Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril del 2016, relativo a la protección de datos personales

Estimados/as Colegiados/as:

En primer lugar, transmitiros tranquilidad sobre el nuevo Reglamento de Protección de Datos.
Su aplicación comienza mañana 25 de mayo, pero la Agencia Española de Protección de Datos es consciente de lo compleja que es la adaptación de la Ley a este nuevo Reglamento.

Como ya sabéis, el Colegio ha celebrado elecciones a Junta de Gobierno el pasado 20 de mayo, por lo que estamos en un momento de transición, pero seguimos trabajando para dar respuesta a todas vuestras cuestiones, especialmente a las relacionas con este asunto; que son las que entendemos que más os preocupan.

A continuación, vamos a tratar de aclarar las posibles dudas que tengáis y a facilitaros información de la propia Angencia Española de Protección de Datos, la Unión Interprofesional y nuestro Consejo General de Colegios Oficiales de Podólogos:

Varios compañeros nos han trasladado consultas sobre **si los *centros sanitarios unipersonales tienen la obligatoriedad de designar un DPD*** *teniendo en cuenta que 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, define "Centro sanitario" como el conjunto organizado de profesionales, instalaciones y medios técnicos que realiza actividades y presta servicios para cuidar la salud de los pacientes y usuarios*; por ello, les remitimos a continuación la respuesta ofrecida a las mismas por el departamento de protección de datos de Unión Profesional (UP), en virtud de la colaboración existente en esta materia entre UP, la Agencia Española de Protección de Datos, y la Unión Interprofesional, de la que este Colegio es socio:

El RGPD establece la obligatoriedad de nombrar un DPD bajo determinadas circunstancias (art. 37.1):

- Cuando el tratamiento se lleve a cabo por una **autoridad u organismo público**, excepto por los tribunales en el ejercicio de sus funciones.

- Cuando las **actividades principales** del responsable o encargado de tratamiento, son claves para lograr sus objetivos, consistan en operaciones de **tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.** El concepto a gran escala, es ambiguo, pero el articulo 91 lo define como "operaciones de tratamiento que tengan por objeto procesar una cantidad considerable de datos personales", es decir, un gran número de interesados y que sean susceptibles de generar un riesgo elevado. El Grupo de Trabajo del articulo 29 añade tener en cuenta el número de interesados, el volumen o tipo de datos, la duración del tratamiento y el alcance geográfico.
- Cuando las actividades principales del responsable o del encargado consistan en el **tratamiento a gran escala de categorías especiales de datos,** el art. 9 datos personas que revelen origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas o la pertenencia a sindicatos, tratamiento de datos genéticos, datos biométricos para la identificación exclusiva de personas físicas, **datos relativos a la salud** y datos relativos a condenas e infracciones penales.
- **En este sentido no se considera tratamiento a gran escala el llevado a cabo por un solo médico (considerando el artículo 91). Por lo tanto, no sería obligatorio la figura del DPD.**

Las personas que trabajen en el centro habrán de firmar sea un centro unipersonal o multipersonal un documento de confidencialidad respecto a la protección de datos de sus pacientes, a raíz del Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril del 2016, relativo a la protección de datos personales y a libre circulación de estos datos aplicable el 25 de mayo del 2018.

En las páginas siguientes os facilitamos el informe realizado por nuestro Consejo General sobre la Protección de Datos en el ÁMBITO SANITARIO

C/ SAN BERNARDO, 74 - BAJO - IZQ. - TELEF. 91 532 69 [illegible] COLEGIO PROFESIONAL DE PODÓLOGOS DE LA COMUNIDAD MADRID C/ SAN BERNARDO, 74 - 28015 MADRID

Madrid, 24 de mayo de 2018

Consejo General
de Colegios
Oficiales
de Podólogos
de España

Protección de datos en el ámbito sanitario

Como ya todos vosotros sabréis, el próximo día 25 de mayo de 2018 entra en vigor el nuevo Reglamento de Protección de Datos Personales dictado por la Comisión Europea en 2016 y que es de aplicación en todos los países de la Unión.

La protección de Datos personales es un derecho fundamental recogido en el artículo 18.4 de la Constitución Española y regulado por el Reglamento Europeo de Protección de Datos (RGPD), la LOPD y su reglamento de desarrollo.

