, el tratamiento de los datos personales referentes a la salud implica un riesgo importante para los derechos y las libertades fundamentales de los ciudadanos, y es por ello que merecen una especial

---

3 J. F. RODRÍGUEZ AYUSO, «Estado de alarma y protección de la privacidad en tiempos de pandemia: licitud del tratamiento de categorías especiales de datos», *Revista de Derecho político*, 110, 2021, p. 302.

4 Es preciso mencionar, no obstante, que el art. 9.1 LOPD excluye la posibilidad de superar la prohibición del art. 9.1 RGDPR mediante el consentimiento con el objetivo de evitar situaciones discriminatorias cuando la finalidad principal de los datos sea identificar la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico del afectado. No se excluyen, no obstante, los datos personales relativos a la salud del interesado.

5 Si bien la norma general es la prohibición del tratamiento de los datos de salud, el cdo. 52 RGDPR establece que deben autorizarse excepciones cuando lo establezca el Derecho de la Unión y de los Estados miembros, siempre que se den las garantías necesarias.

protección<sup>6</sup>. Como afirma MERINO MARTÍN<sup>7</sup>, los datos de salud constituyen datos «de carácter íntimo que afectan a la dignidad de la persona» cuyo acceso no autorizado por terceros puede atentar contra la intimidad personal y familiar del interesado. Este tipo de datos se definen en el citado art. 4 RGPD como un subtipo de datos personales «relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud» (ap. 15). También son categorías específicas de datos personales los «datos genéticos» y los «datos biométricos», definidos en los apartados 13 y 14 del RGPD. Los primeros se refieren a aquellos datos personales relacionados con las características genéticas de una persona física, ya sean heredadas o adquiridas, que aportan información única sobre su fisiología o salud, y que se obtienen, entre otros métodos, mediante el análisis de una muestra biológica. Por su parte, los datos biométricos hacen referencia a información personal derivada de tratamientos técnicos específicos que reflejan características físicas, fisiológicas o conductuales de una persona física, y que permiten confirmar su identificación de manera única, como es el caso de imágenes faciales o huellas dactilares.

Si bien la definición legal de «datos relativos a la salud» que hace el Reglamento resulta limitada, pues no incorpora criterios concretos que permitan determinar qué información sobre la persona debe ser considerada en esta esfera de su salud<sup>8</sup>, en la parte expositiva del RGPD (cdo. 35) se incorporan más elementos que permiten concretar y delimitar mejor dicho concepto. Considera el legislador comunitario que, entre los datos personales referentes a la salud se deben incluir «todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro», incorporando una relación de datos personales desde un planteamiento *numerus apertus* que incluye información recopilada en el contexto de la inscripción para la asistencia sanitaria o durante la prestación de dicha asistencia, conforme a la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1). Así, cualquier número, símbolo o dato que identifique de manera única a una persona física a efectos sanitarios; información obtenida mediante pruebas o exámenes corporales, incluidos los datos genéticos y

---

6 El cdo. 51 RGPD establece que los datos personales merecen una especial protección por tratarse de datos particularmente sensibles en relación con los derechos y las libertades fundamentales de los ciudadanos. Por su parte, CRISTEA UIVARU sostiene que tendrán consideración de datos sensibles «aquellos que, en caso de divulgarse de manera indebida, perturbarían la esfera más íntima del ser humano», entre los que se encuentran los datos de salud. L. Cristea Uivaru, *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud*, Bosch Editor, 2018, p. 46.

7 J. Merino Martín, «Los datos personales relativos a la salud y la Historia Clínica», *Revista Aranzadi Doctrinal*, 10/2019, 2019, pp. 5-6.

8 Misma consideración hace H. O. HERRÁN ORTIZ, «Datos personales de salud, investigación científica y tecnología big data. De la necesidad de un marco normativo propio en la UE», en *E-salud, autonomía y datos clínicos: un nuevo paradigma*, Dykinson, 2021, p. 188.

muestras biológicas; y «cualquier información»<sup>9</sup>, a modo de ejemplo, relacionada con enfermedades, discapacidades, riesgos de salud, historial médico, tratamientos clínicos o el estado fisiológico o biomédico del interesado, con independencia de la fuente, ya sea un médico, otro profesional de la salud, un hospital, un dispositivo médico o una prueba diagnóstica *in vitro*.

