CODEPA

Colegio Oficial de Enfermería del Principado de Asturias

OBSERVACIONES DEL COLEGIO OFICIAL DE ENFERMERÍA DEL PRINCIPADO DE ASTURIAS AL TRÁMITE DE CONSULTA PÚBLICA PREVIA SOBRE EL ANTEPROYECTO DE LEY DE SALUD DIGITAL POR EL QUE SE ADAPTA AL ORDENAMIENTO NACIONAL 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, Y POR EL QUE SE MODIFICAN LA DIRECTIVA 2011/24/UE Y EL REGLAMENTO (UE) 2024/284 Y SE REGULA LA HISTORIA CLÍNICA DIGITAL INTEROPERABLE NACIONAL Y EL USO DE TECNOLOGÍAS DIGITALES EN LA ASISTENCIA SANITARIA.

ESCRITO DE OBSERVACIONES

D. Esteban Gómez Suárez, en mi condición de Presidente del COLEGIO OFICIAL DE ENFERMERÍA DEL PRINCIPADO DE ASTURIAS (en adelante, CODEPA), ante el MINISTERIO DE SANIDAD, al amparo de lo dispuesto en los artículos 4.2 y 133.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, por vía electrónica COMPAREZCO y DIGO:

LEGITIMACIÓN

Que se ha acordado por el Ministerio de Sanidad la apertura de Consulta Pública previa sobre el Anteproyecto de Ley de Salud Digital por el que se adapta al ordenamiento nacional 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, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/284 y se regula la historia clínica digital interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria, al objeto de recabar la opinión de las personas y organizaciones más representativas potencialmente afectados por la futura norma sobre los problemas que se pretenden solucionar con la

iniciativa, la necesidad y oportunidad de su aprobación, los objetivos y las posibles soluciones alternativas regulatorias y no regulatorias.

La consulta pública estará abierta entre el 22 de septiembre y el 20 de octubre de 2025.

Que están legitimadas para efectuar las alegaciones que se estimen oportunas sobre el contenido de la norma en tramitación las organizaciones o asociaciones reconocidas por ley que agrupen o representen a las personas cuyos derechos o intereses legítimos se vieren afectados por la misma y cuyos fines guarden relación directa con su objeto. Así, el CODEPA ostenta la representación institucional de las más de 8.400 enfermeras y enfermeros colegiadas en el Principado de Asturias, de acuerdo con lo dispuesto en la Ley 2/1974 sobre Colegios Profesionales.

Que el CODEPA ha hecho consulta pública a colegiados y sociedades científicas con el fin de obtener criterios profesionales y técnicos para disponer de una argumentación más fundada.

En virtud de lo anterior, mediante el presente escrito, vengo a realizar en el trámite de consulta pública, las siguientes observaciones al Anteproyecto de Ley de Salud Digital por el que se adapta al ordenamiento nacional 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, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/284 y se regula la historia clínica digital interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria, con carácter previo a la elaboración de la disposición de referencia.

PROBLEMAS QUE SE PRETENDEN SOLUCIONAR CON LA NORMA

El Colegio de Enfermería de Asturias valora positivamente la iniciativa de adaptar el ordenamiento jurídico español al Reglamento (UE) 2025/327 relativo al Espacio Europeo de Datos de Salud (EEDS), que busca fortalecer los derechos de las personas sobre sus datos de salud y fomentar la interoperabilidad y el uso seguro de tecnologías sanitarias digitales.

Sin embargo, con el fin de asegurar que la norma futura sea operativa, garantista y proteja tanto los derechos de los pacientes como la integridad del ejercicio

profesional, se formulan las siguientes observaciones, estructuradas según los principales retos que el Anteproyecto pretende solucionar.

