La Ley de protección de datos, el nuevo reglamento y su incidencia en el ámbito sanitario

Ricardo de Lorenzo, De Lorenzo Abogados

La normativa de protección de datos afecta directamente al sector de la salud por la cantidad de datos que maneja y por el carácter sensible de los mismos, ya que afecta a la esfera más íntima de las personas. En este sentido, se debe ser consciente de la especial sensibilidad de los datos contenidos en las historias clínicas de los pacientes de Oncología Médica, debido a su peculiar susceptibilidad para causar perjuicios de especial gravedad en los derechos de los titulares, concretamente en su derecho a la intimidad.

El día de 19 de abril entró en vigor el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante LOPD), que tiene por finalidad desarrollar los mandatos contenidos en la mencionada Ley y aquellos aspectos que durante estos años de vigencia de la LOPD han planteado dudas interpretativas, tratando de aportar un mayor grado de seguridad jurídica.

Asimismo, se han introducido algunas novedades, siendo la más destacada la inclusión de un listado de medidas de seguridad que, en el caso que nos ocupa, deberán cumplir aquéllos que almacenan los historiales clínicos de sus pacientes en formato no informatizado. Hasta la fecha, este tipo de ficheros debía incorporar las medidas de seguridad necesarias para evitar que se produjeran pérdidas, alteraciones o accesos no autorizados existiendo únicamente un listado de medidas de seguridad para los ficheros informatizados.

En concreto, el responsable del fichero debe elaborar un documento de seguridad que recogerá todas las medidas técnicas y organizativas que será de obligado cumplimiento para todo el personal con acceso a datos de carácter personal y cuyo contenido viene dispuesto en el nuevo Reglamento. Como medidas de seguridad específicas del soporte manual, se establece que deberá existir en cada organización un criterio de archivo, de conformidad con lo establecido en la Ley 41/2002, de14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

En cuanto al almacenamiento de la información, se dispone que cuando se recaben datos de salud, los armarios o archivadores donde se encuentren, deberán situarse en áreas en las que el acceso esté protegido con sistemas de apertura mediante llave u otro dispositivo equivalente, que deberán permanecer cerradas cuando no sea preciso el acceso a la documentación que contiene datos de carácter personal.

Sólo se podrán hacer copias de la documentación bajo el control del personal autorizado en el documento de seguridad. Únicamente podrá acceder a la documentación el personal autorizado, debiéndose establecer mecanismos que permitan identificar los accesos realizados cuando los documentos puedan ser utilizados por múltiples usuarios.

Por último, destacar que, entre otras obligaciones, el responsable del fichero debe designar un responsable de seguridad, como ya está previsto para los ficheros

Sólo se podrán hacer copias de la documentación bajo el control del personal autorizado en el documento de seguridad. Únicamente podrá acceder a la documentación el personal autorizado, debiéndose establecer mecanismos que permitan identificar los accesos realizados cuando los documentos puedan ser utilizados por múltiples usuarios

automatizados y que este tipo de ficheros deberán someterse cada dos años a una auditoría externa o interna que verifique el cumplimiento de las medidas de seguridad.

Un aspecto interesante para los profesionales que, sin embargo, utilicen un soporte informático para el tratamiento de sus datos es que los programas de gestión que utilicen deberán especificar el nivel de seguridad que proporcionan: básico, medio o alto. Recomendamos que si se desea adquirir un software de gestión de pacientes, se verifique que cumple las medidas de seguridad de nivel alto.

Otra de las novedades que afecta al sector médico, y por tanto al oncológico, es la inclusión en el Reglamento de una definición de dato de salud, hasta la fecha inexistente, entendiendo por como tal *"las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética"*. Sin duda se trata de una definición amplia del concepto de dato de salud, con lo que el legislador pretende dotar al conjunto de informaciones contenidas bajo su ámbito de una mayor cobertura garantista, pues no se debe olvidar que se trata de datos sensibles que afectan a la esfera más íntima y personal de las personas, por lo que su uso debe estar rodeado de las mayores salvaguardas.

La regla general para tratar datos de carácter personal sigue siendo la obtención previa del consentimiento del titular de los datos. En el sector que nos ocupa, al tratarse como se ha visto de datos de salud, el consentimiento debe ser expreso. Sin embargo, existe una excepción a esta regla en el caso de que los datos se recojan para la prestación de asistencia sanitaria.

Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genérica

Esta excepción exige atender, por un lado, a la finalidad a la que se destinen los datos: la asistencia sanitaria, que es la finalidad para la que se realiza la historia clínica de acuerdo con el art. 15.2 de la citada Ley 41/2002 y, por otro lado, al principio de calidad de los datos, ya que sólo se pueden recabar aquéllos datos que sean adecuados, pertinentes y no excesivos en relación con la finalidad a la que se van a destinar tales datos. Por tanto, siempre que los datos se utilicen para otras finalidades, tales como la realización de estudios epidemiológicos, investigación, facturación, envío de publicidad, etc o que se pidan más datos de los necesarios para el historial médico, se deberá contar con el consentimiento expreso del paciente.

