# PROPUESTA DE REFORMA LEGISLATIVA A LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

## Protección de datos personales de salud, interoperabilidad y expedientes clínicos electrónicos

***Exposición de motivos, diagnóstico, beneficios, riesgos y proyecto de decreto***

## Presentación

La interoperabilidad de los expedientes clínicos puede ayudar a que una persona reciba atención continua aunque sea atendida por instituciones distintas. Para que esa coordinación funcione, los datos deben circular con oportunidad y bajo reglas claras. La información de salud, sin embargo, revela aspectos íntimos de la vida de una persona y una exposición indebida puede afectar su dignidad, su trabajo, su familia y su acceso a servicios.

Esta propuesta busca dar un marco legal específico para el intercambio de datos de salud entre sujetos obligados, particularmente en el contexto del Sistema Universal de Salud (SUS). No pretende detener la colaboración clínica ni crear una autorización indiscriminada para consultar expedientes. Propone que cada acceso tenga una razón legítima, sea limitado a lo necesario, pueda verificarse y esté respaldado por una evaluación de impacto a la privacidad antes de iniciar o ampliar operaciones de alto riesgo.

El proyecto parte de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados vigente al 14 de noviembre de 2026 y de los instrumentos publicados para la organización y operación del SUS. Deberá armonizarse, durante el proceso legislativo, con cualquier modificación posterior y con las normas sanitarias aplicables.

## Contenido

I. Resumen ejecutivo
II. Antecedentes del Sistema Universal de Salud
III. Beneficios públicos y clínicos esperados
IV. Riesgos que deben atenderse
V. Diagnóstico jurídico y justificación
VI. Evaluación de impacto a la privacidad: alcance propuesto
VII. Experiencias y referentes comparados
VIII. Proyecto de decreto
IX. Régimen transitorio y ruta de implementación
X. Fuentes de consulta

## I. Resumen ejecutivo

Se propone adicionar a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados reglas expresas para el tratamiento interoperable de datos personales de salud. La reforma se apoya en deberes ya existentes —seguridad, responsabilidad, análisis de riesgos, documentación, confidencialidad y atención de vulneraciones— y los concreta para los sistemas que conecten expedientes clínicos, plataformas de referencia, servicios en la nube y mecanismos de intercambio entre instituciones públicas.

La reforma propuesta: a) define límites de finalidad y acceso; b) exige acuerdos de intercambio con responsabilidades identificables; c) incorpora autenticación robusta, perfiles de acceso, trazabilidad y acceso excepcional de emergencia; d) regula salvaguardas mínimas para servicios de nube; e) establece una evaluación de impacto a la

privacidad previa a la puesta en operación y a cambios de alto riesgo; f) refuerza los derechos de las personas; g) dispone coordinación inmediata ante incidentes; y h) separa la atención clínica de usos secundarios como investigación, planeación o entrenamiento de sistemas automatizados.

La evaluación de impacto propuesta no sustituye el análisis de riesgos ni el documento de seguridad de la ley. Es una revisión previa, documentada y centrada en las personas, que analiza necesidad, proporcionalidad, flujos de datos, riesgos concretos, alternativas y medidas de mitigación antes de conectar sistemas o aumentar el alcance del tratamiento.

## II. Antecedentes del Sistema Universal de Salud

### 1. Creación y finalidad

El decreto presidencial que crea el Servicio Universal de Salud fue publicado en el Diario Oficial de la Federación el 17 de abril de 2026. Su propósito declarado es facilitar que las personas reciban atención oportuna en las instituciones públicas, con independencia de su institución de adscripción, mediante coordinación e intercambio de servicios. El decreto prevé mecanismos de coordinación, comités especializados y el desarrollo de herramientas digitales, incluido el expediente clínico electrónico. [1]

Las reglas de organización y funcionamiento de los comités del SUS, publicadas el 20 de julio de 2026, contemplan un Comité de Transformación Digital encargado de impulsar conectividad, interoperabilidad, intercambio de información y fortalecimiento del expediente clínico electrónico. La modificación publicada el 24 de julio de 2026 ajustó la organización de los comités, incluida la materia de calidad y atención primaria. Estos instrumentos confirman que la interoperabilidad es una pieza operativa del sistema, no una posibilidad remota. [2][3]

En la integración institucional del SUS participa el ISSSTE junto con otras instituciones públicas. Por ello, la protección de datos no es una tarea aislada de cada unidad médica: requiere reglas comunes para identificar a la persona, consultar información pertinente, registrar los accesos, responder incidentes y asegurar continuidad cuando intervengan varias instituciones.

