Confidencialidad de los datos médicos: marco jurídico-ético y casos prácticos en España/UE. Revisión panorámica

José Luis Pardal-Refoyo

https://doi.org/10.1590/SciELOPreprints.12082

Envíado en: 2025-05-25
Postado en: 2025-06-16 (versión 1)
(AAAA-MM-DD)

Confidencialidad de los datos médicos: marco jurídico-ético y casos prácticos en España/UE. Revisión panorámica

Confidentiality of medical data: legal-ethical framework and practical cases in Spain/EU. Overview

José Luis Pardal-Refoyo
Hospital Universitario de Salamanca. Otorrinolaringología y Cirugía de Cabeza y Cuello. Universidad de Salamanca. Departamento de Cirugía. Facultad de Medicina. Área de Otorrinolaringología. IBSAL. Salamanca. España
https://orcid.org/0000-0002-7462-1606
jlpardal@usal.es

Resumen
Introducción La confidencialidad de los datos médicos de los pacientes es un principio esencial en la asistencia sanitaria, regulado tanto por los marcos legales como éticos de España y de la Unión Europea. Los recientes desarrollos legislativos y los avances tecnológicos han planteado nuevos retos relacionados con la privacidad de los datos, especialmente en lo que respecta a casos reales de incumplimiento por parte de los profesionales sanitarios.
Objetivos Este análisis tuvo como objetivo caracterizar conjuntamente los marcos legales y éticos vigentes que regulan la confidencialidad de los datos médicos de los pacientes en España y Europa, y examinar los casos de sanciones judiciales o administrativas derivadas de incumplimientos por parte de profesionales sanitarios en diversos entornos asistenciales y medios de comunicación.
Método Se realizó un análisis exhaustivo de la literatura utilizando fuentes seleccionadas que incluyeron estudios empíricos, revisiones estadísticas y análisis doctrinales de los marcos legales españoles y europeos. La revisión ha consistido en el análisis de encuestas empíricas sobre conocimientos y comportamientos de los profesionales sanitarios, así como en una revisión sistemática de 201 resoluciones administrativas dictadas por la Agencia Española de Protección de Datos en el sector sanitario entre 2005 y 2018.
Resultados La revisión encontró que el GDPR y la ley española (LOPDGDD) proporcionan bases regulatorias estrictas para el manejo de datos de salud, reforzadas por códigos de ética profesional. Más de la mitad de los profesionales encuestados carecían de conocimiento de las leyes pertinentes, y las infracciones informales eran más frecuentes entre el personal de mayor edad. El análisis detallado de los casos administrativos reveló infracciones como transferencias de datos no autorizadas y pérdidas de medios electrónicos. Pocos estudios incorporaron evidencia legal, ética y empírica, y la mayoría careció de descripciones completas de los casos.
Conclusiones Existe una brecha entre los requisitos legales y éticos existentes y el cumplimiento práctico entre los profesionales de la salud en España. Aunque los marcos regulatorios son sólidos, la evidencia empírica revela incumplimientos persistentes y conocimientos insuficientes. Los análisis integrados que combinan datos legales, éticos y de sanciones son escasos, lo que indica la necesidad de más investigación y medidas institucionales para garantizar la confidencialidad en la gestión de los datos sanitarios.
Palabras clave: confidencialidad de datos médicos; marco legal y ético; RGPD; sanciones administrativas; España; profesionales sanitarios