Desde la Agencia Española de Protección de Datos (AEPD) se han elaborado varias guías enfocadas, sobre todo, a la aplicación del RGPD en PYMES. Estos materiales incluyen la Guía de Análisis de Riesgo y la Guía de Evaluación de Impacto en la Protección de Datos, presentadas recientemente.

El RGPD da la categoría de datos **Especialmente Protegidos** a los datos relativos a la salud, lo cual hace que se deban cumplir una serie de condiciones adicionales para su tratamiento conforme a la normativa.

Estas son las novedades que afectan a los pacientes y a los profesionales que operan en el sector sanitario, a las clínicas, a los hospitales, a los centros médicos y a las instituciones sanitarias (responsables y encargados de tratamiento).

1. Derechos de los pacientes:

- Clausula

Será necesario incluir la base legal sobre la que se fundamenta cada vez que que pidamos los datos al paciente. Esto puede añadirse al documento que se debe entregar al paciente solicitando su autorización para ser incluido en el archivo de protección de datos de la clínica. Las clausulas de protección de datos deben ser "*concisas, trasparente, inteligible, fácil acceso y lenguaje claro y sencillo*" evitando textos confusos.

Por tanto, habría que incluir la ley sobre la que se fundamenta: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

- Consentimiento

Según la nueva normativa europea, este deberá ser:

- Explícito
- Recogido por escrito

- Calidad de los datos

Se recogerá los datos de los pacientes siempre que sean adecuados, veraces y pertinentes. La recogida y el tratamiento de datos de salud **garantizar una asistencia adecuada al paciente** por lo que la información trascendental para la asistencia sanitaria ha de contar, como mínimo, con los siguientes datos (si procede):

- Documentación referida a la hoja clínico-estadística
- Autorización de ingreso
- Informe de urgencia
- Exploración física
- Evolución
- Órdenes médicas
- Hoja de interconsulta
- Informes de exploración complementaria
- Consentimiento informado
- Informe de anestesia
- Informe de quirófano o de registro del parto
- Dosier de anatomía patológica
- Evolución y planificación de cuidados de enfermería
- Aplicación terapéutica de enfermería

- Información

Los pacientes deben ser informados en todo momento de:

- Existencia de estos ficheros
- Finalidad del mismo
- Posibles destinatarios de la información
- Identidad y dirección del responsable del mantenimiento del mismo
- Posibilidad del ejercicio de sus derechos

Es **obligatorio** en cada centro sanitario la existencia de una **hoja de información al paciente** en la que le solicita su autorización **para el tratamiento de sus datos**.

En ella se recoge, entre otros datos:

- Nombre del profesional y del centro donde ha sido atendido el paciente
- Propósitos de la petición

- Expresa conformidad de publicación del caso clínico en publicaciones científicas dirigidas a profesionales de la salud
- Nombre del paciente
- Documento de identidad o pasaporte y su firma autorizando expresamente que se utilicen los datos de su historia clínica en las condiciones que se describen en el informe.

- Comunicación de los datos

Es habitual, que los datos se **comuniquen** entre entidades para el mejor tratamiento del paciente. En estos casos, el interesado deberá tener constancia de ello, ya que será él quien permita esta transmisión.

El responsable del fichero deberá cumplir determinados requisitos:

- Definir en un contrato escrito la **regulación del tratamiento de datos por cuenta de un tercero**,
- Establecer que ese tercero (únicamente tratará los datos conforme a sus instrucciones.
- Comprobar que los datos no serán utilizados con fines distintos a los determinados en el contrato, ni serán comunicados a otras personas.
- El tercero deberá cumplir con las mismas medidas de seguridad que las que cumpla el responsable del fichero.

La única excepción a este consentimiento se establece en el caso de que la comunicación de los datos tenga por objeto la prevención, el diagnóstico y la asistencia sanitaria de los afectados a los que se refieren.

En el caso particular y excepcional de las mutuas y de las compañías de seguros, los datos médicos pueden comunicarse de acuerdo al principio de calidad y únicamente para llevar a cabo la elaboración de la factura del gasto sanitario.