1) Observaciones transversales

1. **Calendario desplegado y fases de implementación claras**
   El Anteproyecto debe incluir un cronograma normativo claro, con fases de pilotaje, adaptaciones progresivas, plazos de cumplimiento y mecanismos de reporte intermedios. Sin esto, hay riesgo de discrepancias entre comunidades autónomas en la velocidad y calidad de implementación.
2. **Evaluación de costes y recursos**
   Se debe exigir al Ministerio que acompañe la ley con un estimado de costes y necesidades de recursos (tecnológicos, humanos, capacitación) que las comunidades autónomas deberán asumir. Debe incluirse una transferencia presupuestaria estatal para ayudar a las regiones con menos posibilidades económicas.
3. **Participación de profesionales en el diseño**
   Durante el despliegue y el diseño técnico de los sistemas, los colegios profesionales (como el de enfermería) deben tener participación activa (comités técnicos, grupos de trabajo) para asegurar que las soluciones digitales respondan a la realidad práctica del ejercicio profesional, eviten cargas administrativas excesivas y respeten la seguridad clínica.
4. **Responsabilidad legal y régimen sancionador**
   La ley debe prever un régimen sancionador proporcional pero efectivo ante incumplimientos graves –por ejemplo, revelar datos confidentes, denegar acceso injustificado, uso indebido de IA, fallos sistemáticos de interoperabilidad– con responsabilidades administrativas, civiles y, en su caso, penales.
5. **Evaluación posterior y mecanismo de revisión**
   Establecer un mecanismo de revisión de la ley (por ejemplo, evaluación a los 3 y 5 años) para ajustar sus disposiciones, corregir deficiencias, adaptarse a avances tecnológicos y recoger lecciones prácticas.
6. **Compatibilidad con normativa europea de IA y protección de datos**
   La futura ley debe asegurar plena armonía con la Ley Europea de Inteligencia Artificial (cuando esté en vigor) y con el RGPD, evitando lagunas legales. No debe crear obligaciones contradictorias o desalineadas con estos marcos supranacionales.

7. **Protección de la privacidad por diseño ("privacy by design")**
   La ley debe exigir que todos los desarrollos tecnológicos en salud adopten principios de privacidad desde el diseño y por defecto (minimización de datos, cifrado extremo, anonimización/seudonimización, limitación de accesos, segmentación).

2) Derechos de las personas y obligaciones de las administraciones y prestadores privados

Claridad normativa sobre responsabilidades competenciales

El Anteproyecto debe incluir un **articulado explícito** que distribuya claramente las responsabilidades entre Estado, comunidades autónomas y prestadores privados en cuanto al ejercicio de los derechos del Reglamento EEDS (acceso, portabilidad, rectificación, supresión, limitación, etc.). De otro modo, se corre el riesgo de lagunas o incumplimientos locales en determinadas comunidades autónomas.

Aplicación uniforme al sector privado

Debe precisarse que todas las obligaciones que impone el Reglamento EEDS (y las que incorporará esta ley nacional) serán aplicables **sin distinción**, tanto a prestadores públicos como privados, plataformas de salud digitales, mutuas, clínicas privadas o cualquier entidad que gestione datos de salud. Ello es esencial para evitar desigualdades en el acceso del paciente a su información sanitaria.

Interoperabilidad obligatoria y certificación de sistemas HCE

El texto legal debe contemplar que los sistemas de historia clínica electrónica (HCE) utilizados por prestadores (tanto públicos como privados) estén sometidos a un **mecanismo de certificación o acreditación de cumplimiento de estándares de interoperabilidad, seguridad y calidad**, con sanciones disuasorias en caso de incumplimiento, para garantizar que los derechos de los usuarios sean efectivos.

Mecanismos de supervisión y control

Se debe dotar a la autoridad nacional de salud digital y a las autoridades autonómicas correspondientes de competencias inspectoras y sancionadoras

para verificar que los prestadores (públicos o privados) cumplan con sus obligaciones (por ejemplo, plazos de respuesta de acceso o portabilidad, registros de acceso a datos, seguridad, trazabilidad, etc.). Es necesario que los derechos no queden en meras declaraciones de principio sin medios efectivos de exigibilidad.

Acceso gradual con derechos provisionales

Dado que la implantación plena del EEDS se realizará por fases (por ejemplo, algunas categorías prioritarias de datos en 2029 y 2031), el Anteproyecto debe prever mecanismos de transición que aseguren derechos "mínimos" desde el inicio (por ejemplo, acceso básico a historia clínica electrónica, recetas, informes clínicos). No debe esperarse la plena interoperabilidad para que el paciente tenga algún acceso.

3) Gobernanza del uso primario de los datos (asistencia sanitaria)

Autoridades de las comunidades autónomas de salud digital con competencias reales

Las autoridades de las comunidades autónomas de salud digital deben tener competencias definidas y recursos adecuados (legales, técnicos y financieros) para coordinar el uso primario dentro de su comunidad, garantizando el cumplimiento del Reglamento EEDS. No basta con nombrarlas: debe desplegarse un régimen operativo con estructuras técnicas y funciones claras.