Summary
Introduction The confidentiality of patients' medical data is an essential principle in healthcare, regulated by both the legal and ethical frameworks of Spain and the European Union. Recent legislative developments and technological advances have posed new challenges related to data privacy, especially about actual cases of non-compliance by healthcare professionals.
Objectives This analysis aimed to jointly characterize the current legal and ethical frameworks that regulate the confidentiality of patients' medical data in Spain and Europe, and to examine cases of judicial or administrative sanctions derived from non-compliance by health professionals in various healthcare settings and the media.
Method An exhaustive analysis of the literature was carried out using selected sources that included empirical studies, statistical reviews and doctrinal analyses of the Spanish and European legal frameworks. The review consisted of the analysis of empirical surveys on the knowledge and behaviour of healthcare professionals, as well as a systematic review of 201 administrative decisions issued by the Spanish Data Protection Agency in the healthcare sector between 2005 and 2018.
Results The review found that the GDPR and the Spanish law (LOPDGDD) provide strict regulatory bases for the handling of health data, reinforced by codes of professional ethics. More than half of the professionals surveyed lacked knowledge of the relevant laws, and informal violations were more frequent among older staff. Detailed analysis of administrative cases revealed violations such as unauthorized data transfers and loss of electronic media. Few studies incorporated legal, ethical, and empirical evidence, and most lacked complete case descriptions.
Conclusions There is a gap between existing legal and ethical requirements and practical compliance among health professionals in Spain. Although regulatory frameworks are robust, empirical evidence reveals persistent non-compliance and insufficient knowledge. Integrated analyses that combine legal, ethical and sanctions data are scarce, indicating the need for more research and institutional measures to ensure confidentiality in the management of health data.
Keywords: confidentiality of medical data; legal and ethical framework; GDPR; administrative sanctions; Spain; health professionals

Introducción

La confidencialidad de los datos médicos de los pacientes constituye un principio fundamental de la práctica sanitaria y un derecho esencial protegido tanto por marcos legales como éticos en España y la Unión Europea [1]. El desarrollo del Reglamento General de Protección de Datos (GDPR) y su adaptación en la legislación española a través de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) han reforzado la regulación de los datos de salud como categoría especialmente protegida, exigiendo bases legales estrictas para su tratamiento y estableciendo obligaciones de notificación frente a posibles brechas [2]. Este marco normativo se complementa con la Ley 41/2002 y los códigos deontológicos de las profesiones sanitarias, que imponen el deber de confidencialidad y sancionan su incumplimiento [3].

A pesar de la existencia de un entramado regulatorio firme, distintas investigaciones han evidenciado un desconocimiento significativo de la normativa aplicable por parte de los profesionales sanitarios, así como la persistencia de infracciones informales y casos documentados de vulneraciones de la confidencialidad, tanto en soportes físicos como electrónicos [1,4]. Asimismo, los organismos reguladores y tribunales han impuesto sanciones administrativas y judiciales ante incumplimientos, lo que subraya la relevancia y actualidad del problema [4].

El objetivo de esta investigación está en analizar de manera conjunta el marco legal y ético actual de la confidencialidad de los datos médicos en España y Europa, así como identificar y describir ejemplos de casos judicializados o sancionados administrativamente como consecuencia de la vulneración de dicha confidencialidad por parte de profesionales sanitarios.

Métodos

Se diseñó una revisión sistemática de alcance *(scoping review)* conforme a las directrices PRISMA (https://www.prisma-statement.org/) para analizar de manera conjunta el marco legal y ético de la confidencialidad de los datos médicos en España y Europa, así como la existencia de casos judicializados o sancionados administrativamente por incumplimiento de dicha confidencialidad.

Las estrategias de búsqueda incluyeron consultas en las bases de datos PubMed (https://pubmed.ncbi.nlm.nih.gov/), Scopus (https://www.scopus.com/), Google Scholar (https://scholar.google.com/), Dialnet (https://dialnet.unirioja.es/), y Web of Science (https://www.webofscience.com/), en los idiomas inglés, español, francés, italiano y alemán. La estrategia de búsqueda concreta empleó los siguientes términos y operadores booleanos: *(“confidentiality” OR “data protection” OR “medical data” OR “health data” OR “GDPR” OR “LOPDGDD” OR “patient privacy”) AND (“Spain” OR “Europe” OR “EU”) AND (“legal” OR “ethical” OR “deontological” OR “law” OR “code of ethics”) AND (“sanction” OR “judicial case” OR “AEPD” OR “court ruling” OR “professional misconduct”)*.