Por otro lado, no hay que olvidar que la excepción para la obtención del consentimiento no supone que no se deba informar al paciente. Este deber persiste en todo momento y de conformidad con el nuevo Reglamento el responsable del fichero (el centro sanitario o profesional que actúe por cuenta propia) deberá conservar el soporte en el que conste el cumplimiento del deber de informar. A efectos prácticos, y dado que la carga de la prueba recae sobre el responsable del fichero, al paciente se le debe informar por escrito, recomendándoles que en la primera visita que el paciente realice se le entregue un documento que contenga los aspectos que la LOPD exige –información sobre la finalidad a la que se van a destinar los datos, los destinatarios de los mismos, la identidad y dirección del responsable del fichero, de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición, etc.- y que tal documento sea firmado por el paciente, así en caso de surgir alguna controversia, el titular podrá probar que se le informó debidamente al paciente. En este sentido, nuestra recomendación es que en este documento se solicite, asimismo, el consentimiento del paciente ya que de este modo se evitarán posibles dudas interpretativas acerca de la utilización de los datos para finalidades que exceden la mera asistencia sanitaria, o la recogida de algunos datos que pueden ser considerados como excesivos para tal finalidad.

Por último, debe señalarse que se ha previsto un plazo para la implantación de las medidas de seguridad. Así, para los ficheros automatizados que contengan datos de salud se establece un plazo

de un año para la implantación de aquellas medidas de seguridad no previstas en el anterior Reglamento de Seguridad, y de dos años para los ficheros no automatizados, es decir, para los que conservan los historiales clínicos en papel.

No obstante, les recomendamos que no agoten los mencionados plazos ya que, en ocasiones, la implantación de las medidas de seguridad conllevará un esfuerzo que no será posible realizar en un solo acto porque además de las inversiones que se tengan que hacer en la organización y gestión de la documentación, se deberá realizar una importante labor de concienciación entre el personal que tenga acceso a los datos de carácter personal.

¿Qué debe hacer para cumplir la normativa de protección de datos?

Como ya se ha comentado la normativa de protección de datos es de obligado cumplimiento siempre que se recojan y almacenen datos de carácter personal, por este motivo todos los especialistas en oncología médica deberán observar la citada normativa. Los pasos a seguir para garantizar un correcto tratamiento de los datos son los siguientes:

1. Inscripción de los ficheros en la Agencia Española de Protección de Datos. Con carácter previo a la creación de una base de datos se debe notificar al Registro de la Agencia y solicitar su inscripción.
2. Sólo se podrán recabar los datos que sean necesarios para llevar a cabo la finalidad para la que el fichero fue creado, es decir, para la prestación de asistencia sanitaria. Cuando los datos ya no sean necesarios para la finalidad, éstos deberán ser cancelados.
3. Se debe informar a los pacientes de que sus datos van a ser almacenados en un fichero, de la finalidad del mismo y de la identidad del responsable del fichero, y habrá que solicitar su consentimiento para poder tratarlos. Como ya se ha mencionado, el responsable deberá garantizar que ha proporcionado esta información a los pacientes.
4. Se deberá facilitar a los interesados el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición. Facilitando, especialmente el derecho de acceso a la historia clínica.
5. Se deben implantar las medidas de seguridad necesarias en los ficheros para evitar su pérdida, alteraciones o accesos indebidos. Es importante contar con un documento de seguridad en el que se recojan todas las medidas de seguridad adoptadas y los protocolos creados en cada consulta para garantizar el correcto tratamiento de los datos. En caso de solicitud de la Agencia Española de Protección de Datos, deberá poner a su disposición el documento de seguridad.
6. Cada dos años se debe realizar una auditoria que verifique el cumplimiento de las medidas de seguridad.
7. Todas las personas que accedan a los datos deben someterse al secreto profesional.
8. Solo se podrán comunicar datos para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y cesionarios, y habrá que informar al paciente y solicitar su consentimiento.

Por último, se debe tener en cuenta la elevada cuantía de las multas que puede imponer la Agencia Española de Protección de Datos, que oscilan entre los 601,01 euros y los 601.012,10 euros, en función de la calificación de la infracción que se determine, que puede ser leve, grave o muy grave.

A pesar de las obligaciones que impone la LOPD y su normativa de desarrollo, hay que tener en cuenta que la seguridad y todos los principios derivados de la Ley ayudarán a los profesionales a garantizar una correcta gestión de los datos que sin duda son el mayor activo de todas las empresas, más aún si se trata de historias clínicas y datos de salud.

Área de Nuevas Tecnologías
De Lorenzo Abogados
ant@delorenzoabogados.es

La normativa de protección de datos es de obligado cumplimiento siempre que se recojan y almacenen datos de carácter personal, por este motivo todos los especialistas en oncología médica deberán observar la citada normativa