Coordinación efectiva con la autoridad nacional

La autoridad nacional de salud digital (órgano representante de España ante el EEDS) debe tener atribuciones explícitas de coordinación, supervisión y mediación cuando surjan conflictos o discrepancias entre comunidades autónomas, especialmente en movilidad de pacientes, interoperabilidad transfronteriza y ejercicio del derecho de portabilidad/transmisión de datos.

Régimen de conflicto y resolución de discrepancias

Debe contemplarse un mecanismo de resolución de conflictos entre comunidades autónomas sobre aspectos como prioridades de intercambio de datos, establecimiento de estándares o criterios de exclusión, con intervención

de la autoridad nacional o un órgano arbitral, para evitar que las comunidades puedan obstaculizar la aplicación del EEDS por decisiones locales.

Financiación y apoyo técnico

Se debe incorporar una disposición que garantice que las comunidades autónomas cuenten con recursos suficientes (financieros, humanos y tecnológicos) para asumir las responsabilidades de salud digital que se le asignen, sin que ello suponga una carga desproporcionada. Además, la autoridad nacional debe ofrecer apoyo técnico, capacitación, guías técnicas, asesoría y auditorías periódicas.

Transparencia y participación

La autoridad nacional y las autoridades autonómicas deben rendir cuentas públicamente (por ejemplo, mediante informes anuales) sobre la implementación del uso primario, indicadores de interoperabilidad, incidencias, incumplimientos y reclamaciones de usuarios.

4) Gobernanza del uso secundario de datos de salud

Órganos de acceso a datos con independencia funcional

Los organismos autonómicos de acceso a datos de salud (y el organismo nacional) deben estar dotados de autonomía funcional, independencia técnica y garantías de transparencia suficientes para evaluar, autorizar, supervisar y revocar permisos de acceso secundario a datos. No deben depender de las autoridades sanitarias operativas para evitar conflictos de interés.

Participación de representaciones sociales y expertos

En los órganos de gobernanza del uso secundario debe preverse la participación de representantes de pacientes, profesionales sanitarios, bioética, expertos en protección de datos y de la administración, para equilibrar intereses y asegurar que las decisiones de acceso se adopten con criterio plural y no exclusivamente burocrático.

Criterios públicos, predecibles y motivados para autorización de accesos

Los permisos que otorgue el organismo de acceso a datos deben basarse en criterios objetivos, públicos y motivados (por ejemplo, relevancia científica, seguridad, proporcionalidad, minimización) y estar sujetos a recurso o apelación administrativa.

Control del cumplimiento por los tenedores de datos

Debe establecerse un régimen de supervisión, auditoría y sanciones para los tenedores de datos (prestadores, instituciones, entidades privadas) que incumplan obligaciones de disponibilización de datos, calidad, anonimización/seudonimización, plazos de respuesta, trazabilidad, etc. Esto es clave para que el uso secundario no quede en meras declaraciones sin cumplimiento real.

Protección reforzada de datos sensibles y poblaciones vulnerables

En aplicaciones de uso secundario de datos sensibles (por ejemplo, genómicos, datos de salud mental, biomarcadores) y cuando afecten grupos vulnerables (niños, personas con discapacidad, pacientes con problemas de salud mental, etc.), se deben imponer requisitos de evaluación ética, consentimiento informado reforzado, comités de ética y mayor nivel de anonimización, o bloqueo de acceso salvo justificación muy estricta.

Transparencia de resultados y rendición de cuentas

Los resultados derivados del uso secundario de datos (por ejemplo, publicaciones científicas, algoritmos, modelos predictivos) deben hacerse públicos, identificando la fuente de datos y, en la medida de lo posible, permitiendo auditoría independiente de su calidad, con plazos y obligaciones claras (por ejemplo, publicación en 18 meses, revisable por razones justificadas).

Régimen transitorio y fases de madurez

Dado que el uso secundario de datos es complejo y exige madurez técnica, el Anteproyecto debería prever una fase piloto, con casos autorizados limitados al principio, evaluación progresiva, indicadores formativos y mecanismos de aprendizaje antes del despliegue generalizado.

5) Igualdad en el acceso, interoperabilidad y calidad de la historia clínica digital.