Los criterios de inclusión fueron: estudios, artículos o informes que analizaran de forma conjunta el marco legal y ético/deontológico de la confidencialidad de datos médicos en España y/o Europa; que incluyeran ejemplos o estudios de casos judicializados o sancionados administrativamente en cualquier ámbito asistencial y soporte. Se excluyeron documentos que abordaran únicamente aspectos técnicos sin integrar perspectiva legal/ética, que no incluyeran casos reales, o que no se centraran en el contexto español o europeo.

El proceso de selección de publicaciones consistió en una primera criba por títulos y resúmenes, posteriormente análisis en texto completo. La aplicación Undermind (https://www.undermind.ai/) fue utilizada para el cribado asistido por inteligencia artificial en la fase de recuperación y preselección de artículos, así como en la extracción semiautomatizada de variables clave y resúmenes analíticos.

Se analizaron estudios empíricos y revisiones doctrinales. Para variables cuantitativas, se obtuvo el volumen de resoluciones administrativas estudiadas (201 casos de la AEPD en el sector sanitario español entre 2005 y 2018). Las variables clave incluyeron: tipo de marco normativo (legal, ético),

conocimientos y actitudes profesionales, frecuencia de infracciones, tipo de sanciones (judiciales/administrativas), cuantía de las multas y ámbito asistencial implicado. Se utilizaron procedimientos de tabulación y estadística descriptivas (frecuencias y porcentajes) para el análisis de los datos extraídos de las fuentes seleccionadas [1,2,3].

No se emplearon pruebas estadísticas inferenciales ni análisis multivariantes debido a la naturaleza descriptiva y exploratoria del estudio.

Resultados

El diagrama PRISMA de la Figura 1 refleja que, de los 227 artículos identificados en la búsqueda inicial, tras la revisión por títulos y resúmenes se seleccionaron 18, y finalmente tras la lectura y aplicación de los criterios de inclusión y exclusión, solo 3 artículos cumplieron con todos los criterios requeridos para el análisis integrado y la aportación empírica de casos sancionadores o judicializados [1,2,3].