### 2. El expediente clínico en un sistema conectado

La interoperabilidad permite que sistemas diferentes intercambien y comprendan información mediante reglas técnicas y organizativas comunes. No significa que cada institución deba copiar todos los expedientes de las demás, ni que cualquier persona trabajadora pueda consultar cualquier dato. Para una atención concreta puede bastar una parte del expediente: alergias, medicamentos, diagnósticos relevantes, estudios recientes o antecedentes que cambien una decisión clínica.

La nube puede facilitar disponibilidad y escalabilidad, pero no traslada la responsabilidad legal a quien presta el servicio tecnológico. La institución pública que decide para qué y cómo se tratan los datos conserva deberes frente a las personas titulares, aun cuando contrate infraestructura, almacenamiento o soporte externo.

## III. Beneficios públicos y clínicos esperados

Si se diseña con cuidado, el intercambio de información puede hacer más sencilla la atención de las personas y reducir cargas para pacientes y personal. Entre sus beneficios posibles se encuentran:

- Continuidad de la atención cuando una persona es referida, trasladada o atendida por una institución distinta.
- Menos repetición de estudios y trámites cuando los resultados recientes son confiables, pertinentes y accesibles para el equipo tratante.
- Mejor conocimiento de alergias, tratamientos y antecedentes relevantes en una urgencia.
- Mayor coordinación entre unidades médicas y mejor seguimiento de referencias y contrarreferencias.
- Información más oportuna para que las personas expliquen menos veces su historia clínica y puedan concentrarse en recibir atención.
- Planeación sanitaria más sólida mediante información agregada y protegida, con separación clara respecto de la atención individual.
- Reducción de errores por expedientes fragmentados, siempre que exista una identificación confiable y mecanismos para corregir datos equivocados.

Un ejemplo cercano: una persona mayor llega a una unidad distinta de la que suele atenderla y no recuerda el nombre de sus medicamentos. Una consulta segura y limitada al tratamiento vigente puede evitar una interacción peligrosa. Ese resultado depende de que el sistema muestre datos actuales, identifique correctamente a la persona y deje registro de quién consultó y por qué.

## IV. Riesgos que deben atenderse

La posibilidad de beneficio no elimina los riesgos. La conexión entre sistemas aumenta el alcance de un error o una intrusión: una cuenta comprometida, una configuración incorrecta o una búsqueda sin control puede exponer información de muchas personas y de varias instituciones a la vez.

**Acceso excesivo o por curiosidad.** La consulta de expedientes por personal sin relación con la atención puede revelar diagnósticos, tratamientos, salud mental, vida sexual o consumo de sustancias. La prohibición debe ser operativa: perfiles por función, autenticación, registro y revisión.

**Filtraciones, robo de credenciales y extorsión.** Los expedientes pueden ser objetivo de ransomware, fraude o venta ilícita. Un incidente puede generar angustia, discriminación o riesgo físico, además de afectar la operación clínica.

**Uso secundario sin transparencia.** Los datos reunidos para atender a una persona podrían reutilizarse para investigación, evaluación, publicidad, decisiones automatizadas o entrenamiento de sistemas sin base jurídica suficiente ni información clara.

**Errores de identidad y mezcla de expedientes.** Una coincidencia incorrecta puede atribuir a una persona el diagnóstico o medicamento de otra. El daño puede ser clínico inmediato y difícil de reparar.

**Información desactualizada o incompleta.** Un dato antiguo puede orientar mal una decisión si no muestra fuente, fecha, autoría o nivel de certeza. El sistema debe permitir distinguir entre registro original, resumen y dato corregido.

**Caídas de red o dependencia de proveedores.** Una falla, un ataque o la terminación de un contrato puede impedir consultar información relevante. La disponibilidad tecnológica debe incluir operación degradada segura, respaldo y recuperación.

**Concentración de riesgo en la nube.** La centralización de datos o llaves de acceso aumenta el impacto potencial de una intrusión. Se deben evaluar ubicación, subcontratistas, segregación, portabilidad y eliminación verificable.

**Discriminación y estigma.** La exposición de información sobre VIH, salud mental, discapacidad, adicciones, genética o salud reproductiva puede repercutir en la vida familiar, laboral o comunitaria.

**Responsabilidad difusa entre instituciones.** Cuando participan varias instituciones, un aviso de privacidad genérico o un contrato ambiguo puede dejar a la persona sin saber quién responde por una consulta o una corrección.

**Desigualdad institucional.** No todas las unidades tienen la misma conectividad, personal especializado o presupuesto. La implementación desigual puede crear sistemas vulnerables y barreras de atención para comunidades rurales o con discapacidad.