Derecho universal a la historia clínica interoperable

Debe garantizarse que todas las personas, con independencia de si utilizan servicios públicos o privados, tengan acceso a su historia clínica digital interoperable. Esto exige que el Anteproyecto contemple obligaciones de conexión al sistema nacional de interoperabilidad para los prestadores privados que presten servicios sanitarios.

Calidad mínima de datos y estándares comunes

Debe establecerse un catálogo mínimo obligatorio de datos, con estándares estructurados (vocabularios clínicos estandarizados, terminologías compartidas, codificación interoperable, metadatos) que aseguren que los datos recabados por distintos sistemas sean utilizables y comparables. La falta de estandarización socava la interoperabilidad real.

Mecanismo de garantía de calidad y auditoría

Debe definirse un sistema de auditorías periódicas de calidad de datos (consistencia, completitud, integridad, actualizaciones, verificaciones) para los sistemas HCE en uso. El incumplimiento de estándares mínimos debería acarrear sanciones o restricciones.

Protección del profesional y fiabilidad clínica

Debe contemplarse que los profesionales sanitarios puedan advertir y corregir errores, discrepancias o datos incorrectos en la historia clínica digital (por ejemplo, módulo de "disconformidad" o "nota profesional"). También debe especificarse que los prestadores no serán responsables de omisiones que resulten del exceso de restricciones impuestas por el usuario en el intercambio de datos (como el bloqueo parcial) cuando esto comprometa la calidad asistencial.

Accesibilidad y usabilidad de la historia digital

Los portales o aplicaciones de acceso del paciente y profesionales deben cumplir criterios de usabilidad, accesibilidad (para personas con discapacidad) y

seguridad. Debe establecerse que estos servicios sean gratuitos, de fácil uso y disponibles de forma efectiva y continua.

6) Marco regulatorio del uso de tecnologías digitales, IA, biometría y neurotecnologías.

Principio de "explicabilidad" y supervisión humana

Las aplicaciones de inteligencia artificial usadas en el ámbito sanitario deben garantizar un nivel adecuado de explicabilidad —es decir, que las decisiones que afecten a una persona puedan entenderse y explicarse— y siempre estar bajo supervisión o validación humana. No debe permitirse que decisiones clínicas relevantes sean tomadas exclusivamente por sistemas opacos.

Evaluaciones de impacto ético, riesgo y bias

Antes de su despliegue, las tecnologías digitales (IA, biometría, algoritmos predictivos) deben ser sometidas a evaluaciones de impacto ético, de sesgos (bias), y riesgos en protección de datos, con requisitos mínimos que deben estar recogidos en la ley. Estas evaluaciones deben ser revisadas por comités independientes y disponibles públicamente.

Consentimiento informado y derecho a oposición

Para el uso de tecnologías digitales sensibles (por ejemplo, biometría facial para identificación, neurotecnologías que puedan alterar percepción o comportamiento), debe requerirse un consentimiento informado específico, claro y separable, y debe garantizarse el derecho de oposición sin penalización alguna en el acceso a la asistencia sanitaria tradicional.

Limitaciones a usos proactivos o predictivos automatizados

Se debe regular estrictamente la utilización de sistemas predictivos automáticos (por ejemplo, para perfiles de riesgo, alertas clínicas anticipadas) que puedan condicionar decisiones asistenciales o discriminar pacientes. Es imprescindible que dichos sistemas cuenten con salvaguardas —por ejemplo, umbrales de confianza, revisión humana, auditorías periódicas, vigilancia regulatoria.

Protección frente a manipulación o alteración

En el caso de neurotecnologías o interfaces cerebro-máquina que puedan influir en percepción, comportamiento o estados cognitivos, debe establecerse un régimen de autorización previa, vigilancia especial, responsabilidad penal y civil en caso de daños, así como garantías de reversibilidad, cuando esto sea técnicamente factible.

Transparencia algorítmica pública

Los algoritmos que se usen en ámbito asistencial (o como apoyo al diagnóstico, recomendación terapéutica, priorización de recursos) deben ser objeto de registro público, con una ficha técnica accesible (propósito, variables usadas, sesgos conocidos, resultados de validación) para que profesionales y pacientes puedan conocer sus límites y riesgos.

Formación obligatoria para profesionales sanitarios

La norma debe incluir la obligación de ofrecer formación continua y específica a los profesionales de la salud en el uso de tecnologías digitales, sus riesgos, sesgos, ética y protección de datos, para que puedan interpretar y supervisar sistemas automatizados con criterio profesional.