La Ley Orgánica de protección de datos personales y garantía de los derechos digitales (en adelante, LOPD<sup>10</sup>) se articula, en su conjunto, en torno a los conceptos previstos en el RGPD, no los redefine ni contradice. Por su parte, también a nivel estatal y en el ámbito regulador de los derechos y deberes de profesionales sanitarios y de pacientes, la Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (en adelante, LBRAP<sup>11</sup>), incorpora en su art. 3 la definición legal de «información clínica» como «todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla». Realizando una comparativa entre la definición de «datos relativos a la salud» incorporada en el RGPD y de la «información clínica» que acabamos de exponer, podemos apreciar que no resulta sencillo diferenciar ambos conceptos, si bien entendemos que los datos relativos a la salud se incluyen dentro de la información clínica, o, dicho de otro modo, que la «información clínica» incorpora datos sobre la salud de las personas: la «información clínica» sería el continente y los datos de salud el contenido.

Según expone la AEPD<sup>12</sup>, los datos personales existentes en bases de datos sanitarias son de dos tipos: los que identifican a la persona, tales como nombre y apellidos, dirección, teléfono, DNI, número de tarjeta sanitaria, etc...; y toda la información acerca de su estado de salud, tales como pruebas diagnósticas, cirugías, medicamentos, antecedentes familiares, etc. Toda esa información personal y de salud de cada paciente constituye la «historia clínica», definida por la LBRAP (art. 3) como «el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial». Posterior-

---

9 Con la expresión «cualquier información» el legislador ha pretendido dar cabida a un amplio conjunto de situaciones, no limitándose estrictamente a lo más íntimo de una persona. Da cuenta de ello L. Cristea Uivaru, *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud*, cit., pp. 40-41.

10 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD) publicada en el «BOE» núm. 294, de 6 de diciembre de 2018: Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>

11 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 publicada en el «BOE» núm. 274, de 15 de noviembre de 2002: Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188>

12 Agencia Española de Protección de Datos (AEPD), *Guía para pacientes y usuarios de la Sanidad*, 2019, p. 5.

mente, en el art. 14.1 del mismo cuerpo legal vuelve a definir añadiéndose que el conjunto de los documentos asistenciales relativos al paciente deben incluir la identificación de los médicos y demás profesionales que han intervenido con la finalidad de «obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro».

El Capítulo V de la LBRAP regula aspectos relacionados con la historia clínica, tales como su definición, archivo, contenido, usos, conservación, derechos de acceso y derechos relacionados con su custodia. En palabras de HURTADO DÍAZ-GUERRA, la historia clínica es el «instrumento básico del buen ejercicio sanitario», pues en ella se recoge la información que necesita el médico para tener una visión completa y global del paciente que le permita asistirle de manera adecuada, además de servir para facilitar el proceso clínico en cuestión. La información que contenga la historia clínica deberá ser la necesaria para conocer de forma veraz y actualizada el estado de salud del paciente, prescindiendo de otros datos que no resulten necesarios para lograr esta finalidad. Los profesionales sanitarios tienen, por tanto, el deber de actualizar la historia clínica de sus pacientes con la finalidad de facilitar el proceso de asistencia sanitaria, de forma que cualquier otro facultativo que les atienda tenga constancia de todos aquellos datos que, bajo criterio médico, puedan ser relevantes para conocer de manera veraz y actualizada su estado de salud. Este deber es, a su vez, un derecho de los pacientes o usuarios, los cuales tienen derecho a que «quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de la atención primaria como de atención especializada», de forma que así puedan ser atendidos con el máximo nivel de garantías (art. 15 LBRAP)<sup>13</sup>.

Cuando la historia clínica se encuentra digitalizada hablamos de «Historia clínica electrónica» (HCE), entendida como «el registro en formato electrónico de información sobre la salud de cada paciente que puede ayudar a los profesionales de salud en la toma de decisiones y el tratamiento»<sup>14</sup>. El art. 4.7 de la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias<sup>15</sup>, cuando se refiere a los principios para el ejercicio de estas profesiones, dispone que la «historia clínica tenderá a ser soportada en medios electrónicos», lo que hoy en día en nuestro país es ya una realidad plenamente instaurada. Entre sus principales ventajas en relación a la seguridad de los datos pueden citarse la posibilidad de control de los accesos, de forma que sólo aquellos profesionales que estén autorizados podrán acceder a la

---

13 El contenido mínimo de la historia clínica se enumera en el art. 15.2 de la LBRAP.

14 S. FERRER GELABERT, «E-Salud: La tecnología al servicio de la salud», en *E-Salud, autonomía y datos clínicos: Un nuevo paradigma*, Dykinson, S.L., 2021, p. 17.

