

Ley de Protección de Datos

Os informamos de las obligaciones y plazos que la normativa en esta materia nos impone para los ficheros de clientes que tenemos en nuestras consultas dentales:

En primer lugar, la actual normativa en protección de datos obliga a todos aquellos que mantengan una serie de datos personales de terceros las obligaciones de registrar los ficheros en la Agencia de Protección de Datos (APD) y de implantar unas medidas de seguridad. El régimen legal se encuentra en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y el Real Decreto 994/1999 de 11 de junio, de Medidas de Seguridad.

Dicha Agencia entiende por fichero todo conjunto organizado de datos de carácter personal cualquiera que sea la forma o modalidad de creación, almacenamiento, organización y acceso, y la obligación de registro afecta tanto a los ficheros automatizados como aquellos que no lo sean.

INSCRIPCIÓN FICHEROS EN LA A.P.D.

- Ficheros de nueva creación: no tiene un plazo para su registro aunque hay que tener en cuenta que la comunicación a la agencia debe ser previa a su utilización.
- Ficheros antiguos: Los ficheros que ya existían al día de 14 de enero de 2000 deben adecuarse a la normativa vigente:
 - Si son ficheros automatizados: antes del 14 de enero de 2003.
 - Si no están automatizados: antes del 24 de octubre de 2007.
- Tramitación de la comunicación: se remitirá a la Agencia un formulario cuyo impreso se puede solicitar a la propia Agencia (calle Sagasta nº 2 - Madrid) o efectuarse a través de su página WEB. (www.agpd.es)
- Régimen sancionador: no solicitar la inscripción de ficheros de nueva creación y no comunicar la adaptación es una infracción leve susceptible de ser sancionada con una multa de cien mil a diez millones de pesetas.

IMPLANTACIÓN DE MEDIDAS DE SEGURIDAD

a) Los ficheros de los colegiados que mantienen datos relativos a la salud de los pacientes deben respetar las medidas de seguridad de nivel alto:

- Creación de un documento de seguridad.
- Nombramiento de un responsable de seguridad.
- Hay que someter a una auditoría, al menos cada dos años, los sistemas de información e instalaciones de tratamiento de datos.
- Cifrado de los datos en caso de transmisión o transporte de los mismos.
- Llevanza de un registro de accesos y otro de incidencias.
- Conservación de una copia de respaldo y procedimientos de recuperación de datos en lugar diferente al del equipo informático que los trate.

- b) Todo fichero de nueva creación debe respetar desde el inicio dichas medidas
- c) Los ficheros creados antes del 26 de junio de 1999 deben implantar las medidas de nivel alto antes del día 26 de junio de 2001.
- d) El hecho de mantener los ficheros sin las debidas condiciones de seguridad constituye una infracción grave de la Ley de Protección de Datos de Carácter Personal susceptible de ser sancionada con una multa de diez a cincuenta millones.

De todos modos, os iremos remitiendo más información a medida que vaya saliendo y disponéis en la administración colegial de copia de los impresos de solicitud. Además, el Colegio estudiará acuerdos de colaboración, si son precisos, con empresas especializadas

NORMATIVA VIGENTE

[Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.](#) Ley que deroga la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

[Real Decreto 994/1999, de 11 de junio, por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.](#) Real Decreto que si bien es anterior a la Ley Orgánica 15/1999 está en vigor en tanto no se apruebe su correspondiente desarrollo reglamentario.

[Acuerdo del Consejo de Ministros de 22 de junio de 2001](#) por el que el plazo para implantar las medidas de seguridad en ficheros automatizados en funcionamiento a la entrada en vigor del Reglamento de Seguridad (26 de junio de 1999) se amplía en un año hasta el **26 DE JUNIO DE 2002.**

ÁMBITO DE APLICACIÓN

Esta legislación tiene por objetivo garantizar las libertas públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar, en todo lo que concierne al tratamiento de los datos personales cualquiera que sea la forma o modo de creación, almacenamiento, organización y acceso. Obliga a todos aquellos que mantengan una serie de datos personales de terceros a registrar los ficheros en la Agencia de Protección de Datos (APD), así como a implantar unas medidas de seguridad

En concreto, en las Consultas y Clínicas Dentales:

- Ficheros tanto físicos como automatizados (software).
- Fichas de datos clínicos
- Fichas de datos contables

Trasvase de datos a :

- Administración (PADI)
- Seguros Médicos y Aseguradoras (Igualatorio, Sanitas ...).
- Proveedores (Protésicos....)
- Acceso por personal interno a dichos datos.