Ejemplo ilustrativo: si una persona acude a urgencias y el sistema vincula su registro con el de alguien con el mismo nombre, una alergia o un tratamiento puede quedar asociado a quien no corresponde. La solución no es bloquear toda consulta, sino confirmar identidad con más de un dato, mostrar procedencia y vigencia, permitir corregir el vínculo y conservar el registro de la decisión clínica.

## V. Diagnóstico jurídico y justificación

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados reconoce como sensibles los datos que se refieren a la salud presente o futura. Exige medidas administrativas, físicas y técnicas; análisis de riesgo; gestión documentada; un documento de seguridad; confidencialidad; registro de vulneraciones y notificación a la persona titular cuando la afectación sea significativa. También contempla transferencias sin consentimiento para prevención o diagnóstico médico, asistencia sanitaria, tratamiento médico o gestión de servicios sanitarios, siempre que esos fines se acrediten. [4]

La ley ya prevé la evaluación de impacto en la protección de datos personales en los artículos 68 a 73. Considera intensivo o relevante el tratamiento de datos sensibles y la realización de transferencias, por lo que los flujos interoperables de información clínica pueden activar esa obligación. La oportunidad legislativa no es crear una evaluación paralela, sino precisar su contenido para sistemas clínicos conectados, asegurar que se

haga antes de ponerlos en operación y acotar la excepción por urgencia para que no sirva para omitir la evaluación de plataformas planeadas.

El marco vigente también incluye obligaciones para personas encargadas y servicios de nube, así como formalización y límites de las transferencias. La propuesta los complementa con reglas comunes para el intercambio clínico entre instituciones: finalidad y acceso por necesidad, acuerdos operativos, trazabilidad, atención de errores de identidad, condiciones mínimas de nube, derechos de las personas y separación de usos secundarios.

La excepción de transferencia para la atención sanitaria no debe leerse como permiso para consultar el expediente completo, conservar copias sin límite o reutilizar la información para cualquier fin relacionado, de manera amplia, con la salud. La finalidad concreta, la necesidad de cada dato y las responsabilidades de quienes participan deben poder explicarse y auditarse.

**La reforma se justifica por cuatro razones**.

**Primero,** la información clínica tiene una sensibilidad y un impacto personal mayores que los de muchos otros datos.

**Segundo,** la interoperabilidad expande los flujos, los puntos de acceso y el número de instituciones involucradas.

**Tercero,** la confianza pública es condición para que las personas compartan información necesaria para su atención.

**Cuarto,** reglas comunes evitan que la protección dependa únicamente del criterio de cada contrato o plataforma.

### Alcance y coordinación con el sector privado

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados regula a los responsables públicos comprendidos en su ámbito. La iniciativa propuesta obliga directamente a esos responsables. Cuando una empresa provea nube, soporte o procesamiento por cuenta de una institución pública, sus obligaciones deberán quedar en el instrumento jurídico correspondiente y en la normativa aplicable a encargados. Si un prestador privado trata datos como responsable propio, su régimen principal es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Por técnica legislativa, esta propuesta no pretende extender por sí sola una ley a sujetos ajenos a su ámbito; se recomienda valorar una armonización paralela de la ley del sector privado para cubrir de manera coherente los intercambios mixtos.

## VI. Evaluación de impacto a la privacidad

La evaluación de impacto en la protección de datos personales (EIPDP) ya está prevista en los artículos 68 a 73 de la ley. La iniciativa aprovecha ese instrumento y propone una regla especial para el sector salud: cuando se habilite interoperabilidad de expedientes, se conecten instituciones o se migren datos clínicos a la nube a escala relevante, la

evaluación deberá abordar riesgos propios de esos flujos y concluir antes de que el sistema comience a operar.

La EIPDP complementa, pero no sustituye, el análisis de riesgos ni el documento de seguridad. El análisis de riesgos identifica amenazas y vulnerabilidades del sistema; el documento de seguridad organiza medidas y responsables; la evaluación de impacto examina, desde la perspectiva de los derechos, si el tratamiento es necesario y proporcional, qué afectaciones puede causar y qué alternativas menos invasivas existen. La propuesta también precisa que una urgencia clínica individual no obliga a suspender la atención, pero tampoco justifica omitir la evaluación previa de una plataforma que se planea con anticipación.