15 Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias publicada en el «BOE» núm. 280, de 22 de noviembre de 2003.  
Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2003-21340>

misma, y la posibilidad de obtener su trazabilidad, pudiéndose conocer quién accede a qué contenidos, en qué momento, etc.<sup>16</sup>

El Código de Deontología Médica<sup>17</sup> recoge la obligación de anotar en la historia clínica del paciente el medio por el que se ha realizado la consultade telemedicina, además del tratamiento médico pautado y las recomendaciones dadas (art. 80.2). Es decir, si la consulta se ha realizado por medios electrónicos como pueden ser la llamada telefónica, videollamada o a través de un programa de mensajería instantánea, deberá constar en la historia clínica el medio concreto por el que se ha desarrollado la atención médica.

El pasado 24 de abril de 2024, el Parlamento Europeo aprobó, en primera lectura, y tras alcanzar un acuerdo con el Consejo de la Unión Europea<sup>18</sup>, la Propuesta de la Comisión Europea<sup>19</sup> relativa al Reglamento sobre el Espacio Europeo de Datos Sanitarios (PREEDS)<sup>20</sup>. Como resultado de este proceso legislativo, recientemente se ha publicado en el «DOUE» núm. 327, de 5 de marzo de 2025 el Reglamento (UE) 2025/327 del Parlamento Europeo y del

16 J. ETREROS HUERTA, «Historia clínica electrónica», en *El derecho a la protección de datos en la historia clínica y la recera electrónica*, Thomson Reuters, 2009, pp. 186 y 189.

17 La última actualización del actual Código de Deontología Médica fue aprobada por la Asamblea General del Consejo General de Colegios Oficiales de Médicos (CGCOM) en diciembre de 2022, con el objetivo de adaptar el marco ético y deontológico a la nueva realidad social. Entre los aspectos más relevantes, destaca la incorporación en el capítulo XXII de un apartado referente a la «Telemedicina y tecnologías de la información y la comunicación (TIC)» (arts. 80.1 a 84.2).

Además, en el curso de la pandemia COVID-19, la Comisión Central de Deontología médica en España, con fecha 10 de junio de 2020, presentó una Declaración bajo el título «La Telemedicina en el acto médico» en la que abordaba los requisitos deontológicos de la modalidad de consulta médica no presencial, e-consulta o consulta online con el objetivo de guiar a los médicos que se veían obligados a usar las tecnologías para atender a sus pacientes. Entre las cuestiones que se abordan en la Declaración, encontramos el deber de garantizar la intimidad, la confidencialidad y el secreto de los datos clínicos, de los que se pudiera tener conocimiento tanto directa como indirectamente.

En el ámbito de la psicología, donde el incremento progresivo de las enfermedades mentales ha venido acompañado de un exponencial uso de las tecnologías de la información y de la telecomunicación a distancia, el Código Deontológico del Psicólogo (su última actualización tuvo lugar el 12 de diciembre de 2015), sin embargo, no incorpora ninguna declaración en este sentido. Entendemos, por tanto, que sería conveniente una modernización.

18 Acuerdo del Consejo de la UE y el Parlamento Europeo de 18 de marzo de 2024 sobre la PREEDS. Disponible en: <https://www.consilium.europa.eu/media/70909/st07553-en24.pdf>

19 La propuesta de Reglamento de Datos Sanitarios fue presentada en el marco de la Estrategia Europea de Datos por la Comisión Europea el 3 de mayo de 2022. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0197#footnote2>

20 Resolución legislativa del Parlamento Europeo de 24 de abril de 2024 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)) (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)).  
Disponible en: [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331\\_ES.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_ES.pdf)

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 (en adelante, REEDS)<sup>21</sup>. El art. 15 del Reglamento fija como horizonte el 26 de marzo de 2027 para que la Comisión Europea defina las especificaciones técnicas necesarias para la implementación de un formato europeo estandarizado de historias clínicas electrónicas que facilite el intercambio y circulación transfronteriza. Este objetivo resulta fundamental para facilitar la asistencia sanitaria a los ciudadanos en los diferentes países europeos a tenor del aumento de las movilidades transfronterizas y la necesidad de interoperabilidad entre sistemas sanitarios. Está previsto que ese formato sea común, legible por máquina y que sirva para facilitar la transmisión de datos de salud entre distintos sistemas y prestadores de asistencia sanitaria. Los Estados miembros adquieren el compromiso de garantizar que los datos de salud prioritarios se proporcionarán en ese formato, y que los prestadores de salud los aceptarán y podrán leerlos.