- Facilitar los derechos ARCO

Los pacientes podrán ejercitar libremente su **derecho de acceso, rectificación, cancelación y oposición de su historia clínica**.

Derecho al acceso: se incluye un cambio importante, ya que habrá que facilitar al paciente la **copia de los datos personales** si así lo solicita. Además, este derecho es gratuito, y el plazo de entrega al paciente es de 1 mes (2 en caso especialmente complejo). Si hay mucha información se puede pedir qué datos concretos necesita. El Reglamento también expone que se debe facilitar la entrega telemática de los datos a los pacientes.

Nuevo derecho al olvido: Viene derivado del derecho al borrado de los datos. La problemática de este derecho en los asuntos de salud es su incoherencia con respecto a la legislación, que obliga a custodiar dichos datos sanitarios por si el paciente quiere reclamarlos (Ley de autonomía del paciente). Por tanto, la Agencia deberá aclarar el alcance del mismo.

- Notificación del mantenimiento de los ficheros a la AEPD

Siempre que se proceda a la creación, modificación o cancelación de un fichero que contenga datos personales, se deberá **notificar a la Agencia Española de Protección de Datos** (AEPD) para llevar a cabo su **inscripción en el Registro General de Protección de Datos** .

Por último, en el caso de alta del fichero, la inscripción en el registro ha de realizarse con **anterioridad** a su uso.

- Portabilidad

Si un paciente solicita los datos para irse a otra clínica, solo tendrá que autorizarnos para que la misma clínica que tiene sus datos, los envíe a la nueva clínica. Sin necesidad de entregárselos al paciente.

- Datos de menores:

El RGPD establece unas consideraciones especiales cuando se tratan y guardan datos de menores de 18 años. La más clara es la necesidad de contar con la autorización expresa de padres o tutores para poder trabajar con datos de menores de 16.

Aun así, el reglamento europeo permite a los estados miembros establecer una edad inferior, siempre que no sea menor de 13 años, en la que el consentimiento directo del afectado es suficiente. **En el caso de España, la edad fijada es de 13 años**, mientras que en la LOPD era de 14. Por otro lado, el RGPD requiere que los responsables del tratamiento verifiquen que se ha dado el consentimiento paterno o de los tutores legales cuando sea necesario.

2. Nuevas obligaciones del responsable y encargado del fichero

El responsable del tratamiento de datos debe garantizar la seguridad de los datos y el cumplimiento del reglamento (y poder demostrarlo).

Toda la documentación nueva que se expone a continuación deberá ser incluida en el documento de seguridad, cuya creación es obligatoria y debe custodiar el responsable del fichero.

– **Contrato de encargo**: El encargado del fichero deberá ofrecer garantías de que va a aplicar las medidas técnicas y organizativas para adecuarse al reglamento, formalizado mediante un contrato de encargo (con forma jurídica de contrato). Las directrices para realizar ese contrato de encargo tienen como base el artículo 25 del Reglamento de la UE. Para facilitar la redacción de dicho contrato la Agencia de protección de datos (AGDP) ha redactado unas directrices que podéis encontrar aquí: Directrices contrato de encargo.

– **Elaborar una valoración de riesgo**: Se debe realizar una valoración de los posibles riesgos iniciales que pueda tener nuestro fichero. Para ello, es necesario responder a una serie de preguntas, que vienen la Guía que ha elaborado la AGDP y que son las siguientes:

- ¿Se tratan datos sensibles?
- ¿Se incluyen datos de una gran cantidad de personas?
- ¿Incluye el tratamiento la elaboración de perfiles?
- ¿Se cruzan los datos obtenidos de los interesados con otros disponibles en otras fuentes?
- ¿Se pretende utilizar los datos obtenidos para una finalidad para otro tipo de finalidades?
- ¿Se están tratando grandes cantidades de datos, incluido con técnicas de análisis masivo tipo big data?
- ¿Se utilizan tecnologías especialmente invasivas para la privacidad, como las relativas a geolocalización, videovigilancia a gran escala o ciertas aplicaciones del Internet de las Cosas?

Se tienen que diseñar unas medidas organizativas y de seguridad conforme a dichos riesgos.