**Contenido mínimo que propone el articulado**

- Descripción de la operación, instituciones, finalidades, categorías de datos, personas afectadas, flujos, nube, subcontratistas y periodos de conservación.
- Fundamento jurídico de cada transferencia o acceso y explicación de la necesidad de interoperar para la finalidad concreta.
- Análisis de proporcionalidad y minimización: qué datos son indispensables, quién necesita consultarlos y durante cuánto tiempo.
- Riesgos para derechos, dignidad, salud y seguridad de las personas, incluidos errores de identidad, discriminación, reidentificación, accesos indebidos, fallas y brechas.
- Medidas técnicas, administrativas y organizativas, responsables de ejecutarlas, evidencia de pruebas y plan de respuesta.
- Riesgo residual después de las mitigaciones, decisión razonada de continuar, modificar o no iniciar el tratamiento.
- Mecanismos para informar a las personas, ejercer derechos, corregir errores, conocer accesos y presentar inconformidades.
- Fecha de revisión, responsable institucional y supuestos que obligan a actualizarla.

La EIP debe actualizarse ante cambios sustanciales de finalidad, datos, instituciones, arquitectura, proveedor de nube, población o volumen de personas, y cuando un incidente o una auditoría revele un riesgo nuevo. La propuesta prevé que la Secretaría y las autoridades garantes emitan criterios comunes dentro de sus competencias. Cuando el riesgo residual sea alto, el sistema no deberá iniciar o ampliar el tratamiento hasta que se reduzca a un nivel aceptable o se adopte la determinación que corresponda conforme a la ley.

## VII. Experiencias y referentes comparados

Los referentes internacionales no se trasladan de forma automática; sirven para identificar controles útiles que deben adaptarse al marco constitucional mexicano.

**Espacio Europeo de Datos de Salud.** El Reglamento (UE) 2025/327 distingue el uso primario de datos para la atención de los usos secundarios y desarrolla condiciones para acceso, gobernanza y entornos seguros de procesamiento. La propuesta retoma

esa separación: el permiso para atender no debe convertirse en autorización general para investigar, planear o entrenar modelos con datos identificables. [5]

**Intercambio sanitario en Estados Unidos.** El marco TEFCA incorpora reglas comunes de privacidad y seguridad para participantes, identidad y autenticación, y exige que las solicitudes de intercambio respondan a un propósito definido. La lección aplicable es que la interoperabilidad necesita reglas homogéneas de confianza, no sólo compatibilidad técnica. [6]

De ambos referentes se toman principios funcionales: finalidad delimitada, gobernanza de participantes, acceso verificable, separación de usos y protección reforzada de datos clínicos. El texto propuesto conserva flexibilidad tecnológica para no imponer un proveedor, arquitectura o estándar comercial específico.

## VIII. Proyecto de decreto

**DECRETO POR EL QUE SE ADICIONAN Y REFORMAN DIVERSAS DISPOSICIONES DE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, EN MATERIA DE TRATAMIENTO INTEROPERABLE DE DATOS PERSONALES DE SALUD**

***Artículo Único. Se adiciona*** *un Capítulo III al Título Segundo, denominado "Del tratamiento interoperable de datos personales de salud", con los artículos 36 Bis a 36 Undecies; un artículo 68 Bis; y una fracción IV al artículo 69, así un párrafo final a la fracción V del artículo 64.* ***Se reforma*** *el artículo 73, todos ellos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para quedar como sigue:*

**TÍTULO SEGUNDO**
**PRINCIPIOS Y DEBERES**

**Capítulo III**
**Del tratamiento interoperable de datos personales de salud**

**Capítulo III**
**Del tratamiento interoperable de datos personales de salud**

**Artículo 36 Bis. Objeto y ámbito de aplicación.** Las disposiciones de este Capítulo son aplicables al tratamiento interoperable de datos personales de salud que realicen los responsables sujetos a esta Ley, directamente o por conducto de personas encargadas, cuando se comuniquen, consulten o pongan a disposición de otra institución pública mediante sistemas, plataformas, servicios en la nube o mecanismos electrónicos de referencia y atención.

La interoperabilidad no modifica la naturaleza sensible de los datos personales de salud ni amplía por sí misma las finalidades, atribuciones o supuestos de transferencia previstos en las disposiciones aplicables. La institución que determine los fines y medios del tratamiento conservará las obligaciones que le correspondan frente a la persona titular.

Para efectos de este Capítulo, se entenderá por sistema interoperable de salud el conjunto de sistemas, plataformas y reglas técnicas y organizativas que permite intercambiar o consultar datos personales de salud entre dos o más responsables. La regulación técnica podrá desarrollar esta definición sin restringirla a una tecnología o proveedor determinados.

**Artículo 36 Ter. Principios de acceso y uso.** El acceso o intercambio de datos personales de salud deberá atender una finalidad concreta, legítima y vinculada con las atribuciones del responsable; ser necesario para la atención, referencia, continuidad o gestión del servicio que legalmente corresponda; y limitarse a los datos pertinentes y estrictamente necesarios para ese propósito.