Conforme a su considerando primero, el Reglamento tiene como propósito fundamental establecer un marco jurídico y técnico uniforme para la gestión y el intercambio de datos de salud electrónicos en la Unión Europea. Se busca garantizar el acceso de las personas físicas a sus datos de salud personales y fortalecer su control sobre los mismos en el contexto de la asistencia sanitaria. Además, el REEDS promueve el aprovechamiento de dichos datos con fines que trascienden el ámbito individual, permitiendo su utilización en actividades de investigación científica, innovación tecnológica, desarrollo de políticas públicas, preparación y respuesta ante emergencias sanitarias, como pandemias, y mejora de la seguridad de los pacientes. Entre sus objetivos específicos, la norma comunitaria destaca la promoción de la medicina personalizada, la generación de estadísticas oficiales y el apoyo a actividades regulatorias relacionadas con la salud. A través de estos mecanismos, se pretende no solo optimizar la asistencia sanitaria, sino también consolidar un mercado interior eficiente mediante la armonización de estándares para el desarrollo, la comercialización y el uso de sistemas de historia clínica electrónica (HCE).

En lo que se refiere al uso de la telemedicina, el Reglamento (cdo. 28) destaca su creciente importancia como herramienta para mejorar el acceso a la asistencia sanitaria y abordar las desigualdades, especialmente en regiones remotas, mediante el uso de tecnologías digitales. Aunque los Estados miembros conservan la responsabilidad de organizar y regular sus políticas sanitarias, incluidas la telemedicina y los servicios farmacéuticos en línea, estas regulaciones no deben obstaculizar la libre circulación de datos de salud electrónicos necesarios para la prestación de asistencia sanitaria transfronteriza. Conforme al art. 24 del REEDS, dichos Estados miembros podrán ofrecer, a través de la plataforma MiSalud@UE, servicios digitales complementarios que faciliten la telemedicina o salud móvil, además del acceso a

---

21 Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2025-80382>

# RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS DE SALUD EN EL ESPACIO EUROPEO DE DATOS DE SALUD (EEDS)

Un marco normativo cohesionado y sólido relativo a los datos personales de salud es hoy piedra angular del avance de la salud digital y el desarrollo de la medicina personalizada. La reciente creación del Espacio Europeo de Datos de Salud aspira a crear una infraestructura interoperable y segura optimizando la prestación de servicios sanitarios, otorgando al ciudadano el control sobre sus datos electrónicos de salud personales y facilitando su intercambio en la UE.

La presente obra monográfica, fruto de un proyecto TED2021 financiado con fondos europeos del que es IP Raquel Luquin Bergareche, realiza un análisis sistemático en cuatro capítulos de las principales cuestiones que suscita la vigente regulación de protección de datos personales en el campo de la salud, con especial atención al reciente Reglamento (UE) 2025/327, relativo al EEDS de 11 de febrero, vigente desde el 25 de marzo de 2025 con determinados plazos de aplicación según la materia.

Normativa europea de aplicación directa en los Estados miembros que pretende concitar un delicado equilibrio entre la salvaguarda de la privacidad y la confidencialidad como derechos fundamentales de la persona y las exigencias del avance tecnológico y de la investigación médica, configurándose como complementaria de lo dispuesto, entre otras, en el Reglamento (UE) 2016/679, General de Protección de Datos y, en nuestro ordenamiento jurídico, en la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales.

## AUTORES

M.<sup>a</sup> Ángeles Egusquiza Balmaseda, Raquel Luquin Bergareche,  
María Jorqui Azofra y Javier Vidán Peña



Esta publicación forma parte del proyecto de investigación «Contratación de Servicios de Telemedicina: Actualidad y Desafíos Jurídicos» (TED2021-129472B-00/MICINN) financiado por MCIN/AEI/10.13039/501100011033 y por la Unión Europea NextGeneration EU/PRTR.

PVP: 30,00 €  
ISBN: 979-13-7011-094-9



9 791370 110949

OA