GUÍA BÁSICA PARA EL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS EN EL SECTOR SANITARIO

INDICE

¿QUÉ ES LA PROTECCIÓN DE DATOS?

La Protección de Datos es un Derecho Fundamental que se desarrolla a partir del artículo 18.4 de la Constitución Española. Este derecho hace referencia al poder de disposición y control sobre los datos personales que faculta a las personas físicas para consentir el conocimiento y tratamiento de sus datos por terceros. De esta manera es **la persona física la única facultada para decidir lo que se puede hacer con sus datos de carácter personal**.

Trasladado al ámbito que nos ocupa, son los pacientes los que deciden qué es lo que el titular de la Clínica puede hacer con los datos que el propio paciente le da al acudir a la consulta. Así, se podría entender que existe un consentimiento tácito por parte del paciente cuando acude a un doctor para recibir asistencia sanitaria, sin embargo no se debe olvidar que esos datos, en numerosas ocasiones se utilizan para más finalidades, como la facturación, la gestión administrativa de la clínica, el envío de publicidad sobre la clínica, la comunicación a doctores colaboradores, etc...

La Ley Orgánica de Protección de Datos nace con el objeto de garantizar y proteger el tratamiento de los datos personales entre los que se incluyen los relativos a la salud de una persona física identificada o identificable. En este sentido, la Ley en su artículo 7 y 8 hace referencia a este tipo de datos a fin de garantizar la protección jurídica necesaria en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos.

Además de la legislación relativa a la protección de datos, debemos tener en cuenta la Ley 41/2002, de 14 de noviembre, básica[1] reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (en adelante Ley 41/2002), en la que se regula la historia clínica.

[1] La normativa referida, en la Comunidad Valenciana, se complementa con la Ley 1/2003, de 28 de enero, de Derechos e Información al Paciente de la Comunidad Valenciana.

¿QUÉ SE ENTIENDE POR DATO DE CARÁCTER PERSONAL?

La Ley Orgánica de Protección de Datos define dato de carácter personal como **cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que identifique o haga identificable a una persona física**.

Así, el nombre y los apellidos de un paciente son datos de carácter personal, al igual que su nº de D.N.I, su dirección de correo electrónico, sus antecedentes médicos, el tratamiento que se le realiza, sus facturas, etc,... porque todos estos datos aportan información sobre una persona física.

¿QUÉ SE ENTIENDE POR DATO DE SALUD?

Hasta que no entró en vigor el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, no existía en la legislación española una definición de dato de salud, por lo que se debía acudir a textos internacionales para delimitar este concepto.

El mencionado Reglamento define dato de carácter personal relacionado con la salud como aquellas **informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, de consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.**

Hay que destacar que no solo los datos de salud que indiquen una enfermedad o una anomalía son datos de carácter personal de salud, también lo serán aquéllos que indican un buen estado de salud.

¿QUÉ SE ENTIENDE POR FICHERO?

De acuerdo con la normativa un fichero es todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, independientemente de su forma o modalidad de creación, almacenamiento, organización y acceso.

Las historias clínicas de los pacientes constituyen un fichero del que disponen todas las consultas médicas, ya que, independientemente del soporte en el que se recojan, se almacenan de manera organizada. Otro fichero común de las clínicas es el fichero de los empleados y colaboradores, compuesto por los contratos, nóminas y otra documentación necesaria para la correcta gestión del personal que presta sus servicios en la clínica. Asimismo, pueden existir otros ficheros, por ejemplo de facturación o de agenda. Cada consulta deberá analizar los ficheros de los que dispone porque como más adelante se explicará, se deben notificar a la Agencia Española de Protección de Datos.

¿A QUIÉN AFECTA LA LEY DE PROTECCIÓN DE DATOS?

La Ley Orgánica de Protección de Datos afecta a toda organización, empresa o autónomo que tenga, utilice o trate datos de carácter personal ya sea en soporte informatizado o en soporte no automatizado.

Por lo tanto, dicha ley **afecta a todos los profesionales que operan en el sector sanitario que desarrollen su actividad de manera individual, a las Clínicas, Hospitales e Instituciones Sanitarias** que con la incorporación de historiales clínicos para el ejercicio de su profesión tienen en su poder datos relativos a la salud del paciente, datos médicos a los que les será de aplicación las medidas de nivel alto que recoge la normativa.

