Derechos del paciente: la confidencialidad de sus datos personales de salud

Santiago Sevilla

Asesor Jurídico del ICOFCV
Abogado, colegiado del ICAV nº 6220

El 25 de mayo entra en vigor el nuevo Reglamento General de Protección de Datos

(*) En breve todos los colegiados recibirán una circular

No hay duda, al menos no debería haberla, sobre el carácter confidencial de los datos de salud de un paciente. Este es uno de sus principales derechos y todo profesional sanitario ha de velar por su cumplimiento. Sin embargo, y con el 25 de mayo en el horizonte, es importante que todos los fisioterapeutas sepan que ese día entra en vigor el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

En España, se entiende que todos estos conceptos son conocidos y aplicados por los profesionales al amparo de la Ley Orgánica de Protección de Datos de Carácter Personal, en vigor en la actualidad. Pero a partir del 25 de mayo habrá que adaptarse también a las nuevas exigencias de dicho Reglamento.

No estamos ante una obligación nueva sino más bien ante una nueva regulación que viene a unificar las distintas normativas que cada Estado Miembro de la UE tenía sobre el tratamiento de los datos personales.

Este nuevo Reglamento no afecta solo a los profesionales sanitarios, pero sí tiene una incidencia especialmente significativa en este sector dado que la nueva norma europea considera los datos de carácter personal que afectan a la salud como **datos especialmente protegidos**, exigiendo garantías reforzadas en su tratamiento, con todo lo que ello implica.

Este artículo no pretende abordar las actuaciones que se deben de llevar a cabo para adaptarse a la nueva normativa europea, una parte excesivamente técnico-jurídica que resultaría engorrosa, pero sí concienciar a los profesionales sanitarios, en especial al colectivo al que nos dirigimos, los fisioterapeutas, sobre el deber de conocer, y aplicar, la regulación del tratamiento de los datos de carácter personal que recaban de sus pacientes en su ejercicio profesional.

Cuando abrimos la Historia Clínica de un paciente, recabamos datos que son necesarios para realizar una buena

anamnesis que nos permita hacer un buen diagnóstico y prestar el mejor servicio asistencial. Esos datos que son tan necesarios afectan al área de intimidad más sensible del paciente. En este sentido, el profesional sanitario, se convierte, permítanme el símil, en el "confesor" del paciente. Y eso es lo que está especialmente protegido: todos aquellos datos de carácter personal que se necesitan obtener del paciente para poder darle una adecuada prestación sanitaria.

Una de las modificaciones más importantes del nuevo Reglamento es lo que podemos definir como "**la exigencia de responsabilidad activa**".

¿Qué significa esto? Pues simple y llanamente que la pelota pasa a estar en el tejado de las clínicas y establecimientos sanitarios, a los que se les exige que adopten las medidas preventivas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que se establecen en la normativa. **El Reglamento entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia** dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar.

El Reglamento prevé una batería completa de medidas dirigidas a la prevención, señalando la no implantación de las mismas como una actuación irresponsable. Es decir, se implanta la **Cultura de la Prevención**. Si el hospital, clínica o profesional sanitario autónomo no ha adoptado las medidas preventivas previstas en el reglamento ya por ello incurre en responsabilidad. La omisión no exime de responsabilidad sino más bien al contrario. Para hacerlo más entendible, podríamos decir que nos encontramos ante una figura similar a los Planes de Prevención.

Todo esto exige una planificación que abarca desde el diseño del Plan de protección de datos a la evaluación de los riesgos. Y por extensión, nos llevará a la adopción de medidas de seguridad, al establecimiento de registros de tratamientos de datos, procedimiento de evaluación de impacto sobre la protección de datos, nombramiento, en su caso, del delegado de protección de datos, establecimiento de canales de notificación de violaciones de la seguridad de los datos, establecimiento de sistemas de certificación, etc.

Evidentemente, no es lo mismo trabajar en un hospital público o privado, en el que es la propia organización sanitaria la que se ocupará de la implementación y adaptación al nuevo Reglamento, que trabajar en una clínica privada o como autónomo, que es la mayoría de los casos en el ejercicio profesional de la fisioterapia, en la que será ésta la que deberá realizar la adaptación por sus propios medios. En este caso, recomendamos ponerse en manos de profesionales que les puedan ayudar a la implementación de los sistemas necesarios para cumplir con el nuevo Reglamento, de obligado cumplimento para toda entidad y/o profesional que presta el servicio sanitario. Como ya he dicho antes, entra en vigor a partir del 25 de mayo de 2018, sin perjuicio de estar cumpliendo ya con la actual normativa.

Cumplir con la normativa en tu clínica a través de 9 pasos

Tras los ejemplos reseñados, y como resumen, para el **cumplimiento de la normativa de protección de datos** en materia sanitaria, los centros han de practicar los siguientes puntos:

1. Los datos recogidos son siempre pertinentes y veraces.
2. El paciente siempre es informado y tiene acceso libre a sus datos.
3. Realizar una evaluación de impacto y mantener un registro de las actividades de tratamiento
4. Nombrar un Delegado de Protección de Datos, si procede
5. Cifrar los datos y guardarlos bajo estrictas medidas de seguridad.
6. Guardar **secreto profesional en todo caso**.
7. En caso de **cesión de datos** a terceras partes se debe firmar un contrato que establezca el uso determinado y definido de los datos cedidos.
8. Facilitar los derechos ARCO respetando los plazos establecidos.
9. Inscripción y actualización de los **ficheros** en la AEPD.
10. Adaptarse antes del 25 de mayo a la nueva normativa Comunitaria.

Siendo consciente que, *a priori*, esto puede parecer un poco complejo, y con el ánimo de que sea más entendible, paso a reseñar un decálogo de la Agencia Española de Protección de Datos dado a conocer en la presentación de los resultados del Plan de inspección sectorial realizado a hospitales público. El decálogo recoge los puntos más relevantes de la normativa de protección de datos orientados al personal sanitario y administrativo de los centros, con el objetivo final de **elevar el nivel de cumplimiento y generar confianza** en las actuaciones de las instituciones sanitarias. Sin duda, unas opciones básicas que pueden aplicarse tanto si se ejerce en hospitales, en clínicas privadas o como autónomo.

DECÁLOGO

1. Trