RECOMENDACIONES SOBRE EL TRATAMIENTO DE

LOS DATOS PERSONALES EN LOS EXPEDIENTES CLÍNICOS DE LAS INSTITUCIONES DE SALUD PÚBLICA

inai

DIRECTORIO

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Insurgentes Sur 3211, Colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, Código Postal 04530,
Ciudad de México.

CONTENIDO

GLOSARIO

ARCO: Derechos de Acceso, Rectificación, Cancelación y Oposición.

Atención médica: Al conjunto de servicios que se proporcionan al individuo, con el fin de promover, proteger y restaurar su salud.[1]

CONAMED: Comisión Nacional de Arbitraje Médico.

Constitución o Carta Magna: Constitución Política de los Estados Unidos Mexicanos.

Datos Personales: Cualquier información concerniente a una persona física identificada o identificable.[2]

Datos personales sensibles: Los que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleva un riesgo grave para éste.[3]

DOF: Diario Oficial de la Federación.

Encargado: Es la persona física o jurídica, pública o privada, ajena a la organización del responsable del tratamiento, que trata los datos personales a nombre y por cuenta del responsable[4]. A diferencia de este último, el encargado no decide sobre el tratamiento de los datos personales, sino que lo realiza siguiendo las instrucciones del responsable.

Expediente clínico: Al conjunto único de información y datos personales de un paciente, que se integra dentro de todo tipo de establecimiento para la atención médica, ya sea público, social o privado, el cual, consta de documentos escritos, gráficos, imagenológicos, electrónicos, magnéticos, electromagnéticos, ópticos, magneto-ópticos y de cualquier otra índole, en los cuales, el personal de salud deberá hacer los registros, anotaciones, en su caso, constancias y certificaciones correspondientes a su intervención en la atención médica del paciente, con apego a las disposiciones jurídicas aplicables.[5]

Expediente clínico electrónico: Es el conjunto de información almacenada en medios electrónicos centrada en el paciente que documenta la atención médica prestada por profesionales de la salud con arreglo a las disposiciones sanitarias, dentro de un establecimiento de salud.[6]

INAI o Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

IMSS: Instituto Mexicano del Seguro Social.

ISSSTE: Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado.

---

[1] Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de Información de registro electrónico para la salud, intercambio de información en salud, publicada en el Diario Oficial de la Federación el 30 de noviembre del 2012.
[2] Artículo 3, fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[3] Artículo 3, fracción X de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[4] Artículo 3, fracción XV de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[5] Norma Oficial Mexicana NOM-004-SSA3-2012, Del expediente clínico, publicada en el Diario Oficial de la Federación el 15 de octubre del 2012.
[6] Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de Información de registro electrónico para la salud, intercambio de información en salud, publicada en el Diario Oficial de la Federación el 30 de noviembre de 2012.

Ley General o LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

LGS: Ley General de Salud.

Lineamientos de portabilidad: Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Norma: Norma Oficial Mexicana.

Paciente: Todo aquel usuario beneficiario directo de la atención médica.[7]

Registro Electrónico de Salud: Datos estructurados de información clínica, imagenológica, demográfica, social, financiera, de infraestructura y de cualquier otra índole que documente la atención médica prestada a un solo individuo y/o la capacidad instalada en los establecimientos de salud, almacenados en medios electrónicos.[8]

Responsable: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.[9]

SIRES: Sistema de Información de Registro Electrónico para la Salud.[10]

SSa: Secretaría de Salud.

Titular: La persona física a quien corresponden los datos personales.[11]

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.[12]

TID: Transferencia Internacional de Datos.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.[13]

Urgencia: A todo problema médico-quirúrgico agudo, que ponga en peligro la vida, un órgano o una función y requiera atención inmediata.[14]

Usuario: A toda aquella persona, que requiera y obtenga la prestación de servicios de atención médica.[15]

---

[8] Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de Información de registro electrónico para la salud, intercambio de información en salud, publicada en el Diario Oficial de la Federación el 30 de noviembre de 2012.
[9] Artículo 1, quinto párrafo de la LGPDPPSO.
[10] Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de Información de registro electrónico para la salud, intercambio de información en salud, publicada en el Diario Oficial de la Federación el 30 de noviembre de 2012.
[11] Artículo 3, fracción XXXI de la LGPDPPSO.
[12] Artículo 3, fracción XXXII de la LGPDPPSO.
[13] Artículo 3, fracción XXXIII de la LGPDPPSO.
[14] Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, publicada en el Diario Oficial de la Federación de fecha 15 de octubre de 2012.
[15] Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, publicada en el Diario Oficial de la Federación de fecha 15 de octubre de 2012.

INTRODUCCIÓN

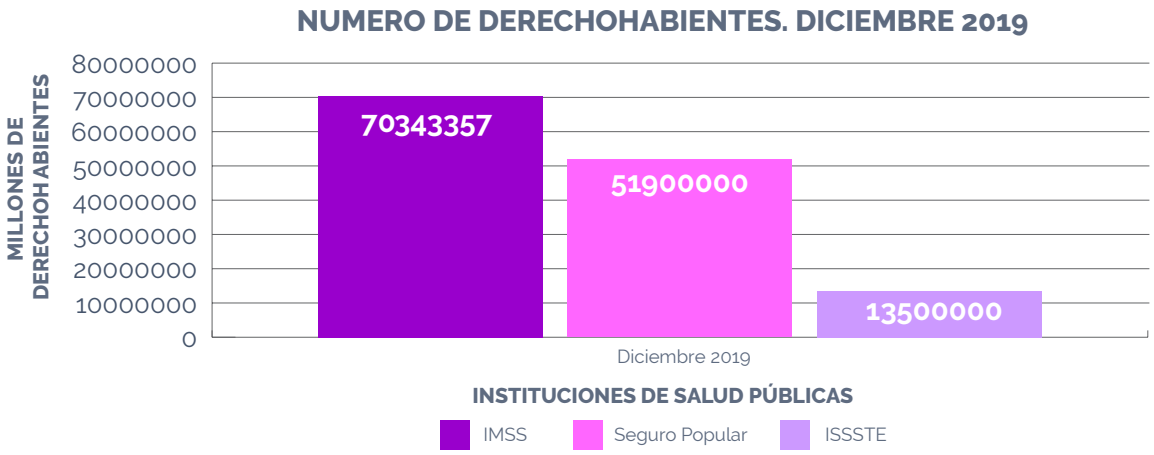
El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, es el responsable de garantizar en el ámbito federal, el ejercicio de los derechos de acceso a la información y la protección de datos personales, conforme a los principios y bases establecidos por los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás disposiciones aplicables.

En este sentido, el INAI cuenta, entre otras, con la atribución de proporcionar apoyo a los responsables para el cumplimiento de sus obligaciones en materia de protección de datos personales, llevar a cabo acciones que promuevan el conocimiento del derecho a la protección de los mismos, así como, promover la actualización en materia de protección de datos personales entre responsables, con el objeto de garantizar el derecho humano que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

Resulta importante señalar, que el artículo 4° de la Carta Magna dispone que toda persona tiene derecho a la protección de la salud, en tal consideración, la Ley General de Salud en sus artículos 77-BIS y 37 fracción VII, determina que los usuarios de servicios de salud tienen el derecho de contar con un expediente clínico, el cual será administrado por las Instituciones de Salud.

La reforma Constitucional del 10 de junio de 2011 se centró en el reconocimiento y goce de los derechos humanos y el principio de interpretación pro-persona, a partir de ello, nace la obligación del Estado mexicano en todos sus niveles de gobierno sin excepción, promover, respetar, proteger y garantizar los derechos humanos. De ahí que, el expediente clínico correctamente elaborado e integrado se constituya en un instrumento idóneo para la protección de la salud de los usuarios; situación que pone de manifiesto la urgencia en el debido cuidado y tratamiento de los datos personales ahí contenidos y, sobretodo, garantizar el derecho a la autodeterminación informativa de las y los mexicanos.

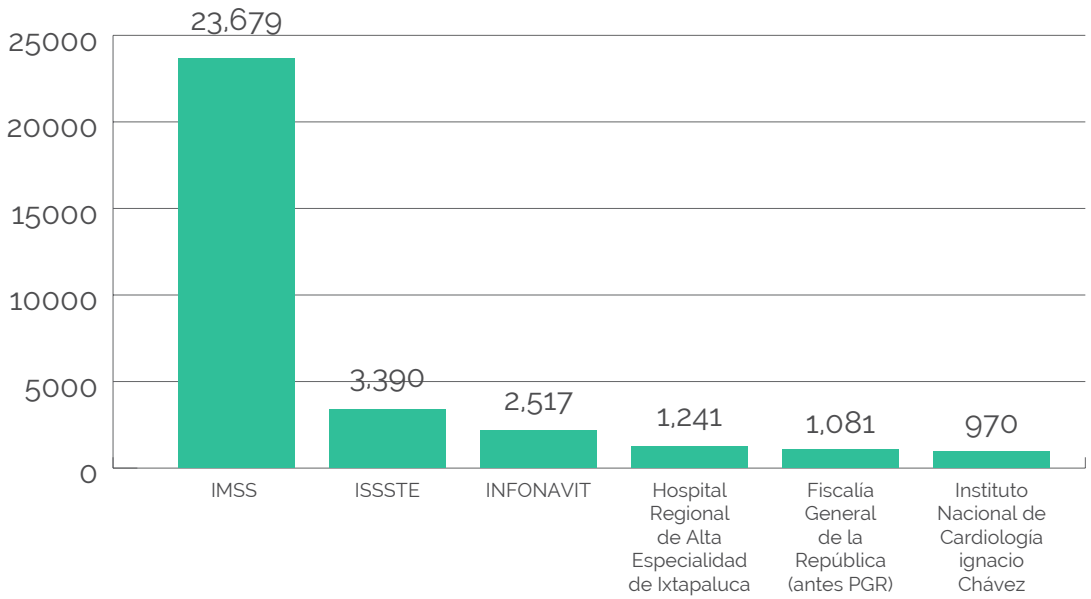
Es de destacar que, en México un total de 135 millones 743 mil 357 personas son atendidas por los servicios de salud públicos. Tan solo al cierre del año 2019, el IMSS contaba con 70 millones 343 mil 357 derechohabientes[16]; en el Sistema de Protección en Salud (Seguro Popular) fue de 51.9 millones[17] y en el ISSSTE fue de 13.5 millones[18]. Enseguida, se muestra una tabla ilustrativa con las cifras antes referidas.



En este tenor, conforme a los principios de universalidad, interdependencia, invisibilidad y progresividad y, en términos de lo dispuesto en los artículos 6, apartado A, fracción II y 16 en su primer y segundo párrafos de la Constitución Política de los Estados Unidos Mexicanos, se advierte que el Estado tiene la obligación de velar por la protección de datos personales de los ciudadanos, más aún, si se trata de datos inherentes al estado de salud de la población mexicana.

En ejercicio a su derecho fundamental de protección de sus datos personales, del período octubre 2018-septiembre 2019, las y los ciudadanos presentaron ante el IMSS un total de 23 mil 679 solicitudes de datos personales, manteniendo la posición como la dependencia que históricamente ha concentrado más requerimientos de este tipo; por su parte, el ISSSTE fue el segundo sujeto obligado con más solicitudes de datos personales, con un total de 3 mil 390; en tanto que el Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT) fue el tercero, con 2 mil 517 requerimientos; en la cuarta posición se encuentra el Hospital Regional de Alta Especialidad de Ixtapaluca (HRAEI) con 1 mil 241 solicitudes; el quinto lugar lo ocupó la Fiscalía General de la República (FGR), anteriormente Procuraduría General de la República, con 1 mil 081 solicitudes, y en el sexto puesto se ubicó el Instituto Nacional de Cardiología Ignacio Chávez (INCARD) con 970 solicitudes[19].

Sujetos obligados con mayor número de solicitudes de datos personales, octubre 2018-septiembre 2019*



FUENTE: INAI, Secretaría de Acceso a la Información, Dirección General de Evaluación, con datos del SISAI de la PNT e información proporcionada por los sujetos obligados del ámbito federal.

[16] Disponible para su consulta en: http://www.imss.gob.mx/sites/all/statics/pdf/informes/20192020/21-InformeCompleto.pdf
[17] Disponible para su consulta en: http://www.transparencia.seguro-popular.gob.mx/contenidos/archivos/transparencia/planesprogramaseinformes/informes/2019/Informe_Resultados_SPSS_2019.pdf
[18] Disponible para su consulta en: http://www.issste.gob.mx/images/downloads/instituto/quienes-somos/IFA_2020.pdf
[19] Disponible para su consulta en: http://inicio.inai.org.mx/Informes%202019/Informe_2019.pdf
[21] Artículo 3, fracción VIII de la LGPDPPSO.

Para las instituciones de salud pública, los derechos y obligaciones relacionados con el tratamiento de los datos personales en los expedientes clínicos están contenidos en la Ley General, en la LGS y principalmente en las Normas Oficiales Mexicanas, como la NOM -004-SSA3-2012, del expediente clínico y la NOM-024-SSA3-2012, Sistemas de Información de registro electrónico para la salud, intercambio de información en salud.