El responsable deberá identificar a la persona usuaria del sistema, su función y la institución a la que pertenece; asignar permisos conforme a sus tareas; y evitar consultas generales, búsquedas masivas o accesos permanentes que no respondan a una necesidad acreditable. La interoperabilidad no autoriza la consulta integral del expediente clínico cuando la finalidad pueda cumplirse con información parcial.

Los datos deberán presentarse con información suficiente sobre su fuente, fecha de registro, vigencia y, cuando sea posible, autoría o institución de origen. La consulta de un registro no deberá ocultar que se trata de información histórica, provisional o pendiente de corroboración.

**Artículo 36 Quáter. Acuerdos de intercambio.** Antes de habilitar el intercambio, los responsables participantes deberán formalizar un instrumento jurídico o acuerdo operativo que establezca, al menos: las instituciones y sistemas participantes; la finalidad y fundamento jurídico; las categorías de datos que podrán intercambiarse; las funciones y responsabilidades de cada participante; los perfiles autorizados; los controles de seguridad; los periodos de conservación; el procedimiento de ejercicio de derechos; la atención de incidentes; la auditoría de accesos; y las condiciones para suspender, terminar o modificar la conexión.

El instrumento no sustituirá las obligaciones, avisos de privacidad ni bases jurídicas previstas en esta Ley. Si una disposición exime de formalizar un instrumento específico de transferencia, los responsables deberán documentar de todas formas las reglas técnicas y operativas necesarias para cumplir este artículo, sin que esa documentación se convierta en una nueva base jurídica.

**Artículo 36 Quinquies. Identidad, autenticación y trazabilidad.** El responsable deberá establecer medidas acordes con el riesgo para verificar la identidad de las personas usuarias y de las personas titulares, administrar permisos individualizados, revisar periódicamente las cuentas y retirar oportunamente aquellas que ya no deban conservar acceso. Cuando el riesgo lo justifique, utilizará autenticación multifactor, cifrado y controles adicionales.

Cada consulta o transmisión deberá generar un registro íntegro y protegido que permita conocer, como mínimo, quién accedió, desde qué institución, a qué expediente o conjunto de datos, cuándo, con qué finalidad declarada y qué acción realizó. Los registros se

conservarán por el plazo que determinen las disposiciones aplicables y las reglas archivísticas, con acceso restringido y protección contra alteración.

En una urgencia clínica, el sistema podrá habilitar un acceso excepcional sujeto a autenticación, justificación de la necesidad, alcance limitado y registro reforzado. El responsable deberá revisar posteriormente estos accesos y documentar la conclusión. El acceso de emergencia no releva del deber de confidencialidad ni permite usos ulteriores ajenos a la urgencia.

**Artículo 36 Sexies. Servicios de cómputo en la nube.** Cuando el responsable utilice servicios de cómputo en la nube para tratar datos personales de salud, deberá documentar la evaluación de riesgos y verificar que el contrato y los controles técnicos garanticen, al menos: confidencialidad, integridad, disponibilidad, segregación lógica, cifrado en tránsito y almacenamiento, administración segura de llaves, respaldos, recuperación, registro de actividad, gestión de vulnerabilidades y atención oportuna de incidentes.

El contrato deberá precisar la ubicación y jurisdicción del tratamiento, las personas subencargadas, las condiciones para auditarlas, la notificación de incidentes, la portabilidad de la información, la devolución o eliminación verificable al terminar el servicio y la asistencia para el ejercicio de derechos. La persona encargada no podrá utilizar los datos para fines propios, publicidad, perfilamiento, entrenamiento de modelos ni comercialización, salvo que exista una base jurídica independiente y se cumplan los requisitos aplicables.

La contratación de un servicio en la nube no libera al responsable de sus obligaciones ni permite que el proveedor decida finalidades incompatibles con las instrucciones documentadas y la ley.

**Artículo 36 Septies. Evaluación de impacto en la protección de datos personales.** La evaluación de impacto aplicable a los tratamientos previstos en este Capítulo se regirá por los artículos 68 a 73 de esta Ley y por las reglas específicas de este artículo. Deberá presentarse en los plazos del artículo 71 y realizarse antes de poner en operación o modificar sustancialmente una plataforma interoperable, conectar una nueva institución, migrar a la nube datos de salud a escala relevante o habilitar una nueva finalidad o categoría de datos.

La evaluación deberá describir el tratamiento y sus flujos; identificar responsables, encargados y personas afectadas; señalar la finalidad y fundamento jurídico; analizar necesidad y proporcionalidad; identificar riesgos para la privacidad, la dignidad, la salud y otros derechos; comparar alternativas menos invasivas; determinar medidas para evitar o reducir los riesgos; asignar responsables y plazos; y valorar el riesgo residual. Deberá documentarse la decisión de iniciar, modificar, posponer o no realizar el tratamiento.