¿QUÉ NECESITO PARA QUE MI CONSULTA CUMPLA CON LA NORMATIVA DE PROTECCIÓN DE DATOS?

La Ley Orgánica de Protección de Datos establece una serie de principios en los que se basan las obligaciones que los responsables de los ficheros deben cumplir. **Con carácter general, será el responsable del fichero el titular de la clínica, ya sea una persona física o jurídica**.

Los responsables, para cumplir con la Ley, deben observar estos principios y cumplir las siguientes obligaciones.

- **PRINCIPIO DE CALIDAD DE LOS DATOS.**

  Sólo se podrán recoger datos de los pacientes cuando sean **adecuados, pertinentes y no excesivos en relación con la finalidad** para la que se hayan obtenido.

  La finalidad debe ser determinada y se debe informar de la misma al paciente. Por tanto, es necesario que se haga una pequeña reflexión sobre las utilidades que se quiere dar a la información de la que se dispone, ya que en ocasiones se utilizará también para el envío de publicidad sobre la Clínica y en este caso se tendrá que haber informado previamente al paciente.

  Se exige también que los datos estén actualizados y que cuando dejen de ser necesarios para la finalidad para la que fueron recabados se proceda a su cancelación. Sin embargo, en este punto se deberá atender a lo dispuesto en la Ley 41/2002 en lo referente al plazo de conservación, como se explicará en las siguientes páginas.

- **PRINCIPIO DE INFORMACIÓN Y CONSENTIMIENTO.**

  Se debe informar a los pacientes de la existencia de un fichero[2], de la finalidad para la que sus datos son recabados, de los destinatarios de la información, de la identidad y dirección del responsable del fichero y de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

  Asimismo, el titular tendrá que solicitar el **consentimiento** de los pacientes para poder tratar sus datos, salvo que nos encontremos en una de las excepciones que la Ley prevé ("*cuando el tratamiento de datos resulte necesario para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto*") . Cuando se recogen datos de salud, la Ley establece, con carácter general, que el consentimiento tendrá que ser expreso.

- **PRINCIPIO DE SEGURIDAD.**

  Se debe cumplir con las medidas de seguridad y disponer de un documento de seguridad.

  Las medidas de seguridad, de conformidad con el Reglamento que desarrolla la Ley Orgánica de Protección de Datos, se establecen en tres niveles en función del tipo de datos que se traten. **Cuando se tratan datos de salud se deben cumplir las medidas de seguridad de nivel alto, ya que se trata de datos especialmente protegidos.**

  Hay que señalar que las medidas de seguridad son de nivel acumulativo, es decir, si nos encontramos en el nivel alto, habrá que cumplir las establecidas para el nivel básico y las de nivel medio.

[2] Se adjunta un modelo de esta cláusula en el Anexo I.

En todos los casos es obligatorio tener un **documento de seguridad**. En este documento se recogen todas las medidas de seguridad que se deban cumplir y los protocolos que sigan en la Clínica para la implementación de las mismas. El documento de seguridad debe responder a la situación actual de la Clínica, ya que será el documento que deberá poner a disposición de la Agencia Española de Protección de Datos si así lo requiriera.

- **PRINCIPIO DE CONFIDENCIALIDAD.**

El titular de la Clínica y sus empleados o colaboradores que tengan acceso a los datos de carácter personal almacenados en las historias clínicas **están obligados al secreto profesional[3].**

El responsable de los ficheros se deberá encargar, mediante la firma de un documento de confidencialidad, de que todas las personas de su entorno que puedan tener acceso a los datos, se sometan a este deber de confidencialidad que debe mantenerse aun cuando la relación que vincule a las partes haya finalizado.

- **PRINCIPIO DE COMUNICACIÓN DE DATOS.**

Siempre que se prevea la comunicación de datos a un tercero, se deberá informar al interesado y solicitar su consentimiento, salvo que nos encontremos ante una de las excepciones que la Ley Orgánica de Protección de Datos dispone (por ejemplo, cuando la cesión de datos está autorizada en una ley o cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero).

Estaremos en este caso si el titular de la Clínica tiene acuerdos, por ejemplo, con sociedades médicas o con doctores colaboradores a los que

[3] Se adjunta un modelo de una cláusula de confidencialidad en el Anexo II

comunique datos de los pacientes (debe recordarse que la comunicación de un nombre ya supone la cesión de un dato de carácter personal).

Se debe tener en cuenta que la mencionada Ley **solo permite que se comuniquen datos para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario.**

Por otro lado, la normativa prevé dos tipos de cesiones, la comunicación de datos propiamente dicha y el acceso a datos por cuenta de terceros. En este ultimo caso, la relación entre las partes deberá quedar reflejada en un documento en el que se especifique, entre otras cosas, que el encargado de prestar el servicio sólo accederá a los datos de conformidad con las instrucciones que le de el responsable del tratamiento. Es el caso de las empresas que ofrecen un mantenimiento para el programa informático de gestión clínica o el supuesto de las gestorías que pueden tener acceso a datos de los empleados de la Clínica para el correcto desarrollo de los servicios que ellos prestan (p. ej. la elaboración de nóminas)

- **FACILITAR LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN.**

  Hay que **informar a los pacientes de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición**. En el caso de que un paciente ejerza, por ejemplo, su derecho de acceso a la historia clínica, el responsable deberá colaborar con ellos, siempre que la solicitud se realice de conformidad con el procedimiento establecido en la normativa, y facilitarle un informe o, en su caso, una copia de la misma, pues no se debe olvidar que los datos de carácter personal en ningún caso dejan de pertenecer a su titular por el hecho de haberlos comunicado a la Clínica o al profesional.

  El procedimiento para el ejercicio de estos derechos debe hacerse siempre conforme a Derecho, ya que existen unos plazos y unas pautas tanto para ejercerlos como para facilitarlos.

- **INSCRIPCIÓN DE LOS FICHEROS EN LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.**

  Siempre que se proceda a la creación de un fichero que contenga datos de carácter personal, deberá notificarse a la Agencia Española de Protección de Datos. Asimismo, cuando se produzca una modificación de la estructura del fichero o la cancelación del mismo, también deberá comunicarse a la Agencia.

  Esta notificación no significa que se deban registrar en la Agencia los datos de los pacientes que tengan incorporados en sus ficheros, sino que la notificación se refiere a la comunicación de la titularidad del fichero, la organización y la estructura del mismo.

¿QUÉ SANCIONES IMPONE LA AGENCIA ESPAÑOLA DE PROTECCIÓN SI INCUMPLO LA LEY DE PROTECCIÓN DE DATOS?

La Ley establece que las infracciones pueden ser leves, graves o muy graves. A modo de ejemplo, establecemos alguna de las infracciones previstas en la normativa.

Leves:

- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.
- Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información necesaria.
- Incumplir el deber de secreto.

Graves:

- Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
- Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.
- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen[4].

Muy graves:

- La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
- No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición
- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

[4] Recientemente la Agencia Española de Protección de Datos ha sancionado a un hospital por la aparición de más de 2.000 documentos con información confidencial de pacientes del centro sanitario, estimando que las medidas de seguridad de nivel alto no fueron totalmente adoptadas o en su caso, su aplicación fue incorrecta.

Las sanciones se impondrán en función del tipo de infracción cometido.

INFRACCIONES	SANCIONES
Leves	601,01 a 60.101,21 €
Graves	60.101,21 a 300.506,05 €
Muy Graves	300.506,05 a 601.012,10 €

¿LOS DATOS DE MIS EMPLEADOS TAMBIÉN SE CONSIDERAN DATOS DE CARÁCTER PERSONAL?

Efectivamente**, los datos de sus empleados son datos de carácter personal**. Cuando una clínica o un profesional autónomo tiene personal contratado, ya sea mediante una relación laboral o mercantil, tendrá archivada documentación que contenga este tipo de datos: copias de los contratos, nóminas, facturas, partes médicos de altas y bajas, etc...

Todos estos documentos contienen datos de carácter personal como el nombre, apellidos, número de la Seguridad Social, categoría profesional, número de colegiado, salario... por lo que **se trata de un fichero que debe cumplir con todas las obligaciones que se disponen en la Ley Orgánica de Protección de Datos**.

Es decir, se tiene que inscribir un fichero en el Registro de la Agencia Española de Protección de Datos que prevea como finalidad la gestión del personal que preste sus servicios en la Clínica: se tendrá que informar a los empleados del tratamiento que se va a efectuar de sus datos, habrá que analizar las relaciones con terceros a los que se les comuniquen sus datos. La documentación de los trabajadores que contenga datos de carácter personal se deberá almacenar y custodiar con las medidas de seguridad establecidas en el Reglamento que desarrolla la Ley Orgánica de Protección de Datos, que tendrán que quedar reflejadas en el documento de seguridad de la clínica, y al igual que en el caso del fichero de las historias clínicas de los pacientes, se les deberá permitir ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

¿CÓMO DEBO ACTUAR SI UN PACIENTE ME PIDE COPIA DE SU HISTORIA CLÍNICA?