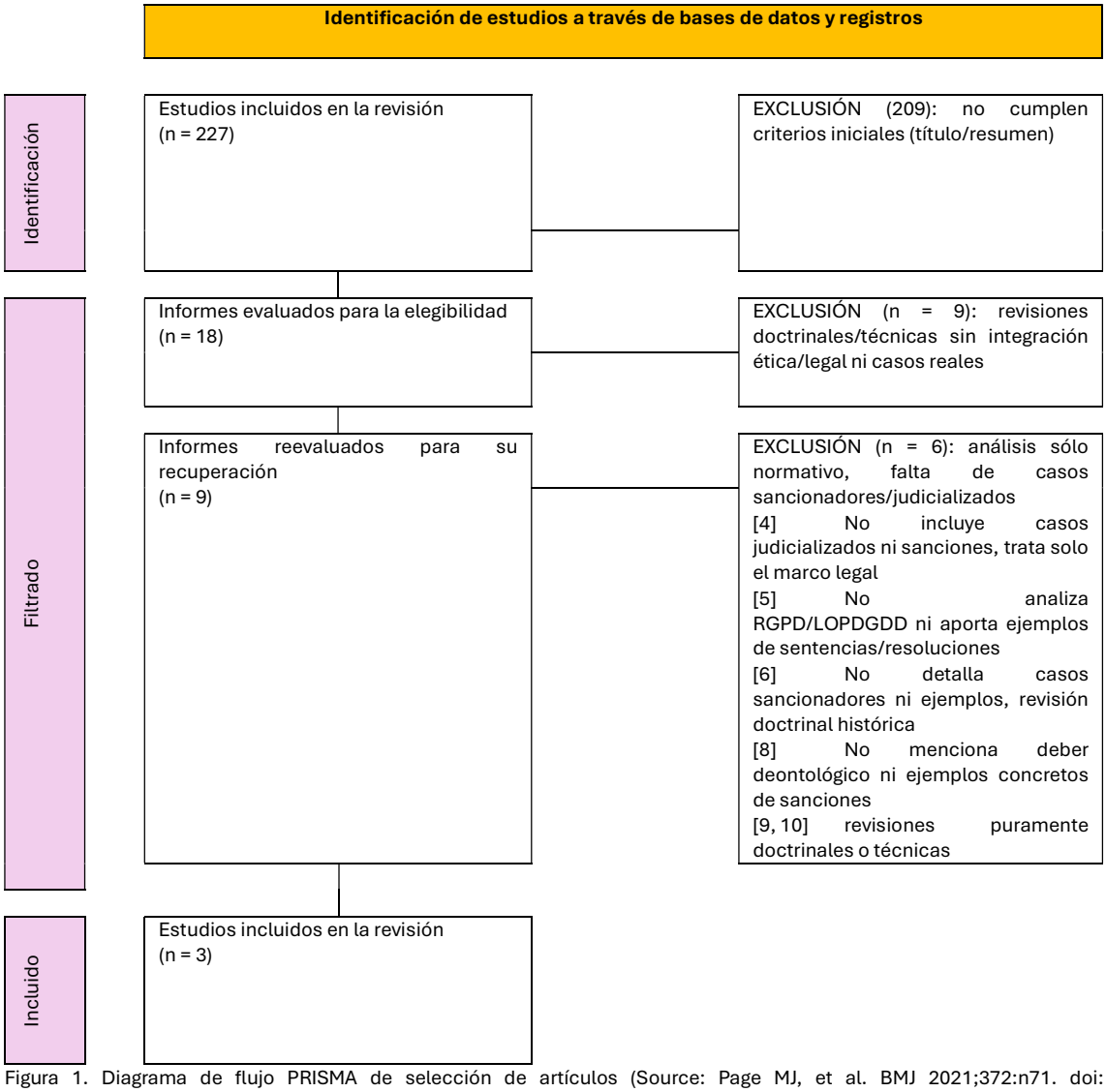

Figura 1. Diagrama de flujo PRISMA de selección de artículos (Source: Page MJ, et al. BMJ 2021;372:n71. doi: 10.1136/bmj.n71)

La Tabla 1 recoge las principales características y resultados de los artículos seleccionados.

No se identificaron metaanálisis ni análisis de heterogeneidad estadística debido a la naturaleza cualitativa y descriptiva de los resultados. Los resultados cuantitativos principales proceden de estudios descriptivos y de análisis retrospectivo de resoluciones sancionadoras.

Tabla 1. Características y resultados clave de los estudios incluidos

Referencia	Alcance legal/ético	Ejemplos reales/casos	Ámbito asistencial	Soporte	Resultados cuantitativos / principales hallazgos
Iraburu et al. 2006 [1]	Legal y ético integrado	Sentencias judiciales	Hospitalario (Pamplona)	Papel/electrónico	58,1% de profesionales desconoce la legislación; infracciones informales hasta 51,9% (>50 años); sentencias ejemplares incluidas
Fernández 2015 [2]	Legal y ético integrado	Caso sancionado informático	Relación clínica genérica	Papel/electrónico	Explica protección por LOPD, Ley 41/2002, Directiva europea; sentencia a entidad por fichero sin base legal y consentimiento
Palomo 2020 [3]	Foco legal/sancionador	Resoluciones administrativas	Multinivel (sector sanitario español)	Electrónico	201 resoluciones AEPD analizadas (2005–2018); sanciones ≥2.000 €; tipos incluyen pérdida de USB, cesiones forzadas, accesos indebidos

Riesgo de sesgo y calidad de la evidencia El análisis de sesgo se muestra en la Tabla 2, utilizando la escala JADAD adaptada para estudios observacionales y revisión documental.