La evaluación deberá examinar, como mínimo, la descripción del tratamiento y sus flujos; las instituciones, personas encargadas y personas afectadas; la finalidad y el fundamento jurídico; la necesidad y proporcionalidad; las categorías y el volumen de datos; las medidas de minimización; los riesgos para la privacidad, dignidad, salud y demás derechos; las alternativas menos invasivas; las medidas para evitar o reducir los riesgos;

las personas responsables y plazos de aplicación; el riesgo residual; y los mecanismos de información, ejercicio de derechos y atención de quejas.

La evaluación deberá actualizarse cuando cambien sustancialmente la finalidad, volumen, categorías de datos, instituciones, arquitectura, proveedor, condiciones de acceso o nivel de riesgo, así como después de una vulneración o auditoría que revele riesgos no considerados. El responsable pondrá a disposición de la persona titular una síntesis clara de sus conclusiones, sin revelar información cuya divulgación comprometa la seguridad de los sistemas o derechos de terceros.

Cuando subsista un riesgo alto, el responsable atenderá las recomendaciones y el procedimiento previstos en los artículos 68 a 72, antes de iniciar o ampliar el tratamiento. La evaluación no sustituye el análisis de riesgos, el análisis de brecha ni las obligaciones previstas en los artículos 25 a 35.

**Artículo 36 Octies. Información y derechos de las personas.** El responsable deberá informar, en lenguaje claro y por medios accesibles, que los datos de salud pueden consultarse o intercambiarse entre instituciones para finalidades determinadas; señalar las instituciones o categorías de participantes, los medios para conocer las condiciones del tratamiento, los mecanismos de ejercicio de derechos y la forma de presentar una queja.

La persona titular podrá conocer, conforme a esta Ley, las condiciones del tratamiento y los accesos a sus datos, así como solicitar su rectificación, cancelación u oposición cuando proceda. Los responsables establecerán un mecanismo para remitir y coordinar solicitudes relacionadas con datos originados en otra institución, sin trasladar a la persona la carga de identificar el sistema técnico o la unidad que causó el error.

La atención urgente o necesaria no podrá condicionarse exclusivamente a la aceptación de una autorización genérica para usos no indispensables. Lo anterior no impide el tratamiento que tenga fundamento legal y sea necesario para prestar el servicio de salud, pero exige informar con claridad y respetar los derechos que procedan conforme a esta Ley.

**Artículo 36 Nonies. Calidad, corrección y seguridad clínica.** Los responsables deberán establecer procedimientos para detectar y corregir errores de identidad, duplicidades, registros incompletos o información desactualizada. La corrección deberá comunicarse, cuando sea técnicamente posible y jurídicamente procedente, a las instituciones que recibieron el dato erróneo, preservando la trazabilidad y evitando que se borre indebidamente el historial clínico.

La información intercambiada deberá conservar su contexto y procedencia. Los sistemas deberán permitir advertir inconsistencias relevantes y evitar que una coincidencia basada únicamente en el nombre de la persona se considere suficiente para vincular expedientes.

**Artículo 36 Decies. Usos secundarios y datos disociados.** La consulta o intercambio autorizado para la atención individual no constituye, por sí mismo, fundamento para tratar los datos con fines de investigación, estadística, evaluación de políticas, planeación, comercialización o desarrollo y entrenamiento de sistemas automatizados.

Los usos secundarios deberán contar con fundamento jurídico propio, finalidad determinada y salvaguardas proporcionales. Cuando se utilicen datos disociados, el responsable deberá aplicar medidas razonables para evitar la identificación o reidentificación; si ésta sigue siendo razonablemente posible, los datos conservarán el carácter de personales y se sujetarán a esta Ley.

**Artículo 36 Undecies. Incidentes, suspensión y rendición de cuentas.** Cuando una vulneración pueda afectar datos personales de salud compartidos, el participante que tenga conocimiento deberá comunicarla sin dilación a los demás responsables involucrados y coordinar acciones de contención, preservación de evidencia, evaluación del impacto y continuidad segura de la atención. Esta comunicación interna no sustituye ni retrasa los avisos a las personas titulares, a la Secretaría o a las autoridades garantes previstos en los artículos 34 y 35.

Los responsables deberán mantener mecanismos para suspender de forma segura cuentas, conexiones o flujos comprometidos, sin interrumpir injustificadamente la atención. Toda suspensión deberá ser proporcional, documentada y acompañada de medidas alternativas para proteger la salud de las personas.