Derivado de que los expedientes clínicos contienen una serie de datos personales para que el personal responsable de su uso pueda monitorear la salud de los pacientes, registrarlos, guardarlos o transferirlos; el procesamiento de los datos personales contenidos en estos archivos es responsabilidad del personal de la salud. Por tanto, el tratamiento de datos personales en las historias clínicas de las instituciones de salud pública debe cumplir con los siguientes principios establecidos en la Ley General:[20]

• **Licitud:** Este principio les exige que el tratamiento de los datos personales lo realicen observando estrictamente lo que ordena la ley, de manera objetiva y respetando el Estado de derecho, lo anterior, con la finalidad de evitar arbitrariedades en el tratamiento de los datos personales.

• **Finalidad:** Este principio busca evitar que se recolecten datos para hacer con ellos lo que sea y delimita los usos que pueda darle el responsable. Asimismo, busca que el tratamiento tenga como objetivo la realización de finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera. Se entenderá que las finalidades son:
:

  • ***Concretas:*** cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular;
  • ***Explícitas***: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;
  • ***Licitas:*** cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable;
  • ***Legítimas:*** cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

• **Lealtad:** Con este principio se busca evitar el tratamiento desleal, deshonesto y no ético al titular sobre su información. El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, prohibiéndole al responsable defraudar esa confianza y recurrir a mecanismos oscuros, ilegales o poco transparentes para recolectar y tratar los datos.

• **Consentimiento:** Este principio reconoce que la persona es el titular del dato y, por ende, ella es quien, en un inicio, tiene control sobre su información y algunos aspectos de su vida relacionados con su información. Para tal efecto, la Ley General define el consentimiento como la manifestación de la voluntad libre, específica e informada

[20] Artículo 16 de la LGPDPPSO.

del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.[21]

Adicionalmente, la _Ley General señala que el consentimiento puede ser:

- ***Expreso***
- ***Tácito***

- **Calidad:** La Ley General exige que los datos personales sean veraces, exactos, completos, correctos y actualizados. La información de calidad es una condición para el debido tratamiento de los datos y de ella dependen algunos derechos de las personas como su buen nombre o que las decisiones que se adopten con fundamento en los datos personales sean correctas, pertinentes o apropiadas; por lo tanto, le corresponde al responsable adoptar medidas para que ello sea así.

- **Proporcionalidad:** El tratamiento de datos personales sólo deberá circunscribirse a los que resulten adecuados, relevantes y no excesivos en relación con la finalidad del tratamiento. Por lo tanto, no está permitido recolectar o usar datos que no guarden estrecha relación con la finalidad del tratamiento.

- **Información:** Con este principio se busca que el titular tenga conocimiento de los principales aspectos que regirán el tratamiento de sus datos personales. La Ley General ordena al responsable informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

- **Responsabilidad:** Consiste en que el responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley General y rendir cuentas al titular, Instituto u organismos garantes, sobre el tratamiento de los datos personales en su posesión. Los mecanismos podrán ser lo siguientes, según corresponda:

- ✔ **Destinar recursos autorizados** para tal fin para la instrumentación de programas y políticas de protección de datos personales;
- ✔ **Elaborar políticas y programas** de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;
- ✔ **Poner en práctica** un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
- ✔ **Revisar periódicamente** las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
- ✔ **Establecer un sistema** de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
- ✔ **Establecer procedimientos** para recibir y responder dudas y quejas de los titulares;
- ✔ **Diseñar,** desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la Ley General y las demás que resulten aplicables en la materia; y
- ✔ **Garantizar** que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la Ley General y las demás que resulten aplicables en la materia.

Tal como se advierte de lo anterior, los principios son las reglas fundamentales de aplicación obligatoria para garantizar el respeto de las personas cuando sus datos recolectados,

almacenados, usados o circulados han sido objeto de cualquier actividad por parte de responsables o encargados del tratamiento, por lo que, éstos cumplen varios objetivos, entre los que se encuentran:

- **Son un instrumento** para garantizar el debido tratamiento de los datos personales y, por ende, el respeto de los derechos de los titulares de los datos;
- **Representan un límite** al tratamiento de los datos personales, pues no pueden hacerse de cualquier manera sino de forma respetuosa;
- **Constituyen una herramienta** de interpretación de la ley y de aplicación correcta de la misma, así como el factor determinante de la solución de casos concretos que se sometan a consideración de las autoridades o los jueces.

Asimismo, los responsables de la salud en las instituciones del sector público deben cumplir con lo establecido en la Ley General y demás normativa vigente aplicable sobre expedientes clínicos, y los pacientes, como proveedores de información son los beneficiarios de los datos que proporciona al personal del área de la salud (aspecto fundamental que se reconoce en la NOM -004-SSA3-2012).

En ese sentido, se han considerado aquellos datos que se refieren a su identidad personal y los que proporciona en relación con su padecimiento; a todos ellos, se les considera información confidencial[22] y gozan de la propiedad de la información para proteger su salud y la confidencialidad de sus datos. Estos datos personales proporcionados por pacientes o terceros al personal de salud e incluidos en los documentos clínicos deben ser tratados según corresponda por todo el personal del sitio de acuerdo con los principios científicos y éticos que guían la práctica médica. Por ejemplo, las disposiciones estipuladas en la Ley General, la LGS y las Normas Oficiales Mexicanas NOM -004-SSA3-2012 y NOM-024-SSA3-2012.

En tal consideración, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable de la salud deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad adoptadas deberán considerar al menos lo siguiente:[23]

- **El riesgo inherente** a los datos personales tratados;
- **La sensibilidad** de los datos personales tratados;
- **El desarrollo tecnológico;**
- **Las posibles consecuencias** de una vulneración para los titulares;
- **Las transferencias de datos personales** que se realicen;
- **El número de titulares;**
- **Las vulneraciones previas** ocurridas en los sistemas de tratamiento;
- **El riesgo** por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Asimismo, con la finalidad de que el responsable de la salud establezca y mantenga las me-

[22] Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, publicada en el Diario Oficial de la Federación de fecha 15 de octubre de 2012.
[23] Artículo 32 de la LGPDPPSO.

didas de seguridad para la protección de los datos personales del paciente, deberá realizar las siguientes actividades interrelacionadas:[24]

- **Crear políticas internas** para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
- **Definir las funciones y obligaciones** del personal involucrado en el tratamiento de datos personales;
- **Elaborar un inventario** de datos personales y de los sistemas de tratamiento;
- **Realizar un análisis de riesgo** de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;
- **Realizar un análisis de brecha,** comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
- **Elaborar un plan de trabajo** para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
- **Monitorear y revisar** de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales;
- **Diseñar y aplicar** diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Adicional a lo anterior, el responsable deberá:

- **Elaborar** un documento de seguridad[25] (instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad);
- **Evitar vulneraciones** a la seguridad (en caso de que ocurra alguna, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso, a efecto de evitar que la vulneración se repita);
- **Guardar confidencialidad** (el sujeto obligado responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo).

[24] Artículo 33 de la LGPDPPSO.
[25] Artículo 3, fracción XIV de la LGPDPPSO.

Hoy, más que en ningún otro momento de la historia del país, se estima necesario que las y los mexicanos tengan la certeza de la seguridad de su información personal, en posesión de los Sujetos Obligados de la Ley General. La pandemia derivada del virus del síndrome respiratorio agudo severo tipo-2 (SARS-CoV-2), causante de la enfermedad conocida como COVID-19, ha puesto de manifiesto, por un lado, el interés de la sociedad sobre la debida prestación de los servicos de salud y, por otro, que su información clínica o médica esté protegida, acorde con el marco jurídico nacional.

De ahí, la importancia que reviste brindar herramientas a los responsables de las instituciones de salud pública que les permitan el cumplimiento de las obligaciones en el tratamiento de los datos personales en los expedientes clínicos, a efecto de realizar de manera adecuada la protección de los datos personales que tienen bajo su resguardo y el ejercicio de los derechos ARCO de los derechohabientes.

Bajo esa óptica, el presente documento tiene como propósito emitir sugerencias y recomendaciones, sobre el tratamiento que se da a los datos personales de carácter sensible, contenidos en los expedientes clínicos, en relación con las medidas de seguridad administrativas, técnicas y físicas necesarias acorde a su naturaleza, para evitar que éstos sean vulnerados o lesionados por un mal tratamiento o inadecuado manejo de los datos personales que contengan este tipo de expedientes.

En tal virtud, con fundamento en lo dispuesto por el artículo 89, fracciones I, XII y XIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el INAI emite las presentes recomendaciones para el Tratamiento de los Datos Personales en los expedientes clínicos de las instituciones de salud pública.

CAPÍTULO 1

PROPÓSITOS Y POBLACIÓN OBJETIVO

a) Propósitos

Generar un documento dirigido a las instituciones de salud del sector público, que analice el tratamiento de los datos personales en los expedientes clínicos, a efecto de realizar de manera adecuada la protección de los datos personales que tienen bajo su resguardo y el ejercicio de los derechos ARCO de los derechohabientes.

Coadyuvar en las acciones de promoción, difusión y facilitación en el cumplimento de las obligaciones, por parte de los responsables del sector público en el tratamiento de datos personales.

Armonizar las prácticas en cuanto a la integración, usos y cuidados que se le da al expediente clínico, adecuándose a las obligaciones que refiere la Ley General en el tema de protección de datos personales y la demás normatividad aplicable.

b) Población objetivo

El presente documento se encuentra dirigido a los responsables del manejo de datos personales en las distintas instituciones que componen el sector salud en México, desde instituciones de seguridad social, hasta institutos y hospitales centralizados y sectorizados. Las instituciones de salud públicas, al estar sectorizadas y centralizadas, podrían implementar esquemas para el tratamiento de sus datos personales homologados, incluso eventualmente la portabilidad, pues podrían compartir sus sistemas informativos.

CAPÍTULO 2

EL EXPEDIENTE CLÍNICO

El expediente clínico es el documento en el que se recaba la información de salud y demás datos personales sensibles de una persona física identificada e identificable, y que se integra dentro de todo tipo de establecimiento para la atención médica al sector público.

En septiembre de 2010, se publicó la **Norma Oficial Mexicana NOM-024-SSA3-2010**, que establece los objetivos funcionales y funcionalidades que deberán observar los productos de Sistemas de Expediente Clínico Electrónico para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos en salud.

Esta Norma establece el reconocimiento de la validez de los expedientes electrónicos por sí mismos y no sólo como auxiliares, así como la obligatoriedad de medidas que garanticen la confidencialidad y seguridad de la información.

En el año 2012, se publicó la **Norma Oficial Mexicana NOM-004-SSA3-2012** que, en su introducción, acertadamente señaló un aspecto fundamental consistente en el reconocimiento de la titularidad del paciente sobre los datos que proporciona al personal del área de la salud. En ese sentido, se han considerado aquellos datos que se refieren a su identidad personal y los que proporciona en relación con su padecimiento; a todos ellos, se les considera información confidencial. En ese mismo año, se emitió la **Norma Oficial Mexicana NOM-024-SSA3-2012**, relativa a los sistemas de información de registro electrónico para la salud e intercambio de información en salud, que en su introducción señaló el avance tecnológico que presenta la informática médica, misma que posibilita que los Sistemas de Información de Registro Electrónico para la Salud, entre los que se encuentran los expedientes clínicos electrónicos, puedan intercambiar información útil con este objetivo, además de permitir explotar información de salud pública, lo que facilita la toma de decisiones en el sector salud; con su entrada en vigor, dejó sin efectos a la Norma Oficial Mexicana NOM-024-SSA3-2010.

La citada Norma define al **expediente clínico electrónico,** como el conjunto único de información y datos personales de un paciente, que puede estar integrado por documentos escritos, gráficos, imagenológicos, electrónicos, magnéticos, electromagnéticos, ópticos, magneto-ópticos y de otras tecnologías, mediante los cuales se hace constar en diferentes momentos el proceso de la atención médica, las diversas intervenciones del personal del área de la salud, así como describir el estado de salud del paciente; además de incluir, en su caso, datos acerca del bienestar físico, mental y social del mismo[26].

[26] Información del Expediente Clínico. Disponible para su consulta en: http://inprf.gob.mx/transparencia/archivos/pdfs/como_solicitar_expediente.pdf

En la actualidad, el expediente clínico electrónico forma parte importante del actuar diario en las instituciones de salud, en virtud del continuo avance de las ciencias y la tecnología con la que se cuenta en este Siglo XXI. Debido a ello, la **Norma Oficial** en cita brinda una referencia al respecto y advierte que tiene como propósito establecer con precisión los criterios científicos, éticos, tecnológicos y administrativos obligatorios en la elaboración, integración, uso, manejo, archivo, conservación, propiedad, titularidad y confidencialidad del expediente clínico, el cual se constituye en una herramienta de uso obligatorio para el personal del área de la salud, de los sectores público, social y privado que integran el Sistema Nacional de Salud[27].

De acuerdo con lo definido en el Manual del Expediente clínico electrónico de la SSa, el expediente clínico electrónico, es el conjunto de información ordenada y detallada que recopila cronológicamente todos los aspectos relativos a la salud de un paciente y a la de su familia en un periodo determinado de su vida; representa una base para conocer las condiciones de salud, los actos médicos y los diferentes procedimientos ejecutados por el equipo médico a lo largo de un proceso asistencial.

El expediente clínico electrónico es una fuente de información que amplía el dictamen médico de un experto, conformándose por una descripción de la propedéutica médica aunado a documentos, imágenes, procedimientos, pruebas diversas, análisis e información de estudios practicados al paciente. Mediante el expediente clínico electrónico se puede brindar información más completa a los médicos y personal de salud, así como habilitar la comunicación al instante entre las diferentes unidades médicas.[28]

Los prestadores de servicios de atención médica de los establecimientos de carácter público, social y privado, están obligados a integrar y conservar el expediente clínico. Los establecimientos son solidariamente responsables respecto del cumplimiento de esta obligación, por parte del personal que preste sus servicios en los mismos, independientemente de la forma en que fuere contratado dicho personal.[29]

De lo anterior, se advierte que el expediente es una de las mayores herramientas de certeza jurídica y técnica de los procedimientos médicos que se aplican a los pacientes hoy en día.

[27] Norma Oficial Mexicana NOM-024-SSA3-2012, Del expediente clínico. Publicada en el Diario Oficial de la Federación el 30 de noviembre de 2012.
[28] Manual del Expediente Clínico Electrónico. Secretaría de Salud, Pag. 11 disponible para su consulta en: https://www.who.int/goe/policies/countries/mex_ehealth.pdf
[29] Información del Expediente Clínico. Disponible para su consulta en: https://www.gob.mx/salud/hraepy/acciones-y-programas/informacion-del-expediente-clinico

TITULARES DEL EXPEDIENTE CLÍNICO

Se considera que el expediente clínico físico es propiedad de las Instituciones que brindan atención médica, sin embargo, la información contenida en éste es propiedad de sus titulares, es decir, de los pacientes o beneficiarios que reciben esa atención.

En este sentido, el artículo 5.4 de la NOM-004-SSA3-2012, señala que los expedientes clínicos son propiedad de la institución o del prestador de servicios médicos que los genera, cuando éste, no dependa de una institución. En caso de instituciones del sector público, además de lo establecido en esta norma, deberán observar las disposiciones que en la materia estén vigentes.

Sin perjuicio de lo anterior, **el paciente en tanto aportante de la información y beneficiario de la atención médica tiene derechos de titularidad sobre la información para la protección de su salud, así como, para la protección de la confidencialidad de sus datos,** en los términos de esta norma y demás disposiciones jurídicas que resulten aplicables.

ELEMENTOS PRINCIPALES

El expediente clínico resulta ser un instrumento que garantiza a los beneficiarios que su asistencia sea apropiada y, a su vez, sirve para que los profesionales que realizan funciones de diagnóstico y tratamiento puedan proporcionar una asistencia adecuada al paciente, teniendo para ello permitido el acceso a su expediente clínico.

Para conseguir esta finalidad el expediente clínico debe perseguir y englobar toda la información referente al paciente de manera ordenada y con arreglo a criterios que permitan garantizar la seguridad y el manejo de la información por los profesionales sanitarios que lo necesiten en cada caso en particular.

En las generalidades del expediente clínico tenemos que los prestadores de servicios de carácter médico de cualquier sector, ya sea social, público o privado, deben integrar y observar el expediente clínico, por ello, son considerados solidariamente responsables en su elaboración.

En este sentido, las instituciones de salud por lo menos deberán observar lo que establece la NOM-004-SSA3-2012, para integrar los expedientes clínicos consistente en los siguientes datos:

1) Tipo, nombre y domicilio del establecimiento y en su caso, nombre de la institución a la que pertenece;
2) En su caso, la razón y denominación social del propietario o concesionario;
3) Nombre, sexo, edad y domicilio del paciente; y
4) Los demás que señalen las disposiciones sanitarias.

En tal consideración, el expediente clínico se integrará atendiendo a los servicios genéricos de consulta general, de especialidad, urgencias y hospitalización, y además de los requisitos mínimos señalados en esta norma, así como también se debe observar a los establecidos en las demás Normas Oficiales Mexicanas, respecto a los siguientes temas:

a) Servicios de planificación familiar.
b) Para la prevención y control de la tuberculosis en la atención primaria a la salud.
c) Atención de la mujer durante el embarazo, parto y puerperio y del recién nacido.
d) Para la prevención y control de enfermedades bucales.
e) Para la prevención, detección, diagnóstico, tratamiento, control y vigilancia epidemiológica del cáncer cérvico uterino.
f) Para la prevención, tratamiento y control de la diabetes mellitus en la atención primaria.
g) Para la prestación de servicios de salud en unidades de atención integral hospitalaria médico-psiquiátrica.
h) Para la atención a la salud del niño.
i) En materia de información en salud.
j) Violencia familiar, sexual y contra las mujeres. Criterios para la prevención y atención.
k) Regulación de los servicios de salud. Que establece los criterios de funcionamiento y atención en los servicios de urgencias de los establecimientos de atención médica.

REQUISITOS DEL EXPEDIENTE CLÍNICO

En términos de lo que establece la NOM-004-SSA3-2012, los expedientes clínicos de consulta general y de especialidad deberán contar con los siguientes requisitos:

HISTORIA CLÍNICA.

Deberá elaborarla el personal médico y otros profesionales del área de la salud, de acuerdo con las necesidades específicas de información de cada uno de ellos en particular, a su vez, la historia clínica deberá contar con los siguientes apartados:

a) Interrogatorio: Deberá tener como mínimo: ficha de identificación, en su caso, grupo étnico, antecedentes heredo-familiares, antecedentes personales patológicos (incluido uso y dependencia del tabaco, del alcohol y de otras sustancias psicoactivas) y no patológicos;
b) Exploración física: Deberá tener como mínimo: habitus exterior, signos vitales (temperatura, tensión arterial, frecuencia cardiaca y respiratoria), peso y talla, así como, datos de la cabeza, cuello, tórax, abdomen, miembros y genitales o específicamente la información que corresponda a la materia del odontólogo, psicólogo, nutriólogo y otros profesionales de la salud;
c) Resultados previos y actuales de estudios de laboratorio, gabinete y otros;
d) Diagnósticos o problemas clínicos;
e) Pronóstico;
f) Indicación terapéutica.

NOTA DE EVOLUCIÓN.

Esta documental deberá elaborarla el médico, cada vez que proporciona atención al paciente ambulatorio, de acuerdo con el estado clínico del paciente. Describirá lo siguiente:

a) Evolución y actualización del cuadro clínico (en su caso, incluir abuso y dependencia del tabaco, del alcohol y de otras sustancias psicoactivas);
b) Signos vitales, según se considere necesario;
c) Resultados relevantes de los estudios de los servicios auxiliares de diagnóstico y tratamiento que hayan sido solicitados previamente;
d) Diagnósticos o problemas clínicos;
e) Pronóstico; y
f) Tratamiento e indicaciones médicas; en el caso de medicamentos, señalando como mínimo la dosis, vía de administración y periodicidad.

NOTA DE INTERCONSULTA.

La solicitud deberá elaborarla el médico cuando se requiera y quedará asentada en el expediente clínico. La nota deberá elaborarla el médico consultado y deberá contar con:

a) Criterios diagnósticos;
b) Plan de estudios;
c) Sugerencias diagnósticas y tratamiento.

Entre los elementos a registrarse en el expediente clínico electrónico se encuentran los siguientes:

- Notas ambulatorias.
- Notas hospitalarias.
- Notas quirúrgicas.
- Interconsultas.
- Tratamientos.
- Examen de laboratorio.
- Reporte de radiología.

Resulta importante señalar que, los sistemas de expediente clínico electrónico integran la información del paciente que proviene de diferentes personas y sistemas involucrados, permitiendo la generación de múltiples beneficios.[30]

USOS DEL EXPEDIENTE CLÍNICO

Usos Primarios:

Con la expectativa de que su contenido se convierta en una firme aportación a los esfuerzos y procesos de integración funcional y desarrollo del Sistema Nacional de Salud, esta norma (Norma Oficial Mexicana NOM-004-SSA3-2012), impulsa el uso más avanzado y sistematizado del expediente clínico convencional en el ámbito de la atención médica y orienta el desarrollo de una cultura de la calidad, permitiendo los usos: médico, jurídico, de enseñanza, investigación, evaluación, administrativo y estadístico principalmente.[31]

En tal consideración, el uso del expediente clínico resulta imprescindible, destacando algunos aspectos del estado de salud del paciente, cuyo registro se considera de la mayor relevancia para su correcta integración, buscando que en el proceso de atención se generen los mayores beneficios.

- Provisión de servicios de salud.
- Gestión de la atención médica.
- Soportar los procesos de atención.
- Soportar procesos financieros y administrativos.
- Gestión del cuidado personal.

Usos Secundarios:

- Educación.
- Regulación.
- Investigación: El uso de los expedientes en investigaciones, de naturaleza científica, cae en dos categorías: investigaciones hechas por un miembro del cuerpo médico del hospital e investigaciones hechas por un médico que no es miembro de él. En el primer caso, no es necesario el consentimiento del médico tratante; en el otro caso, el consentimiento del médico es necesario, así como el consentimiento del administrador del hospital.
- Evaluación: Como un documento impersonal, el expediente clínico tiene muchos usos; para esto, sólo se tomará en cuenta el número del expediente y no podrá ser asociado con ningún nombre excepto por referencia al índice privado del hospital. El uso más frecuente del expediente, es en el informe mensual del trabajo del hospital (análisis del servicio hospitalario). Éste es, primeramente, un informe total hecho por el departamento de bioestadística; pero el informe es suplementado por un estudio detallado de los expedientes que dan la información.

[30] Manual del Expediente Clínico Electrónico. Secretaría de Salud. Disponible para su consulta en: https://www.who.int/goe/policies/countries/mex_ehealth.pdf
[31] Norma Oficial Mexicana NOM-004-SSA3-2012, Del expediente clínico, publicada en el Diario Oficial de la Federación de fecha 15 de octubre de 2012.

- Salud pública y seguridad.
- Soporte de políticas.[32]
- Jurídico.
- Administrativo.

Así, la Norma Oficial Mexicana NOM-004-SSA3-2012, representa el instrumento que regula y orienta el desarrollo de una cultura de calidad para el uso médico, jurídico, de enseñanza, investigación, evaluación, administrativo y estadístico.

CLASIFICACIÓN DE LOS EXPEDIENTES CLÍNICOS

- **Expediente físico**

Como se ha dicho, la NOM-004-SSA3-2012 **define al expediente clínico como el conjunto único de información y datos personales de un paciente, que se integra dentro de todo tipo de establecimiento para la atención médica, ya sea público, social o privado, el cual, consta de documentos escritos, gráficos, imagenológicos, electrónicos, magnéticos, electromagnéticos, ópticos, magneto-ópticos y de cualquier otra índole, en los cuales, el personal de salud deberá hacer los registros, anotaciones, en su caso, constancias y certificaciones correspondientes a su intervención en la atención médica del paciente, con apego a las disposiciones jurídicas aplicables.**

En el numeral 5 y subsecuentes de la Norma en comento, se establecen las reglas tendientes a estandarizar el contenido y manejo de los expedientes clínicos, de manera que, independientemente del hospital, centro de salud o consultorio en el que se atienda a un paciente, se deberá cumplir con una serie de principios mínimos que lo hagan funcional.

- **Expediente clínico electrónico**

El expediente clínico ha evolucionado en sus formas de integración, manejo y resguardo; pueden existir distintos formatos, según la institución o el prestador del servicio de salud de que se trate, la realidad es que no se han aprovechado plenamente los avances tecnológicos e informáticos para la recopilación de los datos de los pacientes.

A nivel internacional, el expediente clínico constituye un aspecto esencial dentro del sistema de salud, puesto que sirve para recabar la información sobre la salud de la población. En este sentido, debe considerarse el paso del expediente clínico en papel al electrónico.

El expediente clínico electrónico reporta diversos beneficios al tratamiento de la información en cuanto a que permite a los profesionales de la salud tener un acceso más rápido y de mayor calidad a los datos, lo que se convierte, al mismo tiempo, en una ventaja para los pacientes y usuarios del sistema de salud, puesto que pasan a ser el eje central del sistema de salud y ello permite actuaciones más rápidas y precisas. El expediente clínico electrónico permite una mayor delimitación de los accesos que al mismo se producen por profesionales sanitarios de un lado, y por profesionales administrativos (técnicos y auxiliares) y de gestión de otro, garantizando de este modo una mayor protección a la intimidad del paciente.

Por ello, conviene referir que la Norma Oficial Mexicana NOM-024-SSA3-2012, **define al expediente clínico electrónico como el conjunto de información almacenada en medios electrónicos centrada en el paciente que documenta la atención médica prestada por profesionales de la salud con arreglo a las disposiciones sanitarias, dentro de un establecimiento de salud.**[33]

[33] Disponible para su consulta en: http://www.dgis.salud.gob.mx/descargas/pdf/NOM-024-SSA3-2012.pdf.

La SSa define al expediente clínico electrónico como el conjunto de información ordenada y detallada que recopila cronológicamente todos los aspectos relativos a la salud de un paciente y a la de su familia en un periodo determinado de su vida; representa una base para conocer las condiciones de salud, los actos médicos y los diferentes procedimientos ejecutados por el equipo médico a lo largo de un proceso asistencial.[34]

Tal como se advierte de lo anterior, el expediente clínico electrónico es una fuente de información que amplía el dictamen médico de un experto, conformándose por una descripción de la propedéutica médica aunado a documentos, imágenes, procedimientos, pruebas diversas, análisis e información de estudios practicados al paciente. Mediante el expediente clínico electrónico se puede brindar información más completa a los médicos y personal de salud, así como, habilitar la comunicación al instante entre las diferentes unidades médicas.

El expediente clínico electrónico además utiliza mensajería conforme a los estándares internacionales para interactuar con sistemas como el de laboratorio, banco de sangre, imagenología y hemodiálisis entre otros. Asimismo, permite intercambiar de forma segura información con otras instituciones bajo estándares de interoperabilidad[35].

En México, existe diversidad de ordenamientos legales aplicables al uso de los medios electrónicos, tanto en materia administrativa, fiscal, financiera y comercial, que podrían presentar riesgos vinculados con el derecho a la privacidad respecto a la información generada en formato electrónico para los expedientes clínicos de los usuarios de los servicios de salud, tanto del sector privado como del sector público; por lo que, los datos personales contenidos en el expediente clínico electrónico requieren de una visión multidisciplinaria, al conjugar los esfuerzos y talentos médicos, radiólogos, laboratoristas y personal administrativos entre otros, para la adecuada integración de la información respectiva, debiendo respetar en todo momento el derecho a la privacidad y la obligación de asumir todas las medidas necesarias para salvaguardar la información contenida en ellos.[36]

- **Tipos de sistemas de Expediente Clínico Electrónico[37]**

Los tipos de Sistemas de Expediente Clínico Electrónico que estarán sujetos a la NOM 024-SSA3-2010, serán aquellos destinados a los siguientes usos en el ámbito de la provisión de servicios de salud:

- Consulta Externa.
- Hospitalización.
- Urgencias.
- Farmacia.
- Laboratorio.
- Imagenología.
- Quirófano.

En el caso de que un sólo sistema cubra más de uno de los puntos anteriores deberá atender todas las funcionalidades requeridas para todos los tipos de sistema que debe satisfacer.

- **Ventajas de contar con un Expediente Clínico Electrónico Universal[38]**

Algunos de los impactos más sobresalientes de esta revolución tecnológica sobre la atención de los usuarios serían los siguientes:

[34] Manual del Expediente Clínico Electrónico. Secretaría de Salud, Pag.11, Disponible para su consulta en: https://www.who.int/goe/policies/countries/mex_ehealth.pdf
[35] Manual del Expediente Clínico Electrónico. Secretaría de Salud, Pag.11, Disponible para su consulta en: https://www.who.int/goe/policies/countries/mex_ehealth.pdf
[36] TENORIO. Guillermo, *"Los datos personales en México", Ed Porrúa, p. 217, México, 2012.*
[37] Disponible para su consulta en: http://www.dgis.salud.gob.mx/descargas/pdf/NOM-024-SSA3-2010_SistemasECE.pdf
[38] Boletín CONAMED, Volumen 3, No. 18, 2018.

- Los médicos podrían realizar diagnósticos clínicos más precisos y oportunos gracias a que se tendría acceso inmediato a resultados de laboratorio y de imagenología generados en otras áreas.

- Se podría acceder al expediente desde cualquier unidad médica del Sistema Nacional de Salud a las que acudiera el paciente a requerir atención médica.

- El expediente estaría también accesible al propio paciente desde su propio domicilio para acceder por ejemplo a citas médicas, información sobre sus padecimientos o esquemas de vacunación.

- El historial clínico del paciente se podría registrar desde el nacimiento a lo largo de toda su línea de vida, favoreciendo la atención más oportuna y eficaz en sus diversas etapas.

Por otra parte, la SSa indica que los principales beneficios de la implementación del Expediente Clínico Electrónico son:[39] :

- Incremento en la seguridad de los pacientes y reducción del número de eventos médicos adversos.

- Aumento de las acciones preventivas identificando con oportunidad las necesidades de atención específicas de la población.

- Reducción de costos hospitalarios aumentando el control de episodios agudos en pacientes con enfermedades crónicas.

- Reducción de costos por tratamientos o estudios innecesarios y/o redundantes.

- Mayor compromiso de la población en el cuidado de su salud a través del acceso a su información médica.

- Acceso rápido y sencillo de información que apoye la investigación y desarrollo en salud.

- Reducción del tiempo de los profesionales de la salud dirigido a actividades administrativas.

- Mayor comodidad y confianza en la institución ya que los pacientes pueden disponer de sus datos de forma segura, rápida y confidencial.

- Mayor facilidad para la integración de la información del paciente y para dar continuidad a la asistencia médica.

- Mejor calidad en la prestación de servicios de salud.

- Mejor soporte y apoyo para realizar el análisis de la actividad clínica, la epidemiológica, la docencia, la administración de recursos y la investigación.

- Agilizar la concurrencia de los diversos servicios hospitalarios.

[39] Manual del Expediente Clínico Electrónico. Secretaría de Salud, Pag.22, Disponible para su consulta en: https://www.who.int/goe/policies/countries/mex_ehealth.pdf

CAPÍTULO 3

TRANSFERENCIAS DE LOS EXPEDIENTES CLÍNICOS

El concepto de transferencia es definido por la Ley General[40], en su fracción XXXII del artículo 3, como toda comunicación de datos personales dentro o fuera del territorio mexicano realizada a persona distinta del titular, del responsable o del encargado.

Toda transferencia de datos personales sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo algunas excepciones, como lo son:[41]

- Cuando la transferencia esté prevista en la Ley General u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;
- Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;
- 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;
- Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;
- Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
- Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la presente Ley, o
- Cuando la transferencia sea necesaria por razones de seguridad nacional.

Adicional a lo anterior, la LGPDPPSO prevé excepciones de manera general[42] en las que el responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales; sin embargo, estas eventualmente también podrían aplicarse al tratamiento específico de una transferencia, como lo es:

- ✔ Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en dicha Ley, en ningún caso, podrán contravenirla;
- ✔ Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de

[40] Disponible para su consulta en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
[41] Artículo 65 de la LG PDPP SO, disponible para su consulta en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
[42] Artículo 22 de la LGPDPPSO.

facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

- ✔ Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- ✔ Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- ✔ Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
- ✔ Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
- ✔ Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;
- ✔ Cuando los datos personales figuren en fuentes de acceso público;
- ✔ Cuando los datos personales se sometan a un procedimiento previo de disociación, o
- ✔ Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

Sin embargo, lo dispuesto en el párrafo anterior, no será aplicable en los siguientes casos:[43]

- Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos, o
- Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.

Cuando la transferencia sea nacional, el receptor de los datos personales deberá tratar los datos personales, comprometiéndose a garantizar su confidencialidad y únicamente los utilizará para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente. El responsable sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obligue a proteger los datos personales conforme a los principios y deberes que establece la Ley General y las disposiciones que resulten aplicables en la materia. En toda transferencia de datos personales, el responsable deberá

[43] Artículo 66 de la LGPDPPSO, disponible para su consulta en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se tratan los datos personales frente al titular. Asimismo, el responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, de conformidad con los supuestos señalados con antelación.

El responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General y los Lineamientos Generales; así como establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares y el Instituto.

Lo anterior, también resultará aplicable cuando los datos personales sean tratados por parte de un encargado a solicitud del responsable; así como al momento de realizar transferencias, nacionales o internacionales, de datos personales. El responsable deberá considerar, de manera enunciativa más no limitativa, el desarrollo tecnológico y las técnicas existentes; la naturaleza, contexto, alcance y finalidades del tratamiento de los datos personales; las atribuciones y facultades del responsable y demás cuestiones que considere convenientes. Para el cumplimiento de la presente obligación, el responsable podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de mejores prácticas, o cualquier otro mecanismo que determine adecuado para tales fines.

La falta de uniformidad en los registros médicos y la necesidad de compartirlos entre diferentes sistemas se ha agudizado en los últimos años con el apogeo de muchos proveedores de este tipo de sistema. Es por esto por lo que se hace necesario el uso de estándares que permitan el intercambio correcto y seguro de información médica, así como, la utilización de catálogos estandarizados que unifiquen los datos empleados en distintas instituciones de salud públicas o privadas.

TRANSFERENCIAS INTERNACIONALES

En la mayoría de los casos, la globalización conlleva la necesidad de procesar datos personales, dando lugar a la Transferencia Internacional de Datos (TID) entre diferentes países. Estos tratamientos han de cumplir con las disposiciones legales establecidas en los distintos ordenamientos jurídicos en juego, que tienen por objeto garantizar a la persona, cuyos datos se tratan, su derecho fundamental a la protección de datos, y así, facilitar la realización de las transacciones. internacional, comercial y no comercial.[44]

La normativa mexicana establece que el responsable sólo podrá transferir datos personales fuera del territorio nacional, cuando el receptor o destinatario se obligue a proteger los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las previstas en la Ley General y demás normatividad mexicana en la materia, asi como a los términos previstos en el aviso de privacidad que le será comunicado por el responsable transferente.[45]

En caso de considerarlo necesario, el responsable podrá solicitar la opinión del Instituto respecto aquellas transferencias internacionales de datos personales que pretenda efectuar en cumplimiento de lo dispuesto en la Ley General y los Lineamientos generales de acuerdo con lo siguiente:

- ✔ El responsable deberá presentar su solicitud directamente en el domicilio del Instituto, o bien, a través de cualquier otro medio que se habilite para tal efecto;

[44] Instituto Federal de Acceso a la Información Pública. *"Protección de datos personales: compendio de lecturas y legislación"*. México. Ed. Tiro corto editores, 2010. Pp 98
[45] Artículo 116 de los Lineamientos Generales.

- ✔ La solicitud deberá describir las generalidades y particularidades de la transferencia internacional de datos personales que se pretende efectuar, con especial énfasis en las finalidades que motivan la transferencia; el o los destinatarios de los datos personales que, en su caso, se pretenda transferir; el fundamento legal que, en su caso, obligue al responsable a transferir los datos personales; los datos personales que se pretendan transferir; las categorías de titulares involucrados; la tecnologia o medios utilizados para, en su caso, efectuar la transferencia; las medidas de seguridad aplicables; las cláusulas contractuales, convenios de colaboración o cualquier otro instrumento juridico que se suscribiria con el destinatario o receptor, en caso de que resulte exigible, así como cualquier otra información relevante para el caso concreto;

- ✔ La solicitud podrá ir acompañada de aquellos documentos que el responsable considere conveniente hacer del conocimiento del Instituto;

  Si el Instituto considera que no cuenta con la suficiente información para emitir su opinión técnica, deberá requerir al responsable, por una sola ocasión y en un plazo que no podrá exceder de cinco días contados a partír del día siguiente de la presentación de la solicitud, la informacíón adicional que considere pertinente;

- ✔ El responsable contará con un plazo máximo de diez dias, contados a partir del dia siguiente de la recepción del requerimiento de información adicional, para proporcionar mayores elementos al Instituto con el apercibimiento de que en caso de no cumplir se tendrá por no presentada su consulta;

- ✔ El requerimiento de información adicional tendrá el efecto de interrumpir el plazo que tiene el Instituto para emitir su opinión técnica, por lo que comenzará a computarse a partir del día siguiente a su desahogo;

  El Instituto deberá emitir la opinión técnica que corresponda en un plazo que no podrá
- ✔ exceder de quince días, contados a partir del día siguiente a la recepción de la consulta, el cual no podrá ampliarse, y

  Si el Instituto no emite su opinión técnica en el plazo señalado en la fracción anterior
- ✔ del presente articulo, se entenderá que su opinión no es favorable respecto a la transferencia internacional de datos personales que se pretende efectuar.

CAPÍTULO 4

PORTABILIDAD DE LOS EXPEDIENTES CLÍNICOS

La portabilidad de los expedientes clínicos electrónicos se refiere a la posibilidad de que el expediente clínico de un paciente, registrado en medios electrónicos, pueda ser accesible mediante algún mecanismo tecnológico por alguna unidad médica distinta a la que lo generó. Es importante recordar que, el expediente clínico electrónico en México tiene la misión de crear condiciones necesarias para que, en un mediano plazo, se utilice con estándares y mecanismos innovadores y que cada uno de los mexicanos pueda contar con uno.

Respecto a la portabilidad de datos personales, la Ley General dispone, en su artículo 57, que cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. Cuando el

titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

Asimismo, el artículo 2, fracción V de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales[46] (en adelante Lineamientos de portabilidad), disponen en la parte conducente lo siguiente:

Artículo 2. Además de las definiciones previstas en el artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para los efectos de los presentes Lineamientos se entenderá por:

…

V. Portabilidad de datos personales: Prerrogativa del titular a que se refiere el artículo 57 de la Ley General o los que correspondan en las legislaciones estatales en la materia;

De lo anterior, surge la cuestión *¿Qué es un formato estructurado?*, de conformidad con lo dispuesto en los Lineamientos de portabilidad se entenderá que un formato adquiere esta calidad cuando se trate de un formato electrónico accesible y legible por medios automatizados, con independencia del sistema informático utilizado para su generación y reproducción, de tal forma que, éstos puedan identificar, reconocer, extraer, explotar o realizar cualquier otra operación con datos personales específicos; también, cuando el formato permita la reutilización y/o aprovechamiento de los datos personales y, cuando el formato sea interoperable con otros sistemas informáticos, es decir, cuando el responsable transmisor[47] y el responsable receptor[48] tengan la capacidad para compartir infraestructura y datos personales a través de la conexión de sus respectivos sistemas o plataformas tecnológicas.

En tal consideración, la portabilidad de los datos personales tiene por objeto lo siguiente:

I. Que el titular solicite una copia de sus datos personales que hubiere facilitado directamente al responsable, en un formato estructurado y comúnmente utilizado, que le permita seguir utilizándolos y, en su caso, entregarlos a otro responsable para su reutilización y aprovechamiento en un nuevo tratamiento, sin que lo impida el responsable al que el titular hubiere facilitado los datos personales, y

II. Que el titular solicite la transmisión de sus datos personales a un responsable receptor, siempre y cuando sea técnicamente posible, el titular hubiere facilitado directamente sus datos personales al responsable transmisor y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.

[46] Disponible para su consulta en: http://dof.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018

[47] Los Lineamientos de portabilidad en la fracción VII del artículo 2, definen al Responsable transmisor como:
Cualquier autoridad, dependencia, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, tribunales administrativos, fideicomisos y fondos públicos y partidos políticos, del orden federal, estatal o municipal, que comunica los datos personales, en un formato estructurado y comúnmente utilizado, a un responsable receptor a petición del titular.

[48] Los Lineamientos de portabilidad en la fracción VI del artículo 2, definen al Responsable receptor como:
Cualquier autoridad, dependencia, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, tribunales administrativos, fideicomisos y fondos públicos y partidos políticos, del orden federal, estatal o municipal, que recibe directamente del responsable transmisor los datos personales, en un formato estructurado y comúnmente utilizado, a petición del titular.

Asimismo, la portabilidad procederá cuando se actualicen cada una de las siguientes condiciones:

- Los datos personales se encuentren en un formato estructurado y comúnmente utilizado;
- El tratamiento se efectúe por medios automatizados o electrónicos;
- Los datos personales del titular se encuentren en posesión del responsable o sus encargados;
- Los datos personales conciernan al titular, o bien, a personas físicas vinculadas a un fallecido que tengan un interés jurídico;
- El titular hubiere proporcionado directamente al responsable sus datos personales, de forma activa y consciente, lo cual incluye los datos personales obtenidos en el contexto del uso, la prestación de un servicio o la realización de un trám ite, o bien, aquellos proporcionados por el titular a través de un dispositivo tecnológico, y
- La portabilidad de los datos personales no afecte los derechos y libertades de terceros.

Además de las condiciones señaladas con antelación, cuando se trate de transmisiones de datos personales a un responsable receptor, (siempre y cuando sea técnicamente posible, el titular hubiere facilitado directamente sus datos personales al responsable transmisor y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato), la portabilidad de los datos personales será procedente cuando exista una relación jurídica entre el responsable receptor y el titular; se dé cumplimiento a una disposición legal, o bien, el titular pretenda ejercer algún derecho.

Cabe señalar que, no será objeto de la portabilidad de datos personales aquella inferida, derivada, creada, generada u obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular, como es el caso de los datos que hubieren sido sometidos a un proceso de personalización, recomendación, categorización, creación de perfiles u otros procesos similares o análogos; tratándose de pseudónimos, salvo que éstos se encuentren claramente vinculados al titular y puedan identificarlo o lo hagan identificable cuando el responsable cuente con información adicional que permita su individualización e identificación, y de los datos personales sujetos a un proceso de disociación, de tal manera que no puedan asociarse al titular ni permitir la identificación del mismo, salvo aquellos datos personales que por medio de un procedimiento posterior se puedan asociar de nuevo al titular. Recordemos que la portabilidad de los datos perso es impone la obligación al responsable de procesar, filtrar, seleccionar, extraer y diferenciar los datos personales que son objeto de portabilidad de aquella que no queda comprendida por ésta.

En tal consideración, para que tenga lugar la figura de la portabilidad de datos personales, el responsable deberá considerar, lo siguiente:

- Normas técnicas; como la implementación de mecanismos, medios y procedimientos idóneos que permitan al titular obtener sus datos personales, ya sea de manera personal, por vía electrónica, a través de opciones de descarga establecidas en sus páginas oficiales de Internet, o por cualquier otra tecnología que considere pertinente.

- Informar al titular sobre el o los tipos de formatos estructurados y comúnmente utilizados disponibles, a través de los cuales podrá entregar o transmitir los datos personales al responsable receptor, en función de la naturaleza de los datos personales y la viabilidad para ser objeto de portabilidad conforme

a los requisitos establecidos en los Lineamientos de portabilidad o en caso de que sea técnicamente posible, el titular tendrá la opción de elegir el formato en el que desea se le entreguen los datos personales o sean transmitidos al responsable receptor.

Cabe señalar que, en caso de necesitarse, la solicitud de portabilidad de datos personales deberá contener los siguientes requisitos:

- La petición de solicitar una copia de sus datos personales en un formato estructurado y comúnmente utilizado, o bien, transmitir sus datos personales al responsable receptor. En caso de que el titular solicite al responsable la copia, podrá acompañar a su solicitud el medio de almacenamiento para la elaboración de la misma. En caso de que el titular no proporcione el medio de almacenamiento, el responsable deberá proporcionarlo con el costo razonable que esto implique.

- La explicación general de la situación de emergencia en la que se encuentra el titular, a efecto de que los plazos de respuesta sobre la procedencia o improcedencia de su solicitud y, en su caso, para hacer efectiva la portabilidad de sus datos personales sean menores, y

- La denominación del responsable receptor y el documento que acredite la relación jurídica entre el responsable y el titular; el cumplimiento de una disposición legal o el derecho que pretende ejercer, en caso de que el titular solicite la transmisión de sus datos personales.

Se considera efectiva la portabilidad de datos personales cuando el titular o su representante reciba copia de sus datos personales en un formato estructurado y comúnmente utilizado, que le permita seguir utilizándolos, previo pago del costo del medio de almacenamiento que en su caso corresponda, o cuando el titular o su representante, hubiere sido notificado que el responsable transmisor ante el cual ejerció la portabilidad de sus datos personales transmitió éstos al responsable receptor conforme a sus instrucciones.

Tal como se ha mencionado, el responsable también deberá garantizar, siempre y cuando sea técnicamente posible, la interoperabilidad del formato estructurado y comúnmente utilizado en el que se entreguen los datos personales al titular o los transmita a otros sistemas y bases de datos en posesión del responsable receptor, con la finalidad de que los datos personales puedan ser comunicados y reutilizados de manera uniforme y eficiente, y procurar que los servicios y sistemas electrónicos en su posesión mantengan la capacidad de interoperar con otros sistemas, adoptando protocolos y estándares que permitan el intercambio de datos personales entre diversos sistemas o plataformas tecnológicas, con independencia del lenguaje de programación o plataforma en la que fueron desarrollados.

Así, la interoperabilidad de los expedientes clínicos electrónicos en las unidades médicas del sector salud en México, es la condición mediante la cual sistemas heterogéneos pueden intercambiar procesos o datos, lo cual, se traducirá en la portabilidad de información consistente en datos clínicos, evaluaciones, estadísticas disponibles para la atención oportuna y de calidad entre otros; de consumarse lo anterior, contribuirá a que los usuarios de los servicios de salud cuenten con la posibilidad de obtener la atención médica necesaria en cualquiera de las instituciones del Sistema Nacional de Salud, obteniendo así múltiples beneficios. Sin embargo, para que esta interoperabilidad sea posible, se recomienda que todos cumplan con una serie de criterios denominados estándares de integración del sistema o factores comunes, mismos que se han agrupado como a continuación se indica:

- Estándares de contenidos y estructura (arquitectura)
- Representación de datos clínicos (codificación)
- Estándares de comunicación (formatos de mensajes)
- Seguridad de datos, confidencialidad y autentificación

Como sabemos, en la actualidad los expedientes clínicos electrónicos varían entre los diferentes proveedores de salud, trayendo consigo diversos problemas de interoperabilidad e intercambio de información clínica entre los distintos proveedores y usuarios. Algunos puntos para resaltar de la problemática que se tiene actualmente son:

- Gran porcentaje de la información aún no ha sido digitalizada, debido a que parte de ella no es posible realizarle un análisis de patrón de datos al ser de carácter histórico. Cabe señalar que, por tratarse de documentos elaborados en interés y beneficio del paciente, deberán ser conservados por un periodo mínimo de 5 años, contados a partir de la fecha del último acto médico, en términos de lo que establece la NOM-004-SSA3-2012.
- Información contenida en expedientes clínicos se encuentra aún en papel.
- No existe una estructura bien definida de los datos que deben contener los diversos expedientes clínicos electrónicos.
- El médico no cuenta con la cultura de documentar el expediente clínico electrónico.
- No existen estándares definidos que permitan el intercambio de información entre proveedores de salud.
- Falta de regulación puntual relativa a confidencialidad y transferibilidad en el intercambio de información entre los agentes del sistema de salud.

En caso de que se utilicen estándares internacionales para normalizar los expedientes clínicos electrónicos como lo hemos señalado, éstos vendrían a minimizar los tres factores que condicionan la interoperabilidad entre sistemas, como lo son:

- La necesidad de información médica accesible desde diferentes lugares
- La mecanización de procesos
- Los problemas éticos y legales

En virtud de lo anterior, resulta importante señalar algunos de los beneficios de la interoperabilidad:

- Actualización y disponibilidad de la información médica las 24 horas.
- Lenguaje común para los diversos sistemas médicos en la elaboración del expediente clínico electrónico.
- Información consultable en línea por todas las unidades médicas.
- Utilización de estándares de códigos para intercambio de información entre los diversos sistemas para el manejo del expediente clínico electrónico.

En tal consideración, se sugiere adoptar medidas preventivas por parte de los prestadores de servicios de salud que garanticen que cualquier tecnología utilizada en la asistencia médica, incluyendo sistemas de expedientes clínicos electrónicos, cumplan con los estándares requeridos en materia de protección de datos personales para su recopilación, guarda y almacenamiento. Igualmente, se considera que dentro de esta categoría de medidas se encuentran las certificaciones en materia de salud, o bien, la adopción de mecanismos de autorregulación previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la LGPDPPSO, mecanismos que permiten elevar los estándares previstos en dicho ordenamiento[49]

[49] Opinión realizada por la Dra. Patricia Kurczyn Villalobos en la Revista de la Facultad de Derecho de México, UNAM. "*Contenido e importancia del expediente clínico. Acceso y confidencialidad*". Tomo LXIX, Número 273. enero-abril 2019.

CAPÍTULO 5

RESPONSABLES EN EL MANEJO DEL EXPEDIENTE CLÍNICO

Tal como se advierte de los preceptos legales establecidos en la Ley General, los responsables son cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, tales como las instituciones de salud, que realizan actividades consistentes en la prestación de servicios médicos y que conlleva necesariamente un tratamiento de datos personales de los pacientes que acuden para recibir un diagnóstico o tratamiento médico, o bien, para la realización de algún estudio o análisis clínico.

Cabe recordar, que los datos personales consisten en cualquier información concerniente a una persona física identificada o identificable, entendida como aquélla cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información; mientras que el tratamiento comprende cualquier actividad como su obtención, uso, acceso, manejo, aprovechamiento, transferencia, disposición, divulgación o almacenamiento por cualquier medio.

En tal consideración, la NOM-004-SSA3-2012, como ya se ha señalado con anterioridad, trata el tema del expediente clínico, mismo que tiene como propósito establecer con precisión los criterios científicos, éticos, tecnológicos y administrativos obligatorios en la elaboración, integración, uso, manejo, archivo, conservación, propiedad, titularidad y confidencialidad del expediente clínico, el cual se constituye en una herramienta de uso obligatorio para el personal del área de la salud, de los sectores público y privado que integran el Sistema Nacional de Salud.

Un aspecto fundamental que considerar en esta Norma es, por una parte, que resulta de observancia obligatoria para el personal del área de la salud y los establecimientos prestadores de servicios de atención médica de los sectores público y privado que, en el caso concreto, el presente documento sólo se ciñe a sector público, incluidos los consultorios y, por la otra, que reconoce la titularidad del paciente sobre los datos que proporciona al personal del área de la salud. En ese sentido, se comprende aquellos datos que se refieren a su identidad personal y los que proporciona en relación con su padecimiento y diagnóstico médico, mismos que son considerados como información confidencial.