Los pacientes, como titulares de sus datos de carácter personal, pueden solicitar y obtener información de sus datos sometidos a tratamiento, del origen de los mismos o conocer si éstos se han cedido. Este derecho se conoce como derecho de acceso.

El derecho de acceso a la historia clínica está regulado en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica porque presenta algunas especificidades en relación con la normativa en materia de protección de datos.

Se establece en esta Ley que **el paciente tiene derecho de acceso a la documentación de la historia clínica y a obtener copia de los datos que figuren en ella**, con dos limitaciones: la referida a las anotaciones subjetivas y cuando el ejercicio de este derecho pueda perjudicar el derecho de terceros a la confidencialidad.

Sin embargo, no debe entenderse que el derecho de acceso supone la entrega de la historia clínica al paciente, sino un informe o, en su caso, copia de la misma, ya que **el profesional o el centro, en su caso, tiene la obligación del deber de custodia de las historias clínicas durante, al menos, cinco años desde el alta del proceso asistencial de cada paciente**. Por tanto, siempre se le debe entregar copia de la historia clínica, por el medio que el paciente haya especificado, si fuera posible.

CUANDO UN PACIENTE DEJA DE VENIR A LA CONSULTA, ¿PUEDO ELIMINAR SU HISTORIA CLÍNICA?

La Ley Orgánica de Protección de Datos establece que los datos se deben cancelar una vez que dejen de ser pertinentes para la finalidad para la que se recogieron. Por tanto, cuando un paciente recibe el alta médica o cuando deja de acudir a la clínica durante un periodo suficientemente largo, sus datos ya no son necesarios para la finalidad para la que se almacenaron, que no es otra que la prestación de la asistencia sanitaria, y por tanto se debería proceder a la cancelación de tales datos.

Sin embargo, la Ley 41/2002 establece que la historia clínica se debe conservar al menos cinco años[5] desde el alta de cada proceso asistencial. Por tanto, **cuando un paciente recibe el alta o deja de asistir a la clínica no se puede proceder a eliminar sus datos ya que existe una obligación de custodia de la historia clínica.**

En este caso concreto, la cancelación de los datos no debe entenderse como eliminación de los mismos, sino como bloqueo de esos datos en caso de estar informatizados o en el supuesto de estar almacenados en soporte papel, se debe proceder a almacenarlos en un lugar diferenciado, con la finalidad exclusiva de su custodia.

[5] Sin perjuicio de la Ley 1/2003, de 28 de enero, de Derechos e Información al Paciente de la Comunidad Valenciana.

¿CUÁNTO TIEMPO DEBO CONSERVAR LAS HISTORIAS CLÍNICAS DE MIS PACIENTES?

Como ya se ha mencionado, de acuerdo con la Ley 41/2002 la historia clínica de un paciente se debe conservar, como mínimo, cinco años contados desde la fecha de alta de cada proceso asistencial, lo que no debe confundir al profesional y llevarle al pensamiento de que una vez finalizado este plazo ya no existe motivo para la conservación de las historias clínicas de sus pacientes.

En este punto, debemos plantearnos **cuánto tiempo ha de pasar para que un paciente nos pueda exigir responsabilidad civil derivada de una prestación médica, es decir, el plazo por el que un paciente puede reclamar a un profesional por una intervención médica.**

El Código Civil establece que se tiene un plazo de quince años para poder plantear una acción por responsabilidad civil. No obstante, se debe tener en cuenta que este plazo computa desde que el reclamante tiene conocimiento del daño, por lo que a efectos prácticos se puede considerar que este plazo es de treinta años ya que si el daño se conoce justo antes de que venzan los quince años automáticamente se prorrogará por otros quince años.

En consecuencia con todo lo anteriormente expuesto, cabe entender que la cancelación a la que obliga la LOPD no supone, automáticamente, un borrado o supresión física de los datos (fin último de la misma), sino que puede conllevar, en caso de que así lo establezca una norma con rango de Ley o se desprenda de la propia relación jurídica que vincula al responsable del fichero con el afectado (y que motiva el propio tratamiento), el bloqueo de los datos.

También es importante mencionar que la Ley 41/2002, se refiere a la **forma de conservación de las historias clínicas** y reconoce la posibilidad de mantenerla en un soporte distinto al original, poniendo de manifiesto la necesidad de implementar las medidas de seguridad exigibles para los ficheros de datos de carácter personal, remitiéndose a la regulación de protección de datos.

¿PUEDO UTILIZAR LOS DATOS DE MIS PACIENTES PARA PUBLICAR ESTUDIOS O DAR CONFERENCIAS?

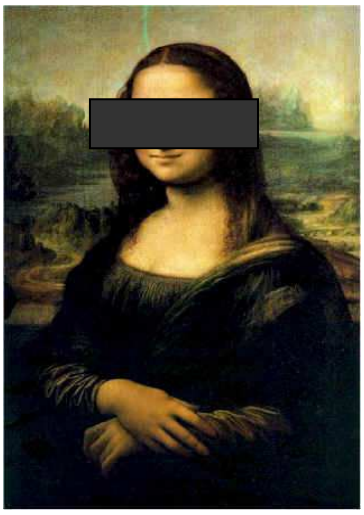
Como regla general, **para poder utilizar los datos de sus pacientes para finalidades distintas a la asistencia médica, se debe contar con el consentimiento expreso del paciente**. Es decir, se debe informar al paciente de que sus datos se van a utilizar para actividades de investigación, docentes o científicas y éste deberá consentir. Para tener prueba de este consentimiento se deberá solicitar por escrito.

Otra opción, y es la que prevé la Ley 41/2002 cuando los datos se quieran emplear para estas finalidades, consiste en **almacenar los datos identificativos del paciente separados de aquéllos de carácter clínico-asistencial, de manera que se garantiza el anonimato de los pacientes.** Así, se tendría una base de datos de historias clínicas que se podrían manejar para fines científicos y que no permitirían identificar al paciente al que pertenecen.

Cuando en los estudios científicos se utilicen imágenes de los pacientes, recomendamos que se obtenga el autorización expresa del paciente. En primer lugar, se debe tener en cuenta que **la imagen es un dato de carácter personal en tanto que permite identificar a una persona física**. Por imagen nos referimos no solo a fotografías sino también a grabaciones, por ejemplo de intervenciones, en las que el paciente pueda resultar identificado.

La fórmula clásica de tapar o deformar la cara para evitar que se identifique al paciente a veces no es suficiente ya que puede tener signos distintivos en otras partes del cuerpo que permitan su identificación. Y por último, hay ocasiones en las que aunque se tape o se deforme la cara del paciente, se aportan datos suficientes como para que mediante la conexión de los mismos el paciente podría ser identificable (sexo, edad, iniciales, especialidad a la que acude el paciente, centro médico).

Por tanto, debe solicitarse al paciente su autorización, explicándole la finalidad y el destino que vayan a tener los datos (incluyendo las imágenes y grabaciones).[6]



En ocasiones, aunque se cubra parte del rostro, es fácil identificar a la persona física cuya intimidad pretendemos preservar.

- Deberá facilitarse el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la normativa.
- Deberán cumplirse las medidas de seguridad previstas al efecto y tratar los datos con la debida diligencia y confidencialidad.

[6] Se adjunta un modelo de cláusula informativa solicitando la autorización del paciente en el Anexo III.

OBLIGACIONES BÁSICAS QUE DEBEN CUMPLIR LOS PROFESIONALES SANITARIOS

- Inscribir los ficheros en la Agencia Española de Protección de Datos.

- Informar a los pacientes de la finalidad a la que van a destinar los datos, de la identidad del responsable del fichero, de los cesionarios en caso de haberlos y de la dirección a la que se deben dirigir para ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

- Solicitar el consentimiento de los pacientes en el caso de que sus datos se vayan a utilizar para finalidades distintas a la prestación de asistencia sanitaria.

- Implementar las medidas de seguridad de nivel alto que establece el Reglamento de desarrollo de la LOPD, y disponer de un documento de seguridad.

- Formar y concienciar al personal que trabaje en la consulta, para que conozcan la normativa de protección de datos y la respeten cuando tengan acceso a los datos de carácter personal de los pacientes.

- En caso de que se comuniquen datos a terceros, analizar el supuesto en el que se produce la cesión y, cuando sea necesario, firmar los acuerdos que la normativa establece.