Tabla 2. Análisis de sesgo de los estudios incluidos

Referencia	Selección	Desempeño	Detección	Declaración de resultados	Otros sesgos	Valoración global
Iraburu et al. 2006 [1]	Baja	Moderado	Moderado	Baja	Moderado	Moderado
Fernández 2015 [2]	Moderado	Moderado	Moderado	Alta	Moderado	Moderado
Palomo 2020 [3]	Baja	Moderado	Moderado	Alta	Moderado	Moderado

Las limitaciones principales incluyen la falta de integración plena entre enfoques ético, legal y casos sancionados en todos los estudios, el diseño fundamentalmente descriptivo, y la ausencia de comparaciones multivariante o inferencias estadísticas avanzadas. Según la escala GRADE, el nivel de evidencia fue considerado “moderado” y la fuerza de la recomendación limitada principalmente por la calidad descriptiva y la falta de heterogeneidad entre fuentes.

En síntesis, los resultados muestran importantes lagunas de conocimiento, elevada prevalencia de desconocimiento normativo entre los profesionales, y la existencia documentada de sanciones judiciales y administrativas por incumplimientos en el ámbito sanitario español (ver Tabla 1).

Discusión

Los resultados obtenidos ponen de manifiesto la existencia de una brecha significativa entre el marco legal y ético que regula la confidencialidad de los datos médicos en España y Europa y su implementación real en la práctica cotidiana de los profesionales sanitarios [1,2]. A pesar de la presencia del RGPD, la LOPDGDD y los códigos deontológicos que imponen obligaciones estrictas de secreto profesional, persiste un desconocimiento normativo relevante entre los profesionales y se documentan infracciones informales y casos de vulneración de la confidencialidad tanto en historias clínicas en papel como electrónicas [1].

Según la literatura revisada, los incumplimientos más frecuentes por parte de los médicos en materia de confidencialidad de los datos médicos en España son los siguientes:

1. Desconocimiento normativo y prácticas informales de divulgación

- Falta de conocimiento legal: En el estudio empírico realizado en el Hospital Virgen del Camino de Pamplona, el 58,1 % de los profesionales sanitarios encuestados no conocían ninguna de las leyes relevantes sobre confidencialidad y protección de datos [1].
- Infracciones informales: Se observa un aumento de prácticas informales de vulneración del secreto profesional con la edad de los médicos; el 51,9 % de los profesionales mayores de 50 años reconoce incurrir en este tipo de infracciones [1].

2. Comunicación inadecuada de datos personales

- Divulgación a terceros sin consentimiento: Se documenta, por ejemplo, un caso en el que una médico residente fue condenada por el Tribunal Supremo por compartir datos de una paciente con su madre sin autorización [1].
- Revelación de información confidencial fuera del ámbito permitido: El mismo estudio cita la existencia de sentencias por acceso o comunicación indebida de datos médicos, y denuncia la persistencia de estas prácticas [1].

3. Gestión deficiente de soportes y documentos

- Pérdida de dispositivos con información sensible: El análisis de resoluciones de la AEPD revela casos concretos como la pérdida de soportes USB que contenían imágenes de pacientes [3].
- Obligación de firmar cesiones de datos de forma abusiva: Se describen situaciones en servicios de urgencias en las que se obliga a los pacientes a firmar cláusulas de cesión de datos sin la base jurídica suficiente [3].

4. Falta de medidas técnicas y organizativas de seguridad

- Accesos indebidos a historias clínicas: Los trabajos, basados en resoluciones administrativas, recogen situaciones en las que profesionales acceden a historias clínicas sin justificación asistencial o autorización expresa [3].
- Déficit en controles de acceso, registros y auditorías: Se señala la insuficiencia de políticas institucionales rigurosas (por ejemplo, falta de logs y controles periódicos) que permitan detectar y prevenir intrusiones no autorizadas [1,10].

En resumen, la literatura identifica como incumplimientos más frecuentes: el desconocimiento de la normativa, la comunicación indebida de datos a terceros, la gestión negligente de dispositivos o documentos con información sensible, y la insuficiencia de medidas de seguridad organizativas o técnicas por parte de los médicos y centros sanitarios [1][3][10].

El análisis de casos sancionados tanto a nivel judicial como administrativo revela que los incumplimientos se deben en muchos casos a errores procedimentales y a la falta de políticas institucionales de formación y control efectivo [3]. Estos hallazgos coinciden con estudios previos que señalan la complejidad de la adaptación operativa de los marcos legales y la necesidad de integrar prácticas continuas de educación y actualización regulatoria en el sector sanitario [1,3]. Además, destaca la escasez de estudios que integren de manera holística los diferentes aspectos del problema: dimensión legal, ética y sancionadora, así como la limitada variedad de contextos asistenciales y soportes documentales analizados en la literatura disponible.

Desde el punto de vista práctico, estos resultados sugieren la necesidad de implementar programas de formación sistemática sobre confidencialidad y protección de datos entre los profesionales, así como la adopción de sistemas de monitorización, auditoría y mejora continua en los centros asistenciales. Para la investigación futura, sería relevante el desarrollo de estudios multicéntricos y longitudinales que integren métodos cuantitativos y cualitativos, así como la comparación entre

distintos entornos asistenciales, tipos de soporte y países europeos, para identificar factores facilitadores y barreras en la efectiva protección de la confidencialidad.

Entre las limitaciones principales del presente análisis se encuentran el reducido número de estudios que cumplen los criterios estrictos de inclusión, el carácter esencialmente descriptivo de los trabajos seleccionados y la escasa disponibilidad de datos sobre la magnitud y el impacto real de las sanciones impuestas [1,2,3]. Adicionalmente, la revisión se vio condicionada por la falta de literatura reciente que trate de modo integrado el marco normativo, la deontología y los ejemplos empíricos de sanciones, lo que dificulta una evaluación exhaustiva de la situación actual.

En conclusión, aunque el diseño normativo es avanzado, la brecha entre teoría y práctica sigue siendo una cuestión crítica, y existe una necesidad evidente de estudios que profundicen en la integración de los enfoques legal, ético y conductual para promover una protección efectiva y sostenible de la confidencialidad de los datos médicos en Europa y España.

Conclusiones

1. Existe una notable brecha entre el marco legal y ético que rige la confidencialidad de los datos médicos en España y Europa y su implementación efectiva en la práctica clínica.
2. Una proporción significativa de profesionales de la salud demuestra una conciencia y un conocimiento insuficientes de las regulaciones aplicables, lo que contribuye a las violaciones informales persistentes de la confidencialidad.
3. Las sanciones judiciales y administrativas documentadas se deben principalmente a errores de procedimiento y políticas institucionales inadecuadas en materia de protección de datos y formación del personal.
4. La literatura existente rara vez integra análisis legales, éticos y basados en casos, lo que destaca la necesidad de una investigación integral y multidisciplinaria en esta área.
5. Se requiere una mayor educación institucional, procesos de auditoría sistemáticos y actualizaciones regulatorias continuas para fortalecer el cumplimiento de los estándares de confidencialidad en la atención médica.
6. Se justifica la realización de más investigaciones para cerrar la brecha entre los requisitos normativos y las prácticas del mundo real, en particular a través de estudios multicéntricos y longitudinales en diversos entornos sanitarios.

Declaración de conflicto de intereses

El autor declara que no tiene conflictos de intereses respecto a este manuscrito

Bibliografía

1. Iraburu Elizondo M, Chamorro Camazón J, de Pedro Montalbán MT. Conocimientos, comportamientos y opiniones de los profesionales sanitarios de un hospital en relación a la confidencialidad. Anales Del Sistema Sanitario De Navarra. 2006;29(3):357-366. (https://doi.org/10.15581/011.1572).
2. Fernández Ruiz-Gálvez E. Intimidad y confidencialidad en la relación clínica. Persona y Derecho. 2015;69:53-101. (https://doi.org/10.15581/011.1572).
3. Palomo Navarro M. Infracciones de la Ley Orgánica de Protección de Datos en el ámbito sanitario. Descripción estadística de las infracciones. Revista De Bioética Y Derecho. 2020;50:385-406. (https://doi.org/10.1344/rbd2020.50.29784).