Por su parte, los numerales 5, 5.1, 5.2, 6, 6.1, 6.2, 6.3 y 6.4 de esa misma Norma, establecen fundamentalmente que los prestadores de servicios de atención médica de los establecimientos de carácter público y privado estarán obligados a integrar y conservar el expediente clínico de sus pacientes, el cual debe contener fundamentalmente lo siguiente:

- Tipo, nombre y domicilio del establecimiento y, en su caso, nombre de la institución a la que pertenece
- La razón y denominación social del propietario o concesionario, en su caso
- Nombre, sexo, edad y domicilio del paciente
- Historia clínica (interrogatorio, exploración física, resultados de laboratorio, diagnóstico, pronóstico, indicación terapéutica)
- Notas de evolución (evolución y actualización del cuadro clínico, signos vitales, resultados relevantes, diagnóstico o problemas clínicos, pronóstico, tratamiento e indicaciones médicas)

- Notas de interconsulta (criterios diagnósticos, plan de estudios, sugerencias diagnósticas y tratamiento)
- Notas de referencia/traslado (establecimiento que envía y receptor, resumen clínico, motivo del envío, impresión diagnóstica y terapéutica empleada).

En ese sentido, no debe pasar desapercibido que, en términos del artículo 3, fracción X de la Ley General, los datos personales sensibles son aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, considerándose como datos personales sensibles de manera enunciativa más no limitativa, los que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual, entre otros.

Por tal motivo, si se toma en cuenta que para la integración del expediente clínico se requiere diversa información de carácter personal de los pacientes, tanto aquella de carácter identificativo, como la referente al estado de salud presente y futuro de los titulares, se puede concluir que las instituciones que prestan servicios de salud, en cualquiera de sus vertientes y enfoques, efectúan el tratamiento de datos personales sensibles.

CAPÍTULO 6

OBLIGACIONES PARA LOS RESPONSABLES EN LA PROTECCIÓN DE DATOS PERSONALES EN LOS EXPEDIENTES CLÍNICOS

La NOM-004-SSA3-2012[50] establece que existe obligación solidaria entre los prestadores de servicios de atención médica de los establecimientos de los distintos sectores y del personal que preste sus servicios en los mismos, de integrar y conservar los expedientes; prevé cuáles deben ser los datos generales que deben asentarse en el expediente clínico tanto del establecimiento o institución de que se trate como del paciente; señala que los expedientes clínicos son propiedad del prestador de servicios médicos, esto es, de la institución o el médico particular, según sea el caso, sin embargo, dispone que los pacientes tendrán derechos de titularidad sobre la información para la protección de su salud, así como para la protección de la confidencialidad de sus datos; y establece también que, al tratarse de instrumentos expedidos en beneficio de los pacientes, los expedientes deberán conservarse por un mínimo de cinco años contados a partir del último acto médico.

Otro punto importante a considerar en la Norma antes señalada, es el relativo al manejo de la información por parte de los responsables, se da cuando un expediente clínico pretenda ser

[49] Disponible para su consulta en: https://dof.gob.mx/nota_detalle_popup.php?codigo=5272787

utilizado con fines de docencia o investigación, en el que los datos personales que posibiliten la identificación del paciente deberán ser omitidos para no ser divulgados, a menos que exista autorización escrita del paciente; dispone también que no se dará información del expediente clínico a terceros, a menos que hubiera una solicitud por escrito del paciente, tutor, representante legal o médico debidamente autorizado por el paciente.

Como se advierte de lo anterior, tanto los médicos y profesionales, como aquéllas otras personas que laboren o tengan acceso a la información y documentación clínica del paciente, deben guardar la reserva debida. En este sentido, la Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos, en su capítulo 3,[51] establece lo siguiente:

"3.2… Los individuos u órganos que trabajen en representación de profesionales sanitarios recogiendo y procesando datos médicos deben estar sujetos a las mismas normas de confidencialidad que pesan sobre los profesionales sanitarios o a normas de confidencialidad comparables.

Los administradores de archivos que no son profesionales sanitarios sólo deben recoger y procesar datos médicos cuando estén sujetos a normas de confidencialidad comparables a las que pesan sobre el profesional sanitario o a medidas de seguridad igualmente eficaces proporcionadas por la Ley nacional".

Además de las ya señaladas, otras de las obligaciones de los médicos, profesionales sanitarios y de aquellas personas que elaboren o tengan acceso a la información y documentación clínica serán las siguientes:

- Observar las medidas de seguridad que se establezcan para los sistemas de datos personales en los que se almacenen los datos de salud
- Informar a los beneficiaros para que puedan decidir libremente sobre su atención
- Informar a los beneficiarios acerca de los riesgos y alternativas de los procedimientos terapéuticos y quirúrgicos que se le indiquen o apliquen, así como, de los procedimientos de consultas o quejas
- Solicitar el consentimiento de los beneficiarios cuando se les informe acerca de los riesgos y alternativas de los procedimientos terapéuticos y quirúrgicos
- Cumplir con el resto de las obligaciones que puedan ser exigibles como consecuencia del tratamiento o el acceso a datos personales, bien sean establecidas por la normativa sobre el expediente clínico o por la normativa que regula la protección de datos personales.

En México, la Norma Oficial Mexicana NOM-024-SSA3-2010[52] establece también que la información contenida en los sistemas de los expedientes clínicos electrónicos será manejada con discreción y confidencialidad, de acuerdo a la normatividad aplicable, y a los principios científicos y éticos que orientan la práctica médica, dicha información podrá ser dada a conocer al paciente, o a quien tenga facultad legal para decidir por él, y en su caso a terceros mediante orden de la autoridad judicial, o administrativa competente, a la Comisión Nacional de Arbitraje Médico, o a las Comisiones Estatales de Arbitraje Médico correspondientes.

Cabe señalar que, la doctrina de manera general acepta las siguientes excepciones al deber de confidencialidad por parte de los responsables:[53]

[51] Disponible para su consulta en: https://www.bioeticaweb.com/recomendaciasn-nao-r-97-5-de-13-de-febrero-de-1997-del-comitac-de-ministros-del-consejo-de-europa-a-los-estados-miembros-sobre-protecciasn-de-datos-macdicos/
[52] Disponible para su consulta en: http://www.dgis.salud.gob.mx/descargas/pdf/NOM-024-SSA3-2010_SistemasECE.pdf
[53] MUREDU. Mariana, *"La Regulación Jurídica del Expediente Clínico Electrónico"*, pp 118, México, 2017.

- El consentimiento expreso del interesado, si es adulto, o de sus representantes legales si es menor de edad o incapacitado.

- Que la información sea compartida con otros facultativos o profesionales de la salud en el medio hospitalario, cuando ello sea necesario para la elaboración de pruebas o de otros tratamientos para garantizar la calidad de la atención médica al paciente.

Adicional a lo anterior, si se toma en consideración que la Ley General establece que los responsables tienen la obligación de implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la referida Ley, así como, rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e Instituto o los Organismos garantes, según corresponda, caso en el cual, deberá observar lo establecido en la Constitución y Tratados Internacionales en los que el Estado mexicano sea parte y cuando no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

Entre los mecanismos a los que se hace referencia en el párrafo anterior, están al menos los siguientes:

- Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;
- Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;
- Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
- Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
- Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
- Establecer procedimientos para recibir y responder dudas y quejas de los titulares;
- Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y
- Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

Al respecto, se señalan las obligaciones del personal responsable de llevar el expediente clínico establecidas en la NOM-004-SSA3-2012,[54] mismas que se traducen en lo siguiente:

1. Integrar expedientes clínicos por cada paciente.
2. Integrarlos cumpliendo con los requisitos que establece la propia NOM-004-SSA3-2012.

[54] Disponible para su consulta en: http://dof.gob.mx/nota_detalle_popup.php?codigo=5272787

3. Ponerlos a disposición de las personas que de acuerdo con la propia NOM-004-SSA3-2012 pueden acceder a su información.

La obligación enunciada en primer lugar, recaerá sobre la institución de salud y específicamente sobre el departamento que lleve a su cargo el registro de los pacientes que ingresan. Asimismo, cada vez que un médico reciba un nuevo paciente deberá abrir un expediente clínico particular para ese paciente.

Respecto a la segunda obligación enunciada, esta deberá ser cumplida, primero por el médico tratante y posteriormente por su equipo de apoyo. Esto vale tanto para las instituciones de salud públicas como para las consultas en clínicas particulares.

Por último, cada institución de salud pública deberá tener una Unidad de Transparencia, que será la encargada de proporcionar la información requerida por los particulares. En el caso de los médicos particulares, ellos mismos tendrán la obligación de proporcionar la información que se les solicite.

Así, respecto del expediente clínico se puede incurrir en dos tipos de responsabilidad: la primera hace referencia a la obligación que establece la NOM-004-SSA3-2012[55] de llevar expedientes clínicos, y la segunda, a la de acceso a su información.

Respecto de la primera, su incumplimiento se puede actualizar en los siguientes casos:

- No integrar expedientes clínicos
- Integrarlos de manera deficiente o incompleta en términos de la NOM-004-SSA3-2012
- Permitir que lo roben
- Maltratarlo o destruirlo
- Alterarlo sin consentimiento de los médicos o del propio paciente

La segunda forma por la que se puede incurrir en responsabilidad, tiene que ver con el acceso a la información contenida en el expediente clínico, y se puede actualizar en los siguientes casos:

1. No entregar el expediente clínico o cualquier información requerida del mismo al paciente, su representante legal o persona autorizada por el propio paciente, así como a autoridades judiciales o administrativas

2. Entregar el expediente clínico o cualquier información que se contenga en este a terceros, sin contar con la autorización del paciente o su representante legal para hacerlo, pues ello vulnera el principio de confidencialidad de los datos del paciente y el secreto médico

Como se ha señalado, resulta una obligación para los médicos (médico tratante, los médicos especialistas, los cirujanos, los residentes, las enfermeras) y las instituciones de salud la integración correcta de los expedientes clínicos, así como su custodia y conservación. El médico también tiene derecho a exigir a cada uno de los actores registre de forma clara en el expediente respectivo todos los actos que realiza en favor del paciente, toda vez que, este instrumento es la prueba material mediante la cual el médico, en caso de que exista alguna controversia respecto de su actuación, podrá demostrar que su actuación fue conforme a la lex artis médica, por lo que al no ser el único que participa en su integración requiere la actuación responsable de los demás participantes.[56]

[55] Disponible para su consulta en: http://dof.gob.mx/nota_detalle_popup.php?codigo=5272787
[56] MUREDU. Mariana, "*La Regulación Jurídica del Expediente Clínico Electrónico*", pp 146, México, 2017.

En general, todo profesional que asista en el ámbito sanitario a pacientes o usuarios estará obligado, además de a prestar correctamente sus técnicas como profesional sanitario, a respetar las decisiones que libre y voluntariamente adopte el paciente y cumplir con los deberes de información y de documentación clínica. Estos últimos, inciden directamente en el tratamiento de datos personales, lo que determina la necesidad de garantizar la aplicación de la normativa sobre protección de datos.

CAPÍTULO 7

EL TRATAMIENTO DE LOS DATOS PERSONALES POR PARTE DE LOS ENCARGADOS EN LOS EXPEDIENTES CLÍNICOS

La Ley General en la fracción XV del artículo 3,[57] define al encargado como la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable. Si bien el responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas por la normatividad aplicable, así como, establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares y el Instituto; no se debe olvidar que lo anterior también le resultará aplicable cuando los datos personales sean tratados por parte de un encargado a solicitud del propio responsable o al momento de realizar transferencias, nacionales o internacionales de datos personales.

En tal consideración, el encargado tendrá las siguientes características:

- Puede ser una persona física o jurídica;
- Del ámbito público o privado;
- Ajeno a la organización del responsable, es decir, los trabajadores que forman parte de la estructura del responsable no son encargados;
- Puede tratar los datos solo o de manera conjunta con otras personas;

Así, el encargado es un prestador de servicios que realiza actividades de tratamiento de datos personales a nombre y por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. El responsable será corresponsable por las vulneraciones de seguridad ocurridas en el tratamiento de datos personales que efectúe el encargado a nombre y por cuenta de éste.

El encargado deberá realizar las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los términos fijados por el responsable y la relación entre éstos deberá estar formalizada mediante un instrumento jurídico que decida el responsable, que permita acreditar la existencia de la relación jurídica, su alcance y contenido, como por ejemplo un contrato, cláusulas contractuales, acuerdos, convenios u otros de conformidad con la normativa que le resulte aplicable. En todo caso, los acuerdos que se alcancen entre el responsable y el encargado deberán ser acordes con lo previsto en el aviso de privacidad que definió las condiciones del tratamiento de los datos personales y no deberá contravenir lo estipulado en la Ley General y demás disposiciones aplicables.

En el contrato o instrumento jurídico que decida el responsable se deberán prever, al menos,

[57] Disponible para su consulta en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:

- Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
- Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
- Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
- Guardar confidencialidad respecto de los datos personales tratados;
- Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
- Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Además de las cláusulas generales señaladas con antelación, para la prestación de los servicios del encargado, el responsable deberá prever en el contrato o instrumento jurídico las siguientes obligaciones:

- Permitir al Instituto o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales;
- Colaborar con el Instituto en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la Ley General y los presentes Lineamientos generales, proporcionando la información y documentación que se estime necesaria para tal efecto, y
- Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.

Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el tratamiento de los datos personales, asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable.

