EL DENTISTA ANTE LA LEY

Compartir archivos en las clínicas dentales: el riesgo sobre las historias clínicas

En nuestra actividad auditora vemos que los hechos fortuitos o accidentales y la actuación del personal de las clínicas dentales están detrás de un importante porcentaje de infracciones de la normativa de protección de datos. Ya no es suficiente que la clínica o el titular de los ficheros cumpla con la Ley Orgánica de Protección de Datos, sino que debe valorar los riesgos a los que su organización está sometida y adoptar las medidas necesarias para minimizarlos.

En el caso del personal auxiliar, evitar una conducta maliciosa puede ser muy complicado, aunque, si tenemos una auditoría bien hecha y la clínica adaptada a la normativa vigente, tendremos los registros necesarios para poder demostrar su actuación, pero cuando se trata de prevenir errores o conductas accidentales es importante ofrecer toda la información y especialmente la formación necesaria de manera que cada trabajador conozca cuáles son sus obligaciones y responsabilidades.

Resulta llamativo cómo encontramos con bastante asiduidad, instalados en los ordenadores del personal auxiliar e incluso de los colaboradores, programas para compartir archivos, y cómo, con sorpresa, los titulares de las clínicas nos preguntan cómo han podido llegar a sus ordenadores o, simplemente, qué es eso de compartir archivos. Compartir archivos es utilizar la tecnología o, en definitiva, programas que permiten a los usuarios compartir archivos que están alojados en sus ordenadores individuales. Las aplicaciones "*peer to peer*", o "entre iguales" (P2P), tales como aquellas utilizadas para compartir archivos de música, son algunas de las formas comunes de la tecnología para compartir archivos.

APLICACIONES P2P

Es evidente que estos programas son un valioso recurso para compartir archivos de manera masiva con varios usuarios. Pero, por otro lado, son una puerta abierta al exterior por la que cualquiera puede explorar las partes del ordenador de la clínica que decidamos mostrarle. Basta con que el ordenador esté encendido y el programa activo para que otro internauta entre a visitar el ordenador de nuestra clínica. Y ese internauta no estará haciendo algo ilegal porque, para empezar, ha sido nuestro personal de la clínica, y por tanto su titular responsable, quien le ha invitado a entrar.

Al usar las aplicaciones de P2P, la clínica está dando a otros usuarios el acceso a su información profesional, ya sea porque

El cumplimiento de las medidas de seguridad establecidas en el Reglamento que desarrolla la LOPD son importantes, pero de nada sirven si no se elaboran protocolos internos por los que los trabajadores conozcan sus obligaciones y responsabilidades

Ricardo de Lorenzo y Aparici

ciertos directorios se encuentran accesibles o porque en su propia actividad profesional está brindándose información clínica a lo que el dentista cree que es una persona u organización fiable, con lo que personas no autorizadas pueden acceder a sus historias. Una vez que la información es expuesta a gente no autorizada, es difícil saber cuántos más accedieron a ella. La disponibilidad de esta información puede incrementar incluso el riesgo de robo de identidad. A pesar de las recomendaciones sobre las medidas de seguridad, es evidente que son errores inexcusables que conllevan la pertinente sanción. Recientemente la Audiencia Nacional ha ratificado una resolución de la Agencia Española de Protección de Datos en la que sancionaba al Servicio Cántabro de Salud por difundir datos personales de alrededor de dos mil pacientes a través de Internet. Se trata de un caso en el que se constató la existencia de un archivo accesible desde el programa eMule, que contenía datos de filiación de pacientes y ciertos datos de salud de los mismos. Dicha resolución fue recurrida por el Servicio Cántabro de Salud alegando, entre otros motivos, que la infracción pudo haber sido cometida por el personal que tenía acceso a las historias clínicas que, en definitiva, sería quien habría infringido la observancia del deber de secreto. Es lógico pensar que efectivamente fue alguno de los trabajadores quien instaló el eMule en su ordenador y quien, probablemente de manera accidental, subió a este programa el archivo que contenía los datos de carácter personal de los pacientes.

Sin embargo, manifiesta la Audiencia Nacional que, si bien es posible que haya sido un trabajador quien haya realizado esta divulgación de datos a través de Internet, esta situación no exime al Servicio Cántabro de Salud, ya que como titular de los ficheros, es al mismo a quien corresponde el cumplimiento de las medidas de seguridad, no sólo su aprobación sino su aplicación real y efectiva.

EXPEDIENTES ABIERTOS

Y no es un hecho aislado, porque desgraciadamente es habitual que, como consecuencia de descargarse música o películas desde el ordenador del trabajo a través de uno de estos programas de intercambio de archivos, se estén produciendo estos efectos trágicos y no calculados, causados por quien quizá sólo pretendía meter en su MP3 la última canción de moda, pero que están motivando como acabamos de ver numerosas resoluciones de la Agencia Española de Protección de Datos en las que se sanciona la aparición en Internet de archivos con datos de pacientes.

El desconocimiento tecnológico de algún empleado de una clínica ginecológica de Bilbao, puso a disposición del ya repetido programa eMule, y por lo tanto al alcance de millones de personas, todos sus datos, contenidos en una carpeta del disco duro de su ordenador. Nunca se ha podido saber con exactitud quién fue el culpable, ni las razones de la filtración, pero la Agencia Española de Protección de Datos sancionó a la clínica, con 150.000 euros.

Como decía, no son casos únicos, existen bastantes expedientes abiertos, por asuntos similares. Éste último citado es especialmente grave al tratarse de datos médicos ginecológicos y de urología y, en 4.000 ca-

sos, son historias clínicas relacionadas con interrupciones voluntarias del embarazo, extremadamente sensibles y cuya divulgación afecta a la intimidad de las mujeres. El Centro Médico afirmó ante la Agencia de Protección de Datos que desconocían cómo el fichero había acabado en Internet a la vista de cualquiera. No sabían si había sido el error de un empleado o algo premeditado por alguna persona.

La Agencia abrió una inspección. En el centro médico bilbaíno encontraron un fichero de gestión de pacientes igual que el que se había hallado en Internet. En el mismo se podía acceder a datos de las consultas de ginecología, vasectomías e interrupciones de embarazo por aspiración y por píldora. Los registros aparecían asociados a pacientes y a su historia clínica.

La clínica implantó de inmediato en su sistema informático las medidas de seguridad de nivel alto que marca la Ley. Pero por la filtración de los datos fue sancionada por "infracción muy grave", como he indicado, con una multa de 150.000 euros. La sanción podía haber sido mayor -la Ley de Protección de Datos castiga este tipo de infracciones con multas de 300.000 a 600.000 euros-, pero se moderó por la colaboración mostrada por los titulares del Centro a lo largo del procedimiento, que desarrolló una extensa actividad para evitar la comisión de infracciones en materia de protección de datos de carácter personal, según la resolución de la Agencia.

Podemos seguir, la Agencia impuso una multa de 6.000 euros a un médico nutricionista del que se encontró un archivo en el mismo programa con datos de más de 500 pacientes. En este caso se trató de un error inexcusable de la clínica, que no tenía las medidas de seguridad necesarias para evitar que pudiera producirse una filtración de estas características.

INVESTIGACIÓN

Debido a la marcada incidencia de denuncias por violación de seguridad y confidencialidad de diversos tipos de documentación sanitaria, la Agencia de Protección de Datos inició en marzo una investigación que culminó recientemente con el llamado "Informe de cumplimiento de la LOPD en Hospitales" orientado a más de 600 entidades instituciones públicas y privadas españolas para recolectar información sobre el acatamiento de la Ley Orgánica de Protección de Datos (LOPD).

Para tener idea de su importancia, en 2009 se interpusieron 123 denuncias y en la mitad del presente 2010, ya se había llegado a las 100. Las causas son el hallazgo de documentos con datos personales en plena calle, el acceso a la información por personas no autorizadas, el mantenimiento de archivos en lugares no seguros, como hemos visto anteriormente, el envio telemático de datos personales sanitarios mediante eMule, pérdida de datos personales en la digitalización de historias clínicas, así

Una vez que la información es expuesta a gente no autorizada, es difícil saber cuántos más accedieron a ella. La disponibilidad de esta información puede incrementar incluso el riesgo de robo de identidad

Para las actuaciones malintencionadas, así como para aquellas realizadas por error o accidente, a pesar de los medios puestos por la clínica dental, lo mejor es proveerse de un buen seguro

como entrega de historias clínicas o información a personas u otras entidades no admitidas.

La recolección de información se llevó a cabo mediante un requerimiento de información que fue completado por el 92%, o sea, 562 de los más de 600 que lo recibieron. El requerimiento se focalizó en medidas de seguridad y confidencialidad adoptadas por las distintas clínicas y hospitales.

A pesar de que el 98% de las clínicas e instituciones hospitalarias privadas y el 83% de las públicas tenían con sus auditorías reglamentarias sus Documentos de Seguridad, pudo observarse que:

-Existía un elevado déficit de medidas de seguridad, protección de datos, auditorias del nivel de seguridad, incorporación de cláusulas informativas en los documentos/formularios para recoger datos de pacientes.

-Si bien se inscriben con carácter general, como establece la normativa, los ficheros estas inscripciones no superan el 75%, en cambio las auditorias bienales legalmente establecidas no superan el 44% en el caso de los hospitales públicos, con un cumplimiento mayor en los privados, así como es también baja la actualización de las inscripciones.

-Muchos hospitales y clínicas no poseen disposiciones de seguridad para que los datos personales de la historia clínica no se pierda o puedan acceder a ella quienes no están autorizados en el momento de su traslado. En cuanto a los registros de quienes pueden acceder a la documentación, un porcentaje significativo no lo poseen. Es notable que sólo el 25% de los públicos y 65% de los privados realicen audiencias para verificar el uso correcto de los datos personales de pacientes por personal autorizado para un objetivo establecido.

-En cuanto a las cláusulas informativas en los documentos/formularios para obtener datos personales de los pacientes que requiere la Ley, no se cumple correctamente. Gran parte de las instituciones hospitalarias, tanto públicas como privadas (86%), utilizan la prestación de servicios externos, lo que obliga a que ciertos datos sean manejados por otros. Entre las actividades realizadas por otros, se encuentran la de archivo de historias clínicas, realización de estudios médicos a pacientes, asesores, gestorías, compañías de asistencia sanitaria. En su mayor parte estos centros cumplen con los requisitos de la LOPD (artículo 12 sobre el manejo de datos por terceros, sus límites, cláusulas y control de seguridad). No obstante solo el 34% disocian los datos personales, lo cual es una recomendación para la protección de datos personales aunque no sea una obligación legal.

- Un porcentaje elevado de las clínicas privadas dicen poseer dispositivos seguridad para el almacenamiento de las historias clínicas en papel. Un 96% de privados y el 84% de los públicos dicen poseer mecanismos para respetar y hacer cumplir los

derechos de acceso, rectificación, cancelación y oposición, aunque la Agencia informa de cada vez más denuncias en solicitud de tutela de derechos para acceder a la historia clínica.

Para encontrar una solución, la Agencia ha enviado una lista de sugerencias y pasos a seguir a cada una de las clínicas y hospitales investigados y a las consejerías de Sanidad, instando a las más de 200 entidades que vulneran la ley a que solucionen e informen sobre los cambios realizados en no más de 6 meses. La Agencia también ha informado a la Subdirección General de Inspección de que 40 entidades hospitalarias no han cumplido con la información solicitada de la institución por lo cual se duda si cumplen o no con los requerimientos de la Ley Orgánica de Protección de Datos.

Por tanto, el cumplimiento de las medidas de seguridad establecidas en el Reglamento que desarrolla la LOPD son importantes, pero de nada sirven si las mismas no son conocidas por el personal o si no se elaboran protocolos internos por los que los trabajadores conozcan sus obligaciones y responsabilidades. De este modo se reducirán los riesgos de actuaciones accidentales por parte de los trabajadores. Para las actuaciones malintencionadas, así como para aquellas realizadas por error o accidente, a pesar de los medios puestos por la clínica dental, lo mejor es proveerse de un buen seguro.

Por último, recordar que la protección de datos es un derecho fundamental que se desarrolla a partir del artículo 18.4 de la Constitución Española. Este derecho hace referencia al poder de disposición y control sobre los datos personales que faculta a las personas físicas para consentir el conocimiento y tratamiento de sus datos por terceros. De esta manera, es la persona física, la única facultada para decidir lo que se puede hacer con sus datos de carácter personal. Trasladado al ámbito que nos ocupa, son los pacientes los que deciden qué es lo que el titular de la clínica puede hacer con los datos que el propio paciente le da al acudir a la consulta. Así, se podría entender que existe un consentimiento tácito por parte del paciente cuando acude a un dentista para recibir asistencia sanitaria, sin embargo, no se debe olvidar que esos datos, en numerosas ocasiones, se utilizan para más finalidades, como la facturación, la gestión administrativa de la clínica, el envío de publicidad sobre la clínica, la comunicación a doctores colaboradores, etc.

La Ley Orgánica de Protección de Datos nace con el objeto de garantizar y proteger el tratamiento de los datos personales entre los que se incluyen los relativos a la salud de una persona física identificada o identificable. En este sentido, la Ley en su artículo 7 y 8 hace referencia a este tipo de datos a fin de garantizar la protección jurídica necesaria en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos.

Finalmente, un consejo: preocúpense de tener un servicio de auditoría y consultoría de protección de datos personales, acreditado y fiable, mediante procedimientos basados en un conjunto de servicios integrales y multidisciplinares que permitan la adaptación de las clínicas dentales a la normativa vigente en materia de protección de datos y, mientras tanto, revisar los ordenadores de las clínicas para verificar si tenemos programas para compartir archivos y especialmente archivos accesibles desde el programa eMule.

* Abogado del Área de Nuevas Tecnologías de "De Lorenzo Abogados"
rdlaparici@delorenzoabogados.es
www.delorenzoabogados.es