NECESIDAD Y OPORTUNIDAD DE APROBACIÓN

El **Colegio Oficial de Enfermería del Principado de Asturias**, como corporación de derecho público que representa y ordena el ejercicio profesional de más de 8.000 enfermeras y enfermeros en nuestra comunidad autónoma, manifiesta su voluntad de contribuir constructivamente a la elaboración del futuro **Anteproyecto de Ley de Salud Digital**, norma de gran relevancia para el desarrollo del Espacio Europeo de Datos de Salud (EEDS) y para el avance de la digitalización sanitaria en España.

El Reglamento (UE) 2025/327, que entrará en vigor el 25 de marzo de 2027, establece un marco jurídico europeo común en materia de interoperabilidad, gobernanza de datos sanitarios, protección de derechos digitales y uso ético de tecnologías emergentes. Sin embargo, dada la singular distribución

competencial del Estado español en materia de sanidad y la necesidad de extender obligaciones al sector privado, resulta evidente la conveniencia –e incluso la necesidad jurídica– de aprobar una norma nacional con rango de ley que asegure la correcta aplicación del Reglamento en todo el territorio y garantice un marco homogéneo de derechos y obligaciones.

El Colegio considera necesaria la aprobación de una Ley de Salud Digital que adapte el Reglamento EEDS al ordenamiento nacional, por las siguientes razones:

- **Distribución competencial en materia sanitaria.** El Estado ostenta competencias para dictar bases y coordinación general de la sanidad (art. 149.1.16ª CE), mientras que las comunidades autónomas gestionan y desarrollan la asistencia sanitaria. Sin una ley nacional que defina las obligaciones de cada administración, podrían producirse disfunciones o desigualdades entre territorios en el ejercicio de los derechos reconocidos por el Reglamento (por ejemplo, acceso, rectificación o portabilidad de datos de salud).
- **Necesidad de homogeneizar obligaciones en el sector privado.** El Reglamento EEDS impone deberes tanto a prestadores públicos como privados. En España, sin una norma de rango legal que lo establezca, no existiría base jurídica suficiente para exigir cumplimiento homogéneo a clínicas privadas, mutuas, aseguradoras u otros operadores que manejan datos sanitarios electrónicos.
- **Garantía del ejercicio efectivo de los derechos de las personas.** Los derechos reconocidos a ciudadanos, pacientes y profesionales (acceso, portabilidad, oposición, transparencia, seguridad, etc.) requieren una estructura de gobernanza definida, con autoridades competentes, procedimientos y plazos. Esto solo puede lograrse mediante una ley que asigne responsabilidades y mecanismos de control claros.
- **Coordinación con el Reglamento General de Protección de Datos (RGPD).**
  Los datos de salud son categorías especiales con régimen de protección reforzado (art. 9 RGPD y LO 3/2018). Es imprescindible una norma con rango de ley que concrete las condiciones nacionales para su tratamiento, las medidas de seguridad, los derechos digitales de los usuarios y la relación con los responsables del tratamiento.

Además del fundamento jurídico, existen razones técnicas que justifican una norma estatal:

- **Interoperabilidad de la Historia Clínica Electrónica (HCE).** En España coexisten múltiples plataformas autonómicas con distinto grado de madurez. Solo una norma nacional puede fijar estándares comunes de interoperabilidad, nomenclaturas clínicas, formatos de intercambio, mecanismos de identificación unívoca y criterios de calidad de datos.
- **Seguridad y trazabilidad de la información sanitaria.** El intercambio digital de datos sensibles requiere una regulación homogénea de autenticación, cifrado, auditoría y trazabilidad, tanto para el acceso de los profesionales como de los ciudadanos, incluyendo mecanismos de custodia y registro de accesos.
- **Gobernanza unificada y conexión europea.** El Reglamento EEDS prevé la creación de nodos nacionales de conexión con MiSalud@EU y DatosSalud@EU. La ley nacional debe crear formalmente la Autoridad Nacional de Salud Digital y definir las relaciones de coordinación con las autoridades autonómicas de salud digital, evitando duplicidades o vacíos de responsabilidad.
- **Garantía de igualdad territorial.** La falta de una norma estatal podría derivar en brechas digitales territoriales, con comunidades que garanticen plenamente los derechos digitales de salud y otras que no. La ley es el instrumento necesario para asegurar la equidad en el acceso a la información sanitaria en todo el territorio nacional.