Como ejemplo, la figura del encargado tendría lugar cuando un organismo desconcentrado en materia de salud contrata a una empresa especializada para encargarse de manipular el sistema de datos personales sensibles con el que se crearán los expedientes clínicos electrónicos de sus pacientes, en virtud de la prestación del servicio, el sujeto obligado (responsable) le comunica los datos personales sensibles de los pacientes para que elabore los expedientes clínicos electrónicos, en este supuesto estaríamos hablando de que la empresa que elabora dichos documentos es la encargada del tratamiento.

De conformidad con lo establecido en la Ley General,[58] el encargado también podrá subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del responsable, siempre que cuente con la autorización de éste, es decir, que se establezca en el instrumento jurídico mediante el cual se haya formalizado la relación entre responsable y encargado. Una vez obtenida la autorización del responsable, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que

[58] Artículo 61 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, disponible para su consulta en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

permita acreditar su existencia, alcance y contenido. Es importante que el encargado prevea en este instrumento que la persona subcontratada asuma las mismas obligaciones que se establezcan para el encargado.

Es común y habitual que en la práctica se presenten casos en los que exista una subcontratación de servicios cuando el encargado del tratamiento tiene que recurrir, a su vez, a otras personas físicas o morales que le prestan algún servicio que implica el acceso a los datos personales del responsable; ejemplo de lo anterior, tiene lugar cuando un responsable ha contratado a un encargado un servicio de software para la realización de estudios clínicos, que implica el tratamiento de datos personales y, este último hace, uso de los servicios de otra persona jurídica para almacenar los datos personales en la nube, este último tratamiento de datos implica una subcontratación, que tendrá que estar autorizada por el responsable. Cabe señalar que, el responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General y demás disposiciones que resulten aplicables en la materia. Los proveedores de servicios de cómputo en la nube y otras materias a que se refieren los artículos 3, fracción VI, 63 y 64 de la Ley General, tendrán el carácter de encargados.

En caso de que el encargado y el subcontratado incumplan las instrucciones del responsable y decidan y determinen por sí mismos los fines, medios y demás cuestiones relacionadas con el tratamiento de los datos personales, asumirán el carácter de responsables conforme a la legislación en la materia que le resulte aplicable en función de su naturaleza pública o privada.

En consecuencia, tal como se advierte de lo anterior, el responsable tiene obligaciones respecto de la relación que establezca con los encargados que traten datos a su nombre, por lo que siempre deberá considerar lo siguiente:

1. La relación con los encargados debe formalizarse mediante contrato o instrumento jurídico, que permita acreditar su existencia, alcance y contenido

2. Incluir en el contrato o instrumento jurídico, al menos las siguientes cláusulas con encargado:

- El tratamiento de datos personales debe realizarse conforme a las instrucciones del responsable;
- El encargado no debe tratar los datos personales para finalidades distintas a las instruidas por el Responsable;
- El encargado debe Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
- El encargado debe informar al responsable cuando suceda una vulneración a los datos personales;
- La obligación de guardar confidencialidad de los datos personales tratados;
- Suprimir o devolver los datos personales una vez cumplida la relación jurídica salvo que exista una previsión legal que exija la conservación de los datos personales;
- No debe el encargado transferir los datos personales, a menos que sea instrucción del responsable, o dicha comunicación derive de una subcontratación, o cuando derive de un mandato expreso de la autoridad competente;
- Permitir al INAI o al Responsable, realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales; Colaborar con el INAI en las investi-

gaciones previas y verificaciones de acuerdo con lo dispuesto en la Ley General y los Lineamientos Generales, el encargado tiene la obligación de proporcionar la información y documentación necesaria, y

- El encargado para acreditar el cumplimiento de obligaciones puede generar, actualizar y conservar la documentación necesaria.

3. El responsable debe autorizar las subcontrataciones que realicen los encargados y que involucren el tratamiento de datos personales.

4. Informar al encargado que el contrato o el instrumento jurídico mediante el cual se formalice la subcontratación deberá incluir cláusulas con las obligaciones antes señaladas.

Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla al menos con lo siguiente:

a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable;
b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y
d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio;

Asimismo, que cuente con mecanismos, al menos para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
c) Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;
d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, y
e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la Ley General y demás disposiciones que resulten aplicables en la materia.

CAPÍTULO 8

DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN (ARCO) EN EL EXPEDIENTE CLÍNICO

Respecto a los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) que tiene el titular de los datos personales o derechohabiente, la Ley General señala que en todo momento el titular o su representante podrán solicitarlos al responsable del tratamiento de los datos personales y el ejercicio de cualquiera de ellos no es requisito previo, ni impide el ejercicio de otro. Asimismo, dispone que el titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, a conocer la información relacionada con las condiciones y generalidades de su tratamiento, y lo faculta para conocer qué datos tiene sobre él y a quiénes se van a comunicar.

En México, la Norma Oficial Mexicana NOM-004-SSA3-2012, establece que los expedientes clínicos son propiedad de la institución o del prestador de servicios médicos que los genera, cuando éste, no dependa de una institución.[59] En caso de instituciones del sector público, además de lo establecido en esta norma, deberán observar las disposiciones que en la materia estén vigentes.

Sin perjuicio de lo anterior, el paciente en tanto aportante de la información y beneficiario de la atención médica tiene derechos de titularidad sobre la información para la protección de su salud, así como, para la protección de la confidencialidad de sus datos, en los términos de esta Norma y demás disposiciones jurídicas que resulten aplicables.

En consecuencia, en principio el paciente tiene derecho de acceso a la documentación de su historial clínico y a la información contenida en él, y la dependencia o entidad debe otorgarlo. Tratándose de una solicitud de acceso a datos personales, el Titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan y el responsable deberá atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales de dicha manera, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

Adicional a lo anterior, el titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.

Asimismo, el titular tiene derecho a solicitar la cancelación de sus datos personales, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados. En esta solicitud de cancelación, el titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros, expedientes, sistemas o bases de datos del responsable.

El titular también podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo cuando se trata de evitar que su persistencia cause un daño o perjuicio al titular y sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias

[59] Numeral 5.4 de la Norma Oficial Mexicana NOM-004-SSA3-2012, disponible para su consulta en: https://dof.gob.mx/nota_detalle_popup.php?codigo=5272787

sexuales, fiabilidad o comportamiento. En este caso, el titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el ejercicio de este derecho de oposición.

La Ley General dispone que para el ejercicio de los derechos ARCO el trámite deberá ser gratuito y sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío y en la solicitud para el ejercicio de estos derechos no podrán imponerse mayores requisitos que los siguientes:

- Nombre del titular;
- Domicilio del titular o cualquier otro medio para recibir notificaciones;
- Documentos que acred iten la identidad del titular;
- Documentos que acrediten la personalidad e identidad de su representante, en su caso;
- Área responsable que trata los datos personales y ante el cual se presenta la solicitud, de ser posible;
- Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;
- Descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y
- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

En la solicitud para el ejercicio de los derechos ARCO, el titular podrá acreditar su identidad a través de los siguientes medios:

- Identificación oficial;
- Instrumentos electrónicos o mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias que permitan su identificación fehacientemente, o
- Mecanismos establecidos por el responsable de manera previa, siempre y cuando permitan de forma inequívoca la acreditación de la identidad del titular.

Cabe señalar, que la identidad de los menores de edad se podrá acreditar mediante su acta de nacimiento, Clave Única de Registro de Población (CURP), credenciales expedidas por instituciones educativas o instituciones de seguridad social, pasaporte, o cualquier otro documento oficial utilizado para tal fin. El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos siempre que el titular de los mismos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para tal efecto.

En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se ha hecho referencia y el Instituto o los organismos garantes no cuenten con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación. Transcurrido el plazo, en caso de no desahogar la prevención, se tendrá por no presentada la referida solicitud. Cabe señalar que dicha prevención tiene el efecto de interrumpir el plazo que tiene el Instituto, o

en su caso, los organismos garantes, para resolver la solicitud de ejercicio de los derechos ARCO.

Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del responsable, en este caso en concreto, de la institución de salud pública que atienda al paciente o que el titular considere competente, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias.

Las únicas causas en las que el ejercicio de los derechos ARCO no será procedente son:

- Cuando el titular o su representante no estén debidamente acreditados para ello;
- Cuando los datos personales no se encuentren en posesión del responsable;
  Cuando exista un impedimento legal;
- Cuando se lesionen los derechos de un tercero;
- Cuando se obstaculicen actuaciones judiciales o administrativas;
- Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;
- Cuando la cancelación u oposición haya sido previamente realizada;
  Cuando el responsable no sea competente;
- Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;
- Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;
- Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o
- Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

En todos los casos anteriores, el responsable deberá informar al titular el motivo de su determinación, en el plazo de hasta veinte días y podrá ser ampliado por una sóla vez hasta por diez días cuando así lo justifiquen las circunstancias, siempre y cuando se le notifique al titular dentro del plazo de respuesta. En caso de resultar procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta al titular por el mismo medio en que se llevó a cabo la solicitud.

Contra la negativa de dar trámite a toda solicitud para el ejercicio de los derechos ARCO o por falta de respuesta del responsable, procederá la interposición del recurso de revisión ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

CAPÍTULO 9

RECOMENDACIONES GENERALES PARA EL TRATAMIENTO DE LOS DATOS PERSONALES DEL EXPEDIENTE CLÍNICO Y AUTORIDADES REGULADORAS

Como se ha mencionado a lo largo del presente documento, los derechos y obligaciones relacionados con el tratamiento de los datos personales contenidos en un expediente clínico para el caso de las instituciones de salud públicas, se encuentran contenidos en la Ley General,[60] la LGS[61], las Normas Oficiales Mexicanas como la NOM-004-SSA3-2012,[62] principalmente.

En este Capítulo plasmamos cuáles serían las recomendaciones que este órgano garante sugiere para el tratamiento de los datos personales en los expedientes clínicos de las instituciones de salud pública, entendiéndose por Tratamiento, a cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales (artículo 3, fracción XXXIII de la Ley General).

Como se ha mencionado, los expedientes clínicos contienen una serie de datos personales, en su mayoría sensibles, los cuales son registrados en los expedientes clínicos que se elaboran por los responsables para su utilización en el seguimiento de salud de sus pacientes, llevando un registro de los mismos, conservándolos o en su caso haciendo transferencia de los mismos, de lo que se desprende claramente que los responsables realizan un conjunto de operaciones a través de diversos procedimientos, lo que deriva que éstos son los responsables del tratamiento de los Datos Personales contenidos en los expedientes clínicos.

Para el tratamiento de los Datos Personales en los expedientes clínicos, se debe atender a los siguientes principios:

TRATAMIENTO

LICITUD Cumplir con los deberes prescritos en las normas jurídicas. Respetado en todo momento los derechos de los titulares de los datos personales.
FINALIDAD. El tratamiento únicamente será para el fin que se ha determinado, relacionado con las actividades propias del responsable de la salud.
PROPORCIONALIDAD. El responsable únicamente deberá solicitar los datos necesarios para el fin que se persigue.
CALIDAD. La calidad de los datos satisface las necesidades requeridas para el fin que se ha determinado.
INFORMACIÓN. Hacer del conocimiento a los titulares, previo a la solicitud de los datos personales, cuál es el tratamiento que se dará a los mismos.
CONSENTIMIENTO. Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.
LEALTAD. Bajo este principio la obtención de los datos personales no podrá hacerse a través de medios engañosos ni fraudulentos.
RESPONSABILIDAD. Con este principio se establece la obligación de los responsables de velar por el cumplimiento del resto de los principios y adoptar las medidas necesarias para su aplicación; es decir, velar por la protección de los datos personales.

[60] Disponible para su consulta en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
[61] Disponible para su consulta en: http://www.diputados.gob.mx/LeyesBiblio/ref/lgs.htm
[62] Disponible para su consulta en: https://dof.gob.mx/nota_detalle_popup.php?codigo=5272787

De tal manera, que los responsables de la salud en las instituciones del sector público deberán observar las disposiciones que en la materia estén vigentes respecto a los expedientes clínicos y el paciente como aportante de la información y beneficiario de la atención médica, tiene derechos de titularidad sobre la información para la protección de su salud, así como para la protección de la confidencialidad de sus datos. Estos datos personales proporcionados por el paciente o por terceros al personal de salud y que se encuentran contenidos en el expediente clínico, deberán ser manejados con discreción por todo el personal del lugar, atendiendo a los principios científicos y éticos que orientan la práctica médica, así como, las disposiciones establecidas en la Ley General y las Normas Oficiales Mexicanas.

Los datos personales contenidos en el expediente clínico que posibiliten la identificación del paciente, en términos de los principios científicos y éticos que orientan la práctica médica, no deberán ser divulgados o dados a conocer. Tratándose de publicación o divulgación de datos personales para efectos de literatura médica, docencia, investigación o fotografías, que posibiliten la identificación del paciente, se requerirá la autorización escrita del mismo y se adoptarán las medidas necesarias para que éste no pueda ser identificado. Los datos personales podrán ser proporcionados a terceros cuando medie la solicitud escrita del paciente, el tutor, representante legal o de un médico debidamente autorizado por el paciente, el tutor o representante legal.

