LAS AUDITORÍAS DE NUESTROS SISTEMAS DE PROTECCIÓN DE DATOS

Mariano Gómez Jara.
Licenciado en Derecho.

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.**

Finalidad de 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.**

Las auditorias deben hacerse cada dos años

"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, generalmente, es de nivel medio).

El podólogo puede realizar su propia auditoria

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, y su confección es fácil, porque mediante un escrito se explican 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** (aquellas que establecimos cuando comunicamos la existencia de nuestros ficheros).

A este documento le 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 (generalmente a nivel del podólogo se dan pocos problemas, pero si los hubo se hace una pequeña reseña de cómo lo hemos solucionado).

Recordemos que en una consulta generalmente

tenemos dos tipos de ficheros:

- el fichero de **clientes** (con finalidad económica).
- el fichero de **historias clínicas** (con la finalidad de la asistencia sanitaria).

Por lo tanto en la carpeta "documento de seguridad" se recogerá la **función de cada fichero y las medidas de seguridad que establecimos o hayamos modificado para mayor seguridad**.

El documento de seguridad **es un documento interno del podólogo** (o de cualquier otro profesional o pequeño empresario). Este sencillo documento, deberá mantenerse actualizado, mediante la auditoria, y deberá ser revisado cuando se produzcan cambios relevantes en el sistema de información o tratamiento de datos, o sea cambios que puedan repercutir en los sistemas de seguridad, por ejemplo unas historias clínicas que teníamos en soporte papel, las pasamos a soporte informático.

Información que debe contener el documento de seguridad

De acuerdo con el artículo 88 de 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 (las historias clínicas son ficheros de nivel alto).

Recordemos que nuestro fichero informático de historias clínicas debe estar protegidos mediante un sistema que garantice su reproducción (por ejemplo, que tengamos que sacar una copia en papel de la historia) pero debe ser un programa que garantice que no pueda manipularse (cambiar datos), que solamente pueda corregirse durante unas horas, pasadas las cuales no se podrá corregir ningún registro de la historia, por ejemplo los datos de una determinada asistencia. También tenemos que tener una clave personal para entrar al fichero de historias clínicas (llave de acceso a restringido al podólogo) para que únicamente pueda acceder el podólogo al objeto de estudio o registro de las actividades sanitarias realizadas que se trasladen a la historia clínica.

c) procedimientos de respuesta a incidencias, caso que existan reclamaciones de algún paciente (o su representante legal) sobre acceso a sus datos comerciales o sanitarios y sobre su cancelación sobre datos económicos o anotaciones subjetivas, etc.
d) procedimientos sobre copias de seguridad que periódicamente debemos realizar sobre los ficheros informáticos (historias clínicas o fichero de clientes) 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, 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 (generalmente es el mismo podólogo).
f) los controles periódicos (auditorias), o sea ver si funciona correctamente el sistema y si han habido quejas o fallos, y en ese caso, como se han tratado, como se han solucionado.

Recordemos las medidas de seguridad

Todos los ficheros deben **adoptar las medidas de seguridad**, las calificadas de nivel básico (que son las habituales y muy simples común a todos los fichero) **más las que correspondan con el tipo de fichero** (los datos sanitarios son de nivel alto y ello exige a un sistema de seguridad estricto).

Ayuda de la Agencia de Protección de Datos

La Agencia, con un medio **totalmente anónimo**, nos ofrece la posibilidad de un **autotest** sobre nuestro sistema mediante un simple procedimiento que la Agencia de Protección de Datos, nos facilita para conocer si lo hacemos correctamente.

El autotest consiste en una serie de preguntas y respuestas muy simples, que nos orientan sobre la bondad o defectos de nuestro sistema de protección de datos personales de nuestros pacientes y su posible corrección.

La forma de acceder al autotes es la siguiente:

Vía **Internet** a la **Agencia de Protección de Datos** y para el uso de la herramienta ir al **link** **http://212.170.243.77:8080/Evalua/home.seam**