La evaluación de impacto es un análisis del riesgo cuyo objetivo es permitir a los responsables del tratamiento **tomar medidas adecuadas para reducir dichos riesgos (minimizar la probabilidad de su materialización y las consecuencias negativas para los interesados).** En función del tipo de riesgo y cuanto mayor sea, se tendrán en cuenta una serie de medidas que no se aplican para tipos de riesgo bajos.

Al margen del análisis de riesgo, se debe tener en cuenta que el RGPD contempla lo que se ha llamado **la protección de datos desde el diseño y por defecto**. Esto quiere decir que, antes de empezar a tratar los datos, los responsables deben tomar medidas organizativas y técnicas para garantizar el cumplimiento del reglamento de protección de datos. Sobre todo, se debe garantizar que solo se traten los datos necesarios.

Asimismo, las medidas de seguridad y los protocolos que se deban llevar a cabo han de plasmarse en un **Documento de Seguridad.** Dicho documento deberá estar siempre a disposición de la Agencia Española de Protección de Datos para su consulta si así lo requiriera.

La LOPD determinaba con detalle las medidas de seguridad a aplicar. Con el RGPD, las empresas deberán establecer sus propias medidas para garantizar la seguridad en función de los riesgos detectados. Así, como recuerdan desde la AEPD, el esquema de medidas de seguridad previsto en la LOPD no seguirá siendo válido.

– Mantener un **registro de actividades de tratamiento**: Los responsables y los encargados están obligados (siempre en los casos de tratamiento de datos de salud, genéticos o biométricos con independencia de emplear o no a más o menos de 250 personas), a mantener un registro de las actividades de tratamiento que realicen.

Este registro debe de contener al menos los siguientes datos:

- Identificación y datos de contacto de responsable, corresponsable, representante y delegado de protección de datos.
- Fines del tratamiento.
- Descripción de categorías de interesados y datos.
- Categorías de destinatarios existentes o previstos (inclusive en terceros países u organizaciones internacionales).
- Transferencias internacionales de datos y documentación de garantías para transferencias de datos internacionales exceptuadas sobre base de intereses legítimos imperiosos.

– **Lista de verificación**: Se obliga a la realización de una lista de verificación, que parece sustituir a la auditoría de seguridad del reglamento anterior y que se guardará junto al documento de seguridad.

3. Otras novedades:

– **Notificación a la AEPD de las violaciones de seguridad**: "La destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos" se entenderá como una violación de seguridad. Así, la pérdida de ordenador o de un disco duro con datos de pacientes son ejemplos de ello. El nuevo reglamento obliga al responsable de fichero a comunicarlo a la Agencia de Protección de datos. Los detalles vienen expuestos a partir de la página 25 de la Guía. La notificación no es necesaria en los siguientes casos:

- El responsable hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado de los datos.

- Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.

– **Delegado de protección de datos**: Es una de las nuevas figuras introducidas por el RGPD. Es el contacto para los interesados dentro de la empresa que trate los datos. Debe disfrutar de autonomía y estar en contacto directo con la directiva de la empresa. Además, la compañía garantizará que dispone de los recursos necesarios.

Esta nueva figura **solo será obligatoria si** se trata de:

- Autoridades y organismos públicos
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a **gran escala.**
- Responsables o encargados que tengan entre sus actividades principales el **tratamiento a gran escala de datos sensibles.**

Nota: La falta aún de la ley española y por lo poco concreto que es el Reglamento europeo lleva a confusión con respecto a la obligatoriedad de la figura de Delegado de Protección de Datos en las clínicas privadas. Si se tiene en cuenta que toda entidad sanitaria estará obligada a contar con un DPO porque es lo que pone en el proyecto de ley español, los podólogos también porque son sanitarios. El problema es que ese proyecto no se ha aprobado aún y es posible que se apruebe después de que el Reglamento entre en vigor. En cuanto a lo que dice el Reglamento Europeo es que obliga a tener DPO a las entidades que traten datos de categorías especialmente protegidas (ahí están los datos de salud) si el tratamiento que realizan es "a gran escala". En ese término está el problema, ya que no está bien definido que se entiende por gran escala. Podemos pensar que una clínica pequeña no trata datos a gran escala, pero el proyecto de ley español no hace distinción en cuanto a grandes o pequeños.