Asimismo, los profesionales de la salud se encuentran obligados a proporcionar información verbal al paciente, a quién ejerza la patria potestad, la tutela, representante legal, familiares o autoridades competentes y cuando se requiera un resumen clínico u otras constancias del expediente el titular o su representante legal deberá solicitarlo por escrito de la manera en la que ha quedado explicada en el cuerpo del presente documento.

Al respecto, los criterios establecidos en la Norma antes referida, inciden en la calidad de los registros médicos, de los servicios y de sus resultados, esta Norma ratifica la importancia de que la autoridad sanitaria garantice la libre manifestación de la voluntad del paciente de ser o no atendido a través de procedimientos clínicos o quirúrgicos, para lo cual, el personal de salud debe recabar su consentimiento, previa información y explicación de los riesgos posibles y beneficios esperados.

Una vez referido lo anterior, es preciso indicar que **el estado de salud** refiere a las condiciones médicas (salud física y mental), sus experiencias en cuanto a reclamaciones, obtención de cuidados de salud, historia clínica, información genética, elegibilidad e incapacidad de un titular de los datos; por tanto, se trata de un dato personal que es confidencial, conforme al artículo 3, fracción X de la Ley General, se trata de **un dato personal sensible.**

En todo caso, los datos personales sensibles forman parte de un determinado grupo de informaciones susceptibles de una reconsideración respecto a una categoría general y homogénea por sus especiales peculiaridades y características, que los constituye en una categoría especial de datos, protegidos bajo reglas específicas. Por ello, en la práctica, se busca restringir aún más la posibilidad legal de su tratamiento. De un lado, mediante herramientas normativas, como la imposibilidad de crear bases de datos con el exclusivo fin de tratar estos datos, y con la exigencia en nuestra normatividad de un consentimiento reforzado para su tratamiento, así como el establecimiento de medidas de seguridad reforzadas.[63]

[63] Isabel Davara Fernández de Marcos, Gregorio Barco Vega y Alexis Cervantes Padilla. En la definición de Dato personal sensible del Diccionario de Protección de Datos Personales. Conceptos Fundamentales, disponible para su consulta en: https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

De tal suerte que, conforme al numeral 7 de la citada Ley General, por regla general **no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso** de su titular o en su defecto, se trate de los casos establecidos de la ley.

En el sistema jurídico mexicano, en la LGPDPSO, se establece en el artículo 3, fracción VIII, que el consentimiento es la manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

En este sentido, el consentimiento es la manifestación de la voluntad del titular de los datos personales, que permite el tratamiento de su información personal. Adicionalmente, con fundamento en el artículo 20 de la LGPDPPSO, la exteriorización y otorgamiento del consentimiento por parte de los titulares de la información personal, debe cumplir con las siguientes características:[64]

- ✔ **Previo:** cuando los datos personales se obtengan de forma personal o directamente del titular.
- ✔ **Libre:** sin que medie error, mala fe, dolo o violencia que impidan al titular conocer los usos a que serán sometida su información personal y, en consecuencia, puedan afectar o viciar su manifestación de voluntad.
- ✔ **Específico:** la autorización que se solicite debe estar vinculada a una o varias finalidades que motiven el tratamiento de los datos personales.
- ✔ **Informado:** el titular tiene conocimiento del aviso de privacidad, previo a que sus datos personales sean tratados.

En seguimiento a lo anterior, el artículo 14 de los Lineamientos Generales[65], deja patente que el consentimiento será expreso cuando la voluntad del titular se manifieste de **forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.**

Para la obtención del consentimiento expreso, el responsable deberá facilitar al titular un medio sencillo y gratuito a través del cual pueda manifestar su voluntad, el cual le permita acreditar de **manera indubitable** y, en su caso, documentar que el titular otorgó su consentimiento ya sea a través de una declaración o una acción afirmativa clara.

En el marco normativo de datos personales en el sector público, el consentimiento expreso está normado por el artículo 21 de la Ley General, en correlación con los artículos 14, 16 y 17 de los Lineamientos Generales, que respectivamente señalan que, cuando lo exija alguna disposición normativa, los responsables en el ámbito público deberán obtener el consentimiento expreso de los titulares de la información, en el cual, la voluntad de los individuos se exteriorizará de forma indubitable, a través de los siguientes recursos:

- ✔ Verbal
- ✔ Escrito
- ✔ Medios electrónicos
- ✔ Medios ópticos
- ✔ Signos inequívocos
- ✔ Cualquier otra tecnología

Con la finalidad de brindar mayores elementos de comprensión, el marco normativo aplicable estableció que el c**onsentimiento expreso de manera verbal,** se actualiza cuando los **titulares de los datos personales** manifiestan su voluntad oralmente ante el responsable de carácter público o mediante el uso de cualquier tecnología que permita la interlocución.

[64] Estudio titulado. Consentimiento en el tratamiento de datos personales, elaborado por la Dirección General de Normatividad y Consulta de la Secretaría de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
[65] Disponible para su consulta en: http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf

Por otra parte, el **consentimiento expreso en forma escrita**, se actualiza cuando los titulares de los datos personales exteriorizan su voluntad a través de un documento físico o electrónico (en el entorno digital) en el que se haga constar lo siguiente:

- Declaración en sentido afirmativo
- Firma autógrafa
- Huella dactilar
- Firma electrónica
- Cualquier otro mecanismo autorizado
- por la normatividad aplicable

Por ello, se recomienda que los sujetos obligados, que tratan datos personales sensibles relativos a su estado de salud, deben contar con el consentimiento expreso de su titular o, en su caso, representante legal.

Cabe señalar que, las instancias de salud deben extremar precauciones en el tratamiento de los datos personales de pacientes y de aquéllos relacionados con el estado de salud actual o futuro de una persona, toda vez que éstos son considerados de carácter sensible, por lo que revelarlos puede poner en riesgo su privacidad y ser motivo de discriminación.

En razón de lo anterior, se debe contar con estrictas medidas de seguridad administrativas, físicas y técnicas para evitar cualquier pérdida, destrucción, robo o uso indebido de los mismos, y cumplir así, con los principios, deberes y obligaciones establecidas en las leyes de protección de datos personales vigentes.

a) MEDIDAS Y RECOMENDACIONES

Con la finalidad de prevenir riesgos que pudieran vulnerar la seguridad, confidencialidad y disponibilidad y respetar la privacidad de los pacientes, a continuación, se proporcionan algunas medidas o recomendaciones para el tratamiento adecuado de los datos personales:

- Los responsables deberán en todo momento observar lo dispuesto en las disposiciones normativas vigentes, así como los principios Internacionales.

- Las medidas implementadas ante cualquier epidemia, pandemia o contingencia que implique el tratamiento de datos personales relacionados con la salud, deben ser necesarias y proporcionales, atendiendo las instrucciones de la SSa y autoridades competentes.

- Se debe informar con claridad quién, para qué y cómo se tratarán los datos personales obtenidos. El titular debe conocer en todo momento las finalidades para las cuáles serán recabados y tratados sus datos personales.

- El responsable previo al tratamiento deberá poner a disposición del titular el Aviso de Privacidad correspondiente, mismo que deberá contener los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO.

- Se deben recabar solamente los datos personales mínimos necesarios para lograr el propósito por el cual fueron implementadas, como lo es prevenir o contener la propagación de algún virus y, en su caso, brindar la atención, diagnóstico y tratamiento médico correspondiente.

- Los datos personales recabados por el responsable con el fin de prevenir o contener la propagación de alguna enfermedad o virus no deben utilizarse para propósitos distintos.

- Se debe solicitar al paciente su consentimiento expreso y por escrito para el tratamiento de datos personales de salud, salvo que se actualice alguna de las cau-

sales de excepción, como cuando sean indispensables para la atención médica, mientras el titular no esté en condiciones de otorgar el consentimiento.

- Los datos personales no deben ser obtenidos por medios fraudulentos ni engañosos.

- Los datos deben ser tratados lícitamente y de conformidad con la normativa aplicable por el profesional de la salud o establecimiento de atención médica, independientemente de que éste tenga naturaleza pública, privada o social.

- La institución de salud debe contar con un expediente clínico, toda vez que, los pacientes de cualquier profesional de la salud o establecimiento médico, tienen derecho a contar con él para que la información relacionada con la atención médica que reciban sea asentada en un mismo lugar, de forma veraz, clara, precisa, legible y completa.

- El responsable debe saber que la titularidad de los datos personales contenidos en un expediente clínico es del paciente, no de los hospitales, médicos o profesionales de la salud. El paciente cuenta con ciertos derechos relacionados con esa información, como el derecho a solicitar una copia de su expediente, de un resumen clínico o de otras constancias que se encuentren en el expediente.

- Las organizaciones deben proteger la confidencialidad sobre cualquier dato personal o personal sensible relacionado con cualquier enfermedad, con la finalidad de evitar daño o discriminación de la persona afectada.

- El responsable sólo podrá compartir los datos personales de salud con terceros con la autorización expresa y por escrito del paciente y de un médico autorizado, salvo los casos en los que por disposición normativa o por cumplimiento de obligaciones se requiera comunicar la información.

- El responsable debe requerir la autorización expresa y por escrito del titular de los datos personales cuando se trate de una divulgación para fines vinculados con la literatura médica, docencia o investigación, en donde sea posible identificar al paciente.

- El responsable debe resguardar el expediente clínico con un nivel alto de medidas de seguridad administrativas, físicas y técnicas, considerando que contiene datos personales sensibles y que la información que contiene es fundamental para la conservación de la vida e integridad física del paciente.

- La identidad de las personas afectadas de alguna enfermedad (por ejemplo, Covid-19) no debe divulgarse, en caso de requerirse una transferencia de datos personales a las autoridades de salud, ésta deberá ser documentada claramente, fundamentada y realizarse considerando medidas de seguridad que garanticen la protección de los datos personales.

- Se debe proporcionar al paciente la información suficiente, clara, oportuna y veraz sobre diagnóstico, pronóstico y tratamiento del paciente, con el fin de favorecer el conocimiento pleno del estado de salud.

- El responsable debe corregir la información contenida en el expediente clínico cuando sea incorrecta siempre y cuando el titular brinde evidencia para realizarlo.

- Los responsables deben definir los plazos de conservación de los datos personales, que no deberán ser menor a un período de 5 años, a partir de la fecha del último acto médico.

- Los responsables deben definir los mecanismos que se emplearán para eliminar los datos personales de forma segura tomando en consideración la normatividad aplicable.

- El responsable debe eliminar de sus bases de datos la información contenida en el expediente clínico cuando el titular lo solicite, salvo que por alguna disposición normativa se deba conservar.

- Toda comunicación que se realice en la organización sobre la posible presencia de alguna enfermedad (ejemplo Covid-19) en el lugar de trabajo no debe identificar a ningún colaborador de forma individual.

  El responsable deberá adoptar todas las medidas de seguridad en la portabilidad de los datos personales de contenidas en los expedientes clínicos bajo su responsabilidad.

b) AUTORIDADES REGULADORAS

La autoridad reguladora en materia de expedientes clínicos es la SSa, quien ha establecido las normas para la integración y manejo de los datos de salud contenidos en los expedientes clínicos, garantizando la privacidad de los titulares.

Por su parte, los órganos garantes a nivel nacional y local, son las autoridades encargadas de garantizar el ejercicio del derecho a la protección de datos personales en posesión de sujetos obligados, les corresponde:

- Vigilar que se de el adecuado tratamiento;

- Vigilar y verificar el cumplimiento de las disposiciones contenidas en la Ley General;

- Coordinarse con las autoridades competentes para que las solicitudes para el ejercicio de los derechos ARCO y los recursos de revisión que se presenten en lengua indígena, sean atendidos en la misma lengua;

- Garantizar, en el ámbito de su respectiva competencia, condiciones de accesibilidad para que los titulares que pertenecen a grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales; y

- Conocer y resolver los recursos de revisión que interpongan los titulares, en términos de lo dispuesto en la Ley General y demás disposiciones que resulten aplicables en la materia; conocer y resolver los recursos de inconformidad que interpongan los titulares, en contra de las resoluciones emitidas por los organismos garantes, de conformidad con lo dispuesto en la Ley General y demás disposiciones que resulten aplicables en la materia; entre otros.

Finalmente, conforme a lo previsto en el artículo 89 fracción XII de la Ley General, el Instituto, a través de la Dirección General de Prevención y Autorregulación, ofrece apoyo técnico a los sujetos obligados o responsables, a efecto que puedan dar cabal cumplimiento a las obligaciones previstas en la Ley de la materia.

La Dirección General de Prevención y Autorregulación del INAI, se encuentra ubicada en Avenida Insurgentes Sur número 3211, segundo piso, Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán, Código Postal 04530, en la Ciudad de México. Con horario de atención de lunes a jueves, en un horario comprendido de las 9:00 a las 18:00 horas y los viernes, de 9:00 a 15:00 horas, en horario continuo, o bien, puede comunicarse al número telefónico gratuito 800 TEL INAI (800 835 4324) o al correo electrónico: atencion@inai.org.mx, o bien, en el número telefónico (55) 5004-2400.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales