GRUPO PSN

Colegio Oficial de
Dietistas - Nutricionistas
de Navarra
CODINNA

Cumplimiento normativo en materia de protección de datos y seguridad de la información para profesionales del ámbito sanitario

Lorea Roncal y Ana Sánchez
Consultoras de Protección de Datos

ANTECEDENTES

*La **Ley Orgánica de Protección de Datos de Carácter Personal** (LOPD), permanece **vigente desde el 15 de enero de 2000**, derogando la anterior Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD). El ámbito de la LOPD abarca **cualquier tipo de soporte**, es decir, ficheros en formato automatizado como en papel.*

*Desde el 24 de mayo de 2016 se encuentra vigente el **Reglamento (UE)** 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*

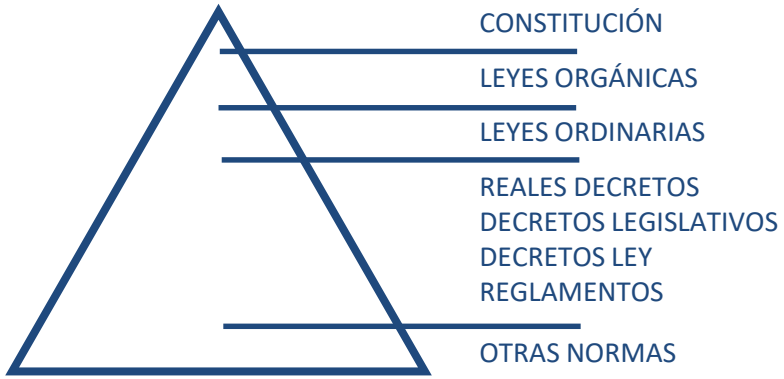
***El nuevo Reglamento General de Protección de Datos** (RGPD) entró en vigor en mayo de 2016 y **será aplicable a partir de mayo de 2018**. Es una norma directamente aplicable, que no requiere de normas internas de trasposición ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación.*

*Por ello, **los responsables de ficheros deben ante todo asumir que la norma de referencia es el RGPD y no las normas nacionales**. No obstante, la ley que sustituirá a la actual Ley Orgánica de Protección de Datos (LOPD) sí podrá incluir algunas precisiones o desarrollos en materias en las que el RGPD lo permite.*

NATURALEZA

*La **LOPD**, es una Ley Orgánica, que tiene por objeto garantizar y proteger, en lo que se refiere al tratamiento de los datos de carácter personal, las **libertades públicas y los derechos fundamentales de las personas físicas**, y especialmente de su **honor, intimidad y privacidad personal y familiar**.*

*Su objetivo principal es regular el **tratamiento de los datos de carácter personal, independientemente del soporte en el cual sean tratados o del tipo de tratamiento que se les aplique**, **los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan**.*



GRUPO PSN

LEGISLACIÓN APLICABLE

*La legislación vigente reconoce, protege y garantiza el derecho de los ciudadanos al **honor** y a la **intimidad** en lo referente a sus datos personales como un derecho fundamental propio.*

- ***Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la LOPD***
- ***Ley 9/2014, de 9 de mayo, General de Telecomunicaciones..***
- ***Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.***
- ***Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.***
- ***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.***

· REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

GRUPO PSN

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)

Organismo público que vigila el cumplimiento de la legislación sobre protección de datos.

Su sede está en Madrid y tiene su ámbito de actuación en toda España; aunque existen otras ***agencias de protección de datos de carácter autonómico*** *en Cataluña y en el País Vasco.*

OTRAS FUNCIONES DE LA AGENCIA

Ejercer la ***potestad sancionadora, tutela de derechos****, emitir las autorizaciones previstas (transferencias de datos internacionales), ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos. Atender a sus* ***peticiones y reclamaciones de los afectados****, promover* ***campañas de difusión sobre la ley*** *a través de los medios, dictar* ***instrucciones y recomendaciones*** *de adecuación de los tratamientos a la legislación vigente.*

www.agpd.es

GRUPO PSN

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ÁMBITO DE LA LEY	***Protección de los datos de carácter personal registrados en soporte informático, papel o video*** *que los haga susceptibles de tratamiento y uso posterior por los sectores público y privado.*
FICHERO DE DATOS	*Todo* ***conjunto organizado de datos de carácter personal****, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.*
RESPONSABLE DEL FICHERO	***Persona física o jurídica****, de naturaleza pública o privada, u órgano administrativo, que* ***decida sobre la finalidad, contenido y uso del tratamiento de los datos****.*
RESPONSABLE DE SEGURIDAD	*Persona o personas a las que el Responsable del Fichero ha asignado formalmente la función de* ***coordinar y controlar las medidas de seguridad aplicables****.*
ENCARGADO DE TRATAMIENTO	*La persona física o jurídica que, sólo o conjuntamente con otros, trate datos personales* ***por cuenta del Responsable del Fichero****, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo* ***para la prestación de un servicio****.*

NIVELES DE SEGURIDAD

*La Ley Orgánica establece **diferentes niveles de seguridad** sobre los datos personales que deben ser protegidos:*

NIVEL BÁSICO

Identificativos, dirección, teléfono de contacto, etc.

NIVEL MEDIO

Económicos, financieros y patrimoniales.
Comisión infracciones administrativas y penales.
Hacienda Pública.

***NIVEL ALTO** (máxima protección)*

Salud.
Vida sexual.
Origen racial.
Religión y creencias.
Ideología, afiliación política y sindical.

GRUPO PSN

OBLIGACIONES BÁSICAS PARA EL NIVEL ALTO

Inscripción de los Ficheros *en el Registro de la Agencia Española de Protección de Datos, así como su actualización, modificación o supresión de los mismos cuando proceda.*

Elaboración, mantenimiento y cumplimiento de un ***Plan de Seguridad****.*

OBLIGACIONES PERIÓDICAS PARA EL NIVEL ALTO

Auditoría *cada dos años (ordinaria) o siempre que haya habido un cambio sustancial en el tratamiento de los datos (extraordinaria).*

Seguimiento del ***Plan de Seguridad*** *y adopción de las medidas correctoras necesarias.*

Notificación *a la Agencia Española de Protección de Datos de cualquier modificación en los Ficheros.*

AVISO LEGAL

*Información sobre los **Ficheros de datos de carácter personal** a los que van a ser incorporados los datos del interesado.*

***Finalidad** de los ficheros.*

***Receptores y destinatarios** de la información.*

***Procedimiento para el ejercicio de derechos** por el interesado y ante quien los puede ejercitar.*

*Identidad y datos de contacto del **Responsable del Fichero**.*

GRUPO PSN

RECOGIDA DE LOS DATOS

NO *pueden ser recabados sin el consentimiento del titular de los mismos.*

NO *pueden ser destinados a usos distintos de aquel para el que fueron recabados.*

NO *se pueden ceder o comunicar datos a terceros sin el consentimiento del titular.*

Deben ser ***adecuados, pertinentes y no excesivos****.*

GRUPO PSN

CONSENTIMIENTO TRATAMIENTO DE LOS DATOS

El tratamiento de los datos requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

TIPOS DE CONSENTIMIENTO

CONSENTIMIENTO TÁCITO

Esta será la forma normal de consentimiento para los supuestos que no se exija un consentimiento expreso.

CONSENTIMIENTO EXPRESO

Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

CONSENTIMIENTO EXPRESO Y POR ESCRITO

Se requiere consentimiento expreso y por escrito del afectado respecto a los datos relativos a la ideología, afiliación sindical, religión y creencias y sólo podrán ser cedidos con consentimiento expreso del afectado.

HISTORIA CLÍNICA

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.

Documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.

Dicha información sanitaria tiene la finalidad de facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud.

ACCESO A LA HISTORIA CLÍNICA

*El acceso a los datos de salud, deberá realizarse atendiendo al **principio de proporcionalidad**, debiendo limitarse los datos necesarios, no pudiendo extenderse a otros no vinculados a la finalidad por la que se accede a los mismos.*

Principios generales aplicables

La dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica" y que "la persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida".

Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

GRUPO PSN

El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la ***Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal****.*

El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, ***separados de los de carácter clínico asistencial*** *(disociados), de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Ej: Inspecciones de Hacienda.*

Se ***exceptúan*** *los supuestos de* ***investigación de la autoridad judicial*** *en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente.*

TITULARIDAD HISTORIA CLÍNICA

Titularidad intelectual *del facultativo, en tanto existe una creación intelectual y científica, donde influyen factores determinantes como la formación académica o la propia experiencia profesional.*

*En este sentido el artículo 17.5 de la Ley 41/2002, dispone que "****los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen****".*

Titularidad material *de la historia clínica, se le atribuye al paciente, al ser sus datos los que se recogen en la historia clínica.*

GRUPO PSN

ANOTACIONES SUBJETIVAS

Entendidas como hipótesis e impresiones personales de los profesionales sanitarios, basadas en sus percepciones, comentarios realizados por terceras personas, que carecen de trascendencia para el conocimiento veraz y actualizado del estado de salud del paciente, sin que puedan tener la consideración de un diagnóstico.

La redacción de dichas anotaciones conlleva una posible problemática relacionada con el derecho al acceso del paciente a su historia clínica.

Como norma general, el paciente tiene derecho al acceso a la historia clínica y a obtener copia de los datos que figuran en ella, no pudiéndose ejercitarse en perjuicio del derecho de terceras personas, ni en perjuicio del derecho de los profesionales participantes en su elaboración, lo cuales pueden oponer al derecho de acceso, la reserva de sus anotaciones subjetivas.

*La Agencia Española de Protección de Datos, en su Resolución 633/2004, afirma que "**la posible denegación del acceso a las anotaciones subjetivas la tiene que realizar el facultativo, no la entidad que la custodia**".*

GRUPO PSN

CONSERVACIÓN HISTORIA CLÍNICA

El artículo 17 de la Ley 41/2002, establece que los centros sanitarios tienen la obligación de ***conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad****, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y,* ***como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial****.*

GRUPO PSN

CONSERVACIÓN HISTORIA CLÍNICA JUBILACIÓN O CESE DE NEGOCIO

Informe jurídico 496/2007 de la Agencia Española de Protección de Datos *indica que "en caso de cesación en el ejercicio de la profesión, subsistirá un deber de conservación que se extenderá a los plazos legalmente previstos, subsistiendo igualmente ese deber, en beneficio de la atención sanitaria del paciente, en caso de fallecimiento de facultativo, subrogándose los herederos en las obligaciones de conservación por aplicación de lo dispuesto en el artículo 661 del Código Civil".*

GRUPO PSN

Informe de 12 de noviembre de 2007 de la Agencia Española de Protección de Datos

Dentro de las obligaciones de gestión y custodia se encuentran las relacionadas con la conservación de la historia clínica, previstas en el propio precepto, cuyo apartado 1 establece que "Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, ***cinco años contados desde la fecha del alta de cada proceso asistencial****", prosiguiendo que "a la vista de las normas citadas, resulta claramente que,* ***con independencia de que se haya producido la cesación en el ejercicio de la actividad profesional, el facultativo se encuentra aún sometido a las exigencias legales de conservación de las historias clínicas****, correspondiéndole su custodia y conservación en tanto no hayan transcurrido los plazos legalmente previstos para que dicha conservación siga teniendo lugar y siendo, por imperativo de la propia Ley 41/2002, responsable del fichero de historias clínicas."*

GRUPO PSN

CONSERVACIÓN HISTORIA CLÍNICA DE PACIENTES FALLECIDOS

El artículo 18.4 de la Ley 41/2002, dispone que "los centros sanitarios y los facultativos de ejercicio individual ***sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él****, por razones familiares o de hecho,* ***salvo que el fallecido lo hubiese prohibido expresamente y así se acredite****", "en cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros".*

GRUPO PSN

SECRETO PROFESIONAL

*La revelación del secreto profesional la encontramos tipificada en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, que en su artículo 199 recoge que "**el que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años**".*

GRUPO PSN

TRATAMIENTO DATOS DE MENORES DE EDAD

Artículo 13 del Real Decreto 1720/2007

Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos ***deberá expresarse en un lenguaje que sea fácilmente comprensible por aquellos****, con expresa indicación de lo dispuesto en este artículo.*

Podrá procederse al tratamiento de los datos de los ***mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela****. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.*

En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos.

No obstante, ***podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista*** *en el apartado anterior.*

GRUPO PSN

DERECHOS A.R.C.O

La LOPD garantiza a las personas el poder de control sobre la información y datos que de ellos tienen las organizaciones, así como del uso de esta información por las mismas.

*Para ello, los **derechos de acceso, rectificación, cancelación y oposición** a la información que se posee de personas físicas, exigiendo que se facilite al ciudadano el ejercicio de estos derechos.*

*Son derechos de **carácter personalísimo**, sólo pueden ser ejercidos por los interesados o representante legal.*

*Son derechos cuyo **ejercicio es gratuito**, han de solicitarse **por escrito acompañado de copia del DNI ante el Responsable del Fichero** por cualquier medio que permita acreditar tanto el envío como su recepción.*

*El **Responsable del Fichero debe contestar** tanto si procede o no atender a la solicitud.*

*El interesado podrá recabar la **tutela ante la Agencia Española de Protección de Datos**.*

DERECHO ACCESO	*El interesado tiene derecho a obtener y solicitar información sobre sus datos personales, el origen de los mismos, así como las cesiones realizadas o que el responsable del fichero prevé realizar.*
DERECHO RECTIFICACIÓN	*Podrá solicitar la rectificación de los datos personales que sean inexactos o incompletos, inadecuados o excesivos.*
DERECHO CANCELACIÓN	*Equivale al bloqueo de los datos por parte del responsable del fichero, conservándolos, únicamente, cuando exista obligación legal o, para mantenerlos a disposición de las Administraciones Públicas, Jueces y Tribunales, con el fin de atender las posibles responsabilidades, durante el plazo de prescripción de éstas. Finalizado el mismo los datos deberán ser suprimidos por el Responsable del Fichero.*
DERECHO OPOSICIÓN	*El afectado podrá oponerse a que se traten sus datos con fines de publicidad y prospección comercial, entre otros.*

INFRACCIONES

LEVES

•No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.
•No solicitar la inscripción del fichero en el Registro General de Protección de Datos
•Recopilar datos personales sin informar previamente
•No atender a las solicitudes de rectificación o cancelación
•Transmitir datos a un encargado de tratamiento sin cumplir las obligaciones formales.

GRAVES

•No inscribir los ficheros en la AEPD.
•Utilizar los ficheros con finalidad distinta con la se crearon.
•No tener el consentimiento del interesado para recabar sus datos personales.
•No permitir el acceso a los ficheros.
•Mantener datos inexactos o no efectuar las modificaciones solicitadas.
•No seguir los principios y garantías de la LOPD.
•Tratar datos especialmente protegidos sin la autorización del afectado
•No remitir a la AEPD las notificaciones previstas en la LOPD.
•Mantener los ficheros sin las debidas condiciones de seguridad.

MUY GRAVES

- *Crear ficheros para almacenar datos especialmente protegidos.*
- *Recogida de datos con engañoso o fraudulentamente.*
- *Recabar datos especialmente protegidos sin la autorización del afectado.*
- *No atender u obstaculizar de forma sistemática las solicitudes de cancelación o rectificación.*
- *Vulnerar el secreto sobre datos especialmente protegidos.*
- *La comunicación o cesión de datos cuando ésta no esté permitida.*
- *No cesar en el uso ilegítimo a petición de la AEPD.*
- *Tratar los datos de forma ilegítima o con menosprecio de principios y garantías que le sean de aplicación.*
- *No atender de forma sistemática los requerimientos de la AEPD.*
- *La transferencia temporal o definitiva de datos de carácter. personal con destino a países sin nivel de protección equiparable o sin autorización.*

La Agencia de Protección de Datos **multa a una web con una sanción de 5.000 euros** por usar 'cookies' sin el consentimiento de los usarios

30/03/2017
http://cultura.elpais.com/cultura/2017/03/30/actualidad/1490869071_674267.html

Sanción de 10.000 euros a empresa por infracción del artículo 21 de LSSI
En concreto por enviar correos electrónicos comerciales sin autorización. Sanciones AEPD 2016

Sanción de 60.000 euros a tres empresas por una infracción del artículo 6 de la LOPD: Consentimiento del afectado
Sanciones AEPD 2016

Multa de 300.000 euros por tirar a la basura datos clínicos
27/08/2010
http://www.lavanguardia.com/vida/20100827/53990509626/multa-de-300-000-euros-por-tirar-a-la-basura-datos-clinicos.html

GRUPO PSN

Blog PSN Sercon

www.psnsercon.com/blog/

GRUPO PSN

MUCHAS GRACIAS
POR SU ATENCIÓN


@GRUPOPSN


GRUPO PSN


GRUPO PSN


GRUPO PSN


HTTP://BLOG.PSN.ES

www.psnsercon.com/blog/

GRUPO PSN

Ad Qualitatem
Calidad Sanitaria
Protección de Datos

SERCON
PSN SERVICIOS Y CONSULTORÍA
GRUPO PSN