Los responsables conservarán evidencia suficiente para demostrar el cumplimiento de este Capítulo y someterán los sistemas interoperables a revisiones periódicas de acceso, seguridad y cumplimiento. La Secretaría y las autoridades garantes, en el ámbito de sus competencias, podrán requerir la evaluación de impacto, los acuerdos, las bitácoras y la evidencia de las medidas, con respeto a la información confidencial y a la seguridad de los sistemas.

**TÍTULO QUINTO**
**COMUNICACIONES DE DATOS PERSONALES**
**Capítulo Único**
**De las Transferencias y Remisiones de Datos Personales**

**Artículo 64.** El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento de la persona titular, en los siguientes supuestos:

**I a IV.** …

**V.** Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;

En los supuestos de esta fracción, el intercambio de datos personales de salud mediante sistemas interoperables deberá sujetarse a los artículos 36 Bis a 36 Undecies de esta Ley. La excepción al consentimiento no autoriza consultas indiscriminadas, acceso integral cuando no sea necesario ni tratamientos para finalidades distintas de las que justificaron la transferencia.

***VI a IX …***

**TÍTULO SEXTO**
**ACCIONES PREVENTIVAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES**
**Capítulo I**
**De las Mejores Prácticas**

**Artículo 68 Bis.** Para los tratamientos interoperables de datos personales de salud, la evaluación de impacto prevista en el artículo 68 deberá incluir, además de lo que determinen la Secretaría o la Autoridad garante competente, los elementos mínimos establecidos en el artículo 36 Septies de esta Ley. La evaluación identificará las instituciones que participan, los flujos de información, los servicios de nube y subcontratistas, los perfiles de acceso, los mecanismos de trazabilidad y las medidas de continuidad de la atención.

**Artículo 69.** Para efectos de esta Ley se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:

**I a III.** …

**IV.** Se traten datos personales de salud mediante sistemas interoperables, plataformas de intercambio o servicios de cómputo en la nube que permitan su consulta por más de una institución responsable.

**Artículo 73.** Cuando a juicio del sujeto obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, o se trate de situaciones de emergencia o urgencia, no será necesario realizar la evaluación de impacto en la protección de datos personales, salvo lo dispuesto en los párrafos siguientes.

La excepción prevista en el párrafo anterior no será aplicable a la planeación, desarrollo, contratación, conexión o puesta en operación de una plataforma o sistema interoperable de datos personales de salud, por el solo hecho de que su objeto sea facilitar la atención de emergencias o urgencias.

Lo anterior no impedirá el acceso excepcional a los datos estrictamente necesarios para atender una urgencia clínica individual mediante sistemas previamente habilitados, conforme a los controles previstos en el artículo 36 Quinquies. Cuando por una emergencia real no sea posible realizar previamente una evaluación de impacto respecto de un tratamiento temporal, el responsable documentará las razones, limitará el tratamiento a lo indispensable y realizará una evaluación posterior tan pronto como sea posible, sin exceder de treinta días naturales.

**Artículos transitorios**

**Primero.** El presente Decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

**Segundo.** La Secretaría Anticorrupción y Buen Gobierno, en coordinación con la Secretaría de Salud y con las instituciones públicas que integren cualquier sistema de

salud, emitirá, en un plazo no mayor a ciento ochenta días naturales contados a partir de la entrada en vigor del Decreto, criterios específicos para la evaluación de impacto de los tratamientos interoperables de datos de salud y para documentar acuerdos de intercambio, perfiles de acceso, trazabilidad, servicios de nube y respuesta coordinada a incidentes. En la elaboración de esos criterios se escuchará a las autoridades garantes competentes y a personas expertas en salud, privacidad, seguridad de la información y accesibilidad.

**Tercero.** Los responsables que, a la entrada en vigor del Decreto, operen sistemas interoperables de datos personales de salud deberán revisar y, en su caso, actualizar la evaluación de impacto prevista en los artículos 68 a 73, así como formalizar los instrumentos operativos previstos en el Capítulo III, dentro de los doce meses siguientes a la emisión de los criterios específicos. Durante ese plazo mantendrán y documentarán medidas provisionales de seguridad y limitarán el acceso a lo necesario para la atención.

**Cuarto.** Los tratamientos nuevos, las conexiones de nuevas instituciones, las migraciones a servicios de nube y las ampliaciones sustanciales que se inicien después de la entrada en vigor deberán sujetarse a los artículos 68 a 73 y a las salvaguardas previstas en el presente Decreto desde su planeación y antes de su puesta en operación, sin esperar a que concluya el plazo establecido en el artículo transitorio anterior.

**Quinto.** Las autoridades competentes realizarán la implementación con cargo a los presupuestos aprobados y conforme a las disposiciones presupuestarias aplicables. Las necesidades de recursos humanos, tecnológicos y de capacitación deberán identificarse en los diagnósticos y programas institucionales correspondientes, sin que esta previsión exima del cumplimiento de las obligaciones legales.

**Sexto.** Las disposiciones administrativas y los instrumentos de coordinación vigentes deberán interpretarse y, en su caso, adecuarse a este Decreto. En caso de incompatibilidad, prevalecerán las disposiciones de protección de datos personales, sin perjuicio de la continuidad de la atención y de las medidas urgentes para proteger la vida y la salud.

## IX. Régimen transitorio y ruta de implementación

La transición debe permitir que las instituciones corrijan brechas sin paralizar servicios ni normalizar conexiones sin evaluación. La propuesta distingue tres momentos:

| Momento | Plazo propuesto | Resultado mínimo |
|---|---|---|
| Entrada en vigor | Día siguiente a la publicación | Las nuevas conexiones y ampliaciones de alto riesgo quedan sujetas de inmediato a la EIP y a controles de acceso. |
| Criterios comunes | Hasta 180 días naturales | Criterios de evaluación, acuerdos de intercambio, nube, trazabilidad y respuesta coordinada. |
| Adecuación de sistemas existentes | 12 meses desde los criterios | EIP actualizada, instrumentos |

| | | |
|---|---|---|
| | | formalizados, responsables y medidas verificables. |
| Revisión periódica | Anual y ante cambios relevantes | Auditoría de accesos, revisión de riesgos, capacitación y actualización de la EIP. |

La regla para sistemas existentes debe aplicarse con una salvaguarda: el plazo de adaptación no habilita una ampliación de datos o finalidades sin evaluación. Cuando se advierta una exposición grave e inmediata, corresponde limitar o suspender el componente comprometido y activar una alternativa clínica segura, no cerrar el acceso asistencial de manera automática.

## X. Consideraciones de técnica legislativa

- La reforma se inserta en la ley que regula a responsables públicos y no atribuye facultades nuevas a órganos distintos de los previstos en el marco vigente.
- Se usan obligaciones verificables: evaluación documentada, acuerdos con contenido mínimo, permisos individualizados, registros de acceso y revisión posterior.
- Se mantiene una arquitectura tecnológicamente neutral: la ley fija garantías y deja a las disposiciones técnicas definir estándares compatibles.
- No se crea un consentimiento universal ni una excepción general nueva. La base para cada transferencia debe encontrarse en la ley vigente.
- Se preserva la diferencia entre atención clínica y usos secundarios, y se establece que la excepción al consentimiento no equivale a ausencia de salvaguardas.
- Los artículos transitorios distinguen las conexiones nuevas de los sistemas existentes y proporcionan plazos medibles.
- El texto requiere revisión final de concordancia con la numeración, reformas publicadas y atribuciones institucionales vigentes al momento de presentar la iniciativa.

## XI. Fuentes de consulta

***Fuentes normativas y técnicas consultadas para elaborar esta propuesta. Las citas identifican los instrumentos de referencia; el articulado propuesto es una formulación legislativa para discusión y no una descripción de derecho vigente.***

[1] Diario Oficial de la Federación, Decreto por el que se crea el Servicio Universal de Salud del Gobierno de México, publicado el 17 de abril de 2026. https://sidof.segob.gob.mx/notas/5785257

[2] Diario Oficial de la Federación, Reglas de organización y funcionamiento de los Comités Interinstitucionales Especializados del Sistema Universal de Salud, 20 de julio de 2026. https://dof.gob.mx/nota_detalle.php?codigo=5793945&fecha=20/07/2026

[3] Diario Oficial de la Federación, Acuerdo por el que se modifican las Reglas de organización y funcionamiento de los Comités Interinstitucionales Especializados, 24 de julio de 2026. https://sidof.segob.gob.mx/notas/5794741

[4] Cámara de Diputados del H. Congreso de la Unión, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, última reforma publicada en el DOF el 14 de noviembre de 2025, en particular artículos 3, 25 a 36 y 59 a 65. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

[5] Unión Europea, Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud. https://eur-lex.europa.eu/eli/reg/2025/327/oj

[6] U.S. Department of Health and Human Services, HealthIT.gov, Trusted Exchange Framework and Common Agreement (TEFCA), materiales de referencia sobre intercambio confiable de información sanitaria. https://www.healthit.gov/topic/interoperability/policy/trusted-exchange-framework-and-common-agreement-tefca