El Colegio considera también adecuada la intención de que esta Ley no se limite a trasponer el Reglamento, sino que regule ámbitos conexos no cubiertos por él, pero de gran impacto asistencial y ético:

Uso de tecnologías digitales en la asistencia sanitaria

- Es necesario definir derechos y deberes de pacientes y profesionales en el uso de tecnologías digitales, incluyendo historia clínica electrónica, teleasistencia, aplicaciones móviles, sistemas de soporte a la decisión clínica y plataformas de seguimiento remoto.

- Debe garantizarse que la digitalización no sustituya la valoración clínica presencial ni vulnere el principio de relación terapéutica humana.
- Las enfermeras, como colectivo mayoritario del Sistema Nacional de Salud, deben contar con formación y recursos suficientes para utilizar con seguridad estos sistemas, evitando que las herramientas digitales se conviertan en una fuente de carga administrativa adicional.

Regulación del uso de inteligencia artificial (IA) en salud

- Resulta imprescindible establecer un marco ético y técnico nacional para el uso de IA, biometría o neurotecnologías en el ámbito sanitario, asegurando la supervisión humana, transparencia y explicabilidad de los algoritmos.
- Deben definirse responsabilidades profesionales y legales ante eventuales errores derivados del uso de sistemas automatizados o de apoyo a la decisión clínica.

Protección reforzada de datos personales de salud

- La ley debe especificar cómo se aplican los principios del RGPD (minimización, finalidad, proporcionalidad, seguridad) en contextos sanitarios concretos, incluyendo:
    - Intercambio de información entre niveles asistenciales.
    - Investigación biomédica y uso secundario de datos.
    - Plataformas privadas y servicios digitales de salud.

El Colegio de Enfermería advierte, no obstante, que la futura ley debe equilibrar cuidadosamente la protección de los derechos digitales con la practicidad y carga operativa para los profesionales sanitarios. Entre los aspectos que deben vigilarse:

1. Evitar sobrecarga burocrática en la asistencia derivada de nuevas obligaciones técnicas o registros digitales.
2. Garantizar la interoperabilidad efectiva, evitando que cada comunidad autónoma desarrolle sistemas paralelos que impidan la comunicación real de datos.

3. Asegurar la participación de los colegios profesionales y sociedades científicas en el diseño y supervisión de los sistemas de historia clínica digital y en la definición de estándares éticos y técnicos.
4. Prever formación obligatoria y recursos tecnológicos adecuados para que el personal sanitario pueda adaptarse a los nuevos sistemas digitales sin perjuicio de la atención directa.
5. Incluir mecanismos de evaluación y mejora continua, que permitan adaptar la ley a la evolución tecnológica y a las recomendaciones europeas.

Por todo lo expuesto, el Colegio Oficial de Enfermería del Principado de Asturia**s**:

- Apoya la tramitación y aprobación del Anteproyecto de Ley de Salud Digital, por ser necesaria desde el punto de vista jurídico, competencial y técnico, para garantizar la correcta aplicación del Reglamento (UE) 2025/327 en España.
- Solicita que el texto resultante refuerce la equidad territorial, la interoperabilidad, la seguridad y la protección de los derechos digitales, tanto de los pacientes como de los profesionales.
- Insta a que los colegios profesionales sean tenidos en cuenta como agentes colaboradores en el proceso de desarrollo reglamentario y en los órganos consultivos de la futura Autoridad Nacional de Salud Digital.
- Reclama que se garantice la formación, participación y protección profesional de las enfermeras ante los nuevos entornos digitales, asegurando que la digitalización de la sanidad siga siendo un proceso centrado en las personas, no solo en la tecnología.

OBJETIVOS DE LA NORMA

El Colegio de Enfermería está de acuerdo con la necesidad de adaptar el ordenamiento nacional al Reglamento Europeo del Espacio de Datos de Salud. Consideramos que esta adaptación es imprescindibl**e** para garantizar:

- El ejercicio uniforme de los derechos digitales en salud de todos los ciudadanos, independientemente de su comunidad autónoma o del prestador sanitario.
- La interoperabilidad técnica y semántica entre los sistemas de historia clínica, tanto dentro de España como con otros Estados miembros.

- La protección reforzada de los datos personales de salud, en coherencia con el RGPD y la Ley Orgánica 3/2018.
- La coordinación institucional entre la futura Autoridad Nacional de Salud Digital y las autoridades autonómicas de salud digital.