4. Pérez MM. La necesidad de una ley de protección de datos en salud. Bioderecho.es. 2019;8. (https://doi.org/10.6018/bioderecho.389951).

5. Sánchez M. Protección de datos personales a través del secreto profesional en el ámbito de la administración sanitaria local. Revista De Estudios De La Administración Local Y Autonómica. 2011;300-301. (https://doi.org/10.24965/reala.vi300-301.9301).

6. Kress A. La Unión Europea como modelo de protección de datos en eHealth, su influencia y barreras a la convergencia. Universitat Politècnica de Catalunya. 2017. (http://hdl.handle.net/2117/108229).

7. Rodríguez Ayuso JF. Estado de alarma y protección de la privacidad en tiempos de pandemia: licitud del tratamiento de categorías especiales de datos. Revista de Derecho Político. 2021;110:299-318. (https://doi.org/10.1344/rbd2020.50.31251).

8. Rodríguez Ayuso JF. Control de la privacidad por parte de las autoridades sanitarias ante situaciones de emergencia. Revista De Bioética Y Derecho. 2020;50:353-368. (https://doi.org/10.1344/rbd2020.50.31251).

9. Berrocal Lanzarot AI. La protección de datos relativos a la salud y la historia clínica en la normativa española y europea. Revista de la Escuela de Medicina Legal. 2012;18:11-44. (http://dx.doi.org/10.5209/rev_REML.2011.v18.38172).

10. Casanova Asencio AS. Mecanismos de prevención del acceso indebido a la historia clínica por parte del personal sanitario y nueva legislación de protección de datos. Bioderecho.es. 2019;8. (https://doi.org/10.6018/bioderecho.389951).

Este preprint fue presentado bajo las siguientes condiciones:

- Los autores declaran que son conscientes de que son los únicos responsables del contenido del preprint y que el depósito en SciELO Preprints no significa ningún compromiso por parte de SciELO, excepto su preservación y difusión.
- Los autores declaran que se obtuvieron los términos necesarios del consentimiento libre e informado de los participantes o pacientes en la investigación y se describen en el manuscrito, cuando corresponde.
- Los autores declaran que la preparación del manuscrito siguió las normas éticas de comunicación científica.
- Los autores declaran que los datos, las aplicaciones y otros contenidos subyacentes al manuscrito están referenciados.
- El manuscrito depositado está en formato PDF.
- Los autores declaran que la investigación que dio origen al manuscrito siguió buenas prácticas éticas y que las aprobaciones necesarias de los comités de ética de investigación, cuando corresponda, se describen en el manuscrito.
- Los autores declaran que una vez que un manuscrito es postado en el servidor SciELO Preprints, sólo puede ser retirado mediante solicitud a la Secretaría Editorial deSciELO Preprints, que publicará un aviso de retracción en su lugar.
- Los autores aceptan que el manuscrito aprobado esté disponible bajo licencia Creative Commons CC-BY.
- El autor que presenta el manuscrito declara que las contribuciones de todos los autores y la declaración de conflicto de intereses se incluyen explícitamente y en secciones específicas del manuscrito.
- Los autores declaran que el manuscrito no fue depositado y/o previamente puesto a disposición en otro servidor de preprints o publicado en una revista.
- Si el manuscrito está siendo evaluado o siendo preparando para su publicación pero aún no ha sido publicado por una revista, los autores declaran que han recibido autorización de la revista para hacer este depósito.
- El autor que envía el manuscrito declara que todos los autores del mismo están de acuerdo con el envío a SciELO Preprints.