Col·legi Oficial de Podòlegs de Catalunya

LAS AUDITORIAS EN NUESTRO SISTEMA DE PROTECCION DE DATOS

Informe Asesoría Jurídica 18 febrero 2016

Problemática planteada: ***¿si es obligatorio, dados sus elevados costes, que las auditorias las realicen empresas especializadas?***

La respuesta: es NO, es una gestión muy fácil de realizar.

¿Qué es y que finalidad tiene una auditoria

La auditoria es un sistema que impone la ley al objeto de que las personas que han comunicado sus ficheros a la Agencia de Protección de Datos, **verifiquen si el sistema de protección que tiene establecido para sus ficheros funciona y garantiza la protección de los datos contenidos en los mismos** y, también es un sistema par realizar un análisis de las incidencias (si es que las hubo) y reflexionar sobre las que puedan surgir.

Por lo tanto, se trata de revisar periódicamente el sistema de protección de los datos contenidos en los ficheros de la consulta, **para evitar que la rutina nos haga olvidar la importancia de proteger la intimidad de nuestros pacientes.**

Obligatoriedad de las auditorias

El artículo 96.1 del Real Decreto 1720/2007, que desarrolla la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales, **establece la obligación de las auditorias.**

Las **auditorias deben hacerse cada dos años**

El artículo 96.1 del Real Decreto 1720/2007, de 21 de diciembre, aprueba el reglamento, aprueba el desarrollo de la

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que señala:

"*A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoria interna o externa que verifique el cumplimiento del presente título* (la ley)…" (**las historias clínicas son de nivel alto y el fichero de clientes, caso de tenerlo, es de nivel medio).**

¿El podólogo puede realizar su propia auditoria?

Sí. La mecánica de **una auditoria a nivel de los profesionales es muy sencilla,** también para las pequeñas empresas, porque el legislador, ha buscado un sistema muy simple de control para que todos puedan cumplir ese requisito. La ley permite **al profesional** y al pequeño empresario **que realicen su propia auditoria,** mediante las siguientes comprobaciones sobre sus ficheros se relacionan en el número 2 del citado artículo 96 y que son las siguientes:

"El informe de auditoria deberá dictaminar sobre la adecuación de las medidas y controles a la Ley … identificar sus deficiencias y proponer las medidas correctoras…"

El informe de la auditoria se realiza mediante el seguimiento del **documento de seguridad,** documento que quedará a disposición de la Agencia de Protección de Datos, o de las autoridades de control de la Comunidad Autónoma.

El documento de seguridad

La elaboración del documento de seguridad es sencilla, podemos hacerlo en una simple carpeta coleccionando en ella los informes de auditoría que vayamos realizando.

Su confección es fácil, porque mediante un escrito se explican de forma escrita las medidas de índole técnica y organizativa que tenemos establecido, de acuerdo con **el sistema de seguridad de nuestros ficheros que comunicamos en su día a la Agencia** (los tipos de ficheros que establecimos cuando los comunicamos en su día a la Agencia Española de Protección de Datos y las medidas de seguridad que adoptamos para que nadie, no autorizado, pueda acceder a ellos).

A este **documento de seguridad**, es un documento interno del podólogo, donde iremos añadiendo los informes de las auditorias que vayamos realizando cada dos años o bien antes, si se da una incidencia, que en ese caso la documentaremos sin esperar a la auditoria (por ejemplo: problemas de acceso, rectificación, cancelación de datos, etc. si los hubo se hace una pequeña reseña de cómo lo hemos solucionado).

Recordemos que en una consulta el podólogo, generalmente, tiene uno o dos tipos de ficheros:
-el obligado fichero de **historias clínicas** (con la finalidad de la asistencia sanitaria).
- y algunos podólogos tienen además el **fichero de clientes** (con la finalidad de tener los datos económicos de las visitas).

Resumiendo: la información que debe contener el documento de seguridad

De acuerdo con el artículo 88 del citado Real Decreto 1720/2007, la tan citada norma, deberemos incluir en el documento:

a)especificación de los ficheros protegidos que tiene el podólogo (ejemplo fichero de clientes, fichero de historias clínicas, etc.).

b) las medidas que hemos adoptado para garantizar la seguridad de los ficheros, o sea las medidas de seguridad que tenemos establecidas para que nadie acceda a esos datos sin previo consentimiento, por ejemplo en un armario con llave, una clave para entrar en las historias informatizadas, etc. (las historias clínicas son ficheros de nivel alto).

c) procedimientos de respuesta a incidencias, caso de solicitudes de acceso, rectificación, cancelación de datos, etc. sean sanitarios o sobre datos económicos o anotaciones subjetivas en las historias, etc. señalando en su caso como se han solucionado y si son adecuadas las medidas de seguridad.

d) procedimientos sobre las copias de seguridad **solamente en historias clínicas informatizadas** que periódicamente debemos realizar sobre los ficheros informáticos, ya que deben hacerse periódicas copias de seguridad, para el caso que por accidente (robo o destrucción) pudiese destruirse el fichero. También debe incluir en el redactado del documento de seguridad, **la localización de las copias de seguridad y la forma de destrucción de las citadas copias anteriores** para quedarnos únicamente con la última.

e) persona responsable de la seguridad de los ficheros Normalmente es el mismo podólogo, que firmará el informe de auditoría.

Los documentos de seguridad quedan a disposición de un posible requerimiento de la Agencia Española de Protección de Datos.

Col·legi Oficial de Podòlegs de Catalunya

Documento recomendado para abrir una historia clínica

Al objeto de informar sobre la Protección de datos e Historias Clínicas, recomendamos que a cada paciente al que se abra una historia clínica, acepte y firme el siguiente documento:

"……, manifiesta: *que ha sido informado/a que sus datos sanitarios incorporados a su historia clínica, quedan protegidos, en aplicación de la L.O. 15/1999, de 13 de diciembre de protección de datos de carácter personal, especialmente por su artículo 10 que señala la obligación del secreto profesional; también ha sido informada de su derecho de acceso, rectificación y cancelación de sus datos personales, de acuerdo con los artículos 15 y 16 de la citada ley.*

En la ciudad de …… a …… de …… de ……"