El CODEPA apoya plenamente la aprobación del Anteproyecto en lo relativo a la adaptación al Reglamento EEDS, siempre que se acompañe de mecanismos de participación profesional, financiación suficiente y medidas que garanticen la equidad, la interoperabilidad y la calidad de los datos.

El Colegio de Enfermería está de acuerdo con la regulación del uso de tecnologías digitales, pero solicita que la ley incluya garantías éticas, formación obligatoria, simplificación administrativa e interoperabilidad universal, asegurando que la tecnología esté al servicio del cuidado y no al revés.

El Colegio apoya el objetivo de regular el uso de los datos personales de salud, siempre que la ley garantice el control del paciente sobre su información, el respeto a la confidencialidad y la existencia de un marco ético y profesional sólido en la gobernanza de los datos.

POSIBLES SOLUCIONES, ALTERNATIVAS REGULATORIAS Y NO REGULATORIAS

La alternativa no regulatoria (no aprobar una ley) no garantiza el cumplimiento del Reglamento EEDS, compromete la equidad, la interoperabilidad y la seguridad jurídica, y por tanto no es recomendable.

La alternativa reglamentaria solo sería útil como complemento posterior, para desarrollar aspectos técnicos una vez aprobada la ley. No puede sustituirla ni garantizar la adaptación integral al Reglamento EEDS.

Integrar el contenido en otras leyes reduciría el número de normas, pero no ofrece una respuesta sistemática y moderna. La digitalización de la sanidad requiere un marco específico, coherente y evolutivo, lo que justifica una ley propia.

Por todo ello, El CODEPA considera que aprobar un Anteproyecto de Ley de Salud Digital que adapte el Reglamento EEDS al derecho español, regule la

historia clínica interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria es la única alternativa plenamente adecuada, por los siguientes motivos:

1. **Proporciona seguridad jurídica y rango normativo suficiente**. Una ley formal puede asignar competencias, crear organismos, reconocer derechos y establecer obligaciones aplicables a todos los prestadores de asistencia sanitaria.
2. **Permite la coordinación entre Estado y comunidades autónomas**. El texto legal puede definir la gobernanza multinivel necesaria para la interoperabilidad y la protección de derechos.
3. **Integra lo público y lo privado bajo los mismos estándares**. Garantiza que todos los prestadores –SNS y sector privado– estén sujetos a las mismas obligaciones de calidad, interoperabilidad y acceso a la información.
4. **Refuerza la participación y el control democrático**. La tramitación parlamentaria asegura transparencia, debate y participación de los agentes profesionales y ciudadanos.
5. **Facilita el desarrollo reglamentario posterior**. Una ley marco puede prever desarrollos técnicos (por Real Decreto) en interoperabilidad, ciberseguridad o IA sanitaria.
6. **Permite incorporar una visión ética y profesional del cuidado digital**.
   La ley puede establecer principios éticos, derechos de los profesionales y garantías para una transformación digital centrada en las personas.

Por todo lo anterior, SOLICITO al MINISTERIO DE SANIDAD que admita a trámite el presente escrito, tenga por comparecido electrónicamente y personado al Colegio Oficial de Enfermería del Principado de Asturias en el procedimiento administrativo de elaboración y aprobación del Anteproyecto de Ley de Salud Digital por el que se adapta al ordenamiento nacional 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, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/284 y se regula la historia clínica digital interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria; así como reconocida su condición de interesado en el

mismo, y tenga por realizadas y evacuadas, en tiempo y forma, las alegaciones y observaciones contenidas en el cuerpo de este escrito.

Oviedo, a 20 de octubre de 2025.

Firmado digitalmente por 10866003K ESTEBAN GOMEZ (R: Q3366003F)
Nombre de reconocimiento (DN): 2.5.4.13=Ref:AEAT/AEAT0392/ PUESTO 1/34842/20092024094015, serialNumber=IDCES-10866003K, givenName=ESTEBAN, sn=GOMEZ SUAREZ, cn=10866003K ESTEBAN GOMEZ (R: Q3366003F), 2.5.4.97=VATES-Q3366003F, o=COLEGIO OFICIAL DE DIPLOMADOS Y GRADUADOS EN ENFERMERIA DEL PRINCIPADO DE ASTURIAS, c=ES

EL PRESIDENTE

ESTEBAN GÓMEZ SUÁREZ