INSCRIPCIÓN DE LOS FICHEROS EN LA AGENCIA DE PROTECCIÓN DE DATOS

Ficheros de nueva creación: no tiene un plazo para su registro aunque hay que tener en cuenta que la comunicación a la agencia debe ser previa a su utilización.

Ficheros antiguos: Los ficheros que ya existían al día de 14 de enero de 2000 deben adecuarse a la normativa vigente:

Si son ficheros automatizados: antes del 14 de enero de 2003.

Si no están automatizados: antes del 24 de octubre de 2007.

Tramitación de la comunicación. Se puede tramitar por diversos medios:

Internet: En su página WEB (www.agpd.rd) se puede descargar el programa para generar notificaciones a través de la red. No obstante la hoja de solicitud generada por el programa se deberá enviar al Fax 91.448.36.80. o por correo ordinario.

- Soporte magnético: En la página web antes citada se puede descargar el programa dentro del apartado Registro General de Protección de Datos.
- En papel: El formulario se puede solicitar a la propia Agencia (calle Sagasta nº 2 - Madrid) u obtenerlo a través de su página web e incluso se encuentra a vuestra disposición en la sede del Colegio, para remitirlo por Correo a la Agencia de protección de datos.

Régimen sancionador: no solicitar la inscripción de ficheros de nueva creación y no comunicar la adaptación es una infracción leve susceptible de ser sancionada con una multa de cien mil a diez millones de pesetas.

CODIGO TIPO DE TRATAMIENTO DE DATOS DE CARACTER PERSONAL PARA ODONTOLOGOS Y ESTOMATOLOGOS DE ESPAÑA

IV IMPLANTACIÓN DE MEDIDAS DE SEGURIDAD

Los ficheros de los colegiados que mantienen datos relativos a la salud de los pacientes deben respetar las medidas de seguridad de nivel alto:

De todos modos, para entender mejor la implantación de las medidas de seguridad es preciso distinguir los tipos de ficheros:

1) Por su nivel de seguridad

-Los referentes a datos contables el nivel de seguridad es bajo.

-Los referentes a datos clínicos son de nivel alto.

2) Por su forma de soporte:

-Físicos (fichas que se guardan en un archivo)

-Software.

Es habitual en las consultas dentales que se presenta una mezcla de ficheros tanto de diferente nivel de seguridad como de soporte. Esto es debido sobre todo a que la informatización de las Consultas es gradual y se usan programas parciales que conviven con otros soportes. No obstante, incluso en aquellas que están totalmente informatizadas se presentan problemas dado que hay un único programa que lo gestiona todo. En la actualidad, tanto los programas parciales como los que integran todo en uno, lo más probable es que no estén adaptados a las necesidades que marca la legislación que nos ocupa.

V MEDIDAS DE SEGURIDAD

En este apartado hemos de distinguir los ficheros físicos de los que están automatizados, dado que si bien en ambos casos estamos ante datos referentes a la salud, que están especialmente protegidos por la Ley Orgánica 15/1999. Sin embargo, en la asunción de medidas de seguridad no existe la misma claridad reglamentaria.

1) Ficheros físicos:

El Real Decreto 994/1999 se refiere a ficheros automatizados y si bien por analogía se pueden adoptar ciertas medidas respecto a ficheros físicos, es evidente que algunas de las medidas son imposibles: mecanismos de acceso, registro de los accesos, copia de respaldo, cifrado de datos que se vayan a transportar.

Por tanto, la situación actual es que no existe una reglamentación al respecto.

Tras consultarlo con la Agencia de Protección de Datos, indica que no hay regulación para este tipo de datos de modo que se deben tomar las medidas que la prudencia y el sentido común exijan.

Por precaución, es aconsejable **guardar bajo llave las fichas de los pacientes**, encontrándose estas bajo la responsabilidad del responsable de seguridad y fuera del acceso de aquellas personas sin autorización para su uso, así como **evitar el traslado de fichas físicas fuera de la consulta**.

2) Ficheros automatizados:

Es en éste caso donde el Real Decreto 994/1999 entra de lleno.

Las medidas de nivel alto que se deben adoptar son las siguientes:

a) **Creación de un documento de seguridad.**

Este documento debe contener como mínimo los siguientes aspectos:

- Identificación del responsable o responsables de seguridad.
- Ámbito de aplicación del documento detallando los recursos protegidos.
- Medidas y reglas para garantizar el nivel de seguridad establecido en el Reglamento.
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos sobre salud y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Procedimientos de realización de copias de seguridad y su recuperación.
- Control periódico para verificar las normas establecida en el documento.
- Medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado.

Este documento debe mantenerse siempre actualizado y será revisado cuando haya cambios.

Su contenido se adecuará a las disposiciones vigentes sobre seguridad de datos de carácter personal.

b) **Nombramiento de responsable de seguridad**

c) **Someter a una auditoría, al menos cada dos años, los sistemas de información e instalaciones de tratamiento de datos.**

Puede ser interna o externa pero es de índole técnica: debe señalar la adecuación de controles a la normativa sobre medidas de Seguridad, identificar deficiencias y proponer medidas correctoras. El informe de auditoria será revisado por el responsable de seguridad.

d) Cifrado de los datos en caso de transmisión o transporte de los mismos.

Es preciso cifrar la copia de respaldo, así como los datos que se transporten fuera de la consulta, del mismo modo se debe cifrar cualquier información que se transmita por redes de telecomunicaciones.

e) Llevanza de un registro de accesos y otro de incidencias.

Es preciso controlar el acceso a los sistemas de información y sólo se autorizará el acceso a aquellos datos que precisen para el desarrollo de sus funciones.

Este control de acceso se puede realizar mediante mecanismos de autenticación mediante contraseñas que se cambiarán con una determinada periodicidad (normalmente no supera el mes).

- **Acceso:**

El responsable de seguridad debe encargarse de que haya una relación actualizada de usuarios con acceso al sistema de información.

De cada acceso se guardará la identificación del usuario, fecha y hora, fichero accedido, tipo de acceso y si ha sido concedido o denegado. Estos datos se deben conservar durante dos años como mínimo y se debe revisar por el responsable de seguridad al menos cada mes

- **Incidencias:**

Debe detallar tipo de incidencia, momento en el que se ha producido, persona que hace la notificación, a quién se le comunica y efectos. Procedimientos llevados en su caso para recuperar datos, quien lo realizó, datos restaurados y datos que han sido necesarios restaurarlos a mano.

f) Realización de copias de respaldo.

Se deben realizar al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de datos.

Deben ser guardados en lugar diferente a donde estén los equipos informáticos y cumpliendo las medidas de seguridad de este reglamento, por lo que lo más idóneo es que estén cifrados, tal y como hemos indicado anteriormente.

Si bien esta lista es exhaustiva, muchos de estos requisitos son asumibles de manera informatizada. Por ello, los consejos que se pueden dar son los siguientes:

Aquellas consultas que se vayan a informatizar se deben asegurar que el programa a comprar esté adaptado a esta normativa. Aquellas que ya tienen un programa deben revisar si cumple las especificaciones de esta normativa y adaptarlo e incluso cambiarlo si no es posible adaptarlo. El coste de la adaptación puede ser más alto que el del cambio por un programa nuevo. Es preferible contar con dos bases de datos separadas; los datos sobre salud y los datos contables o de administración.

VI PLAZOS

- 1) Todo fichero de nueva creación debe respetar desde el inicio dichas medidas.
- 2) Los ficheros creados antes del 26 de junio de 1999 deben implantar las medidas de nivel alto antes **DEL DÍA 26 DE JUNIO DE 2002.**

El hecho de mantener los ficheros sin las debidas condiciones de seguridad constituye una infracción grave de la Ley de Protección de Datos de Carácter Personal susceptible de ser sancionada con una multa de diez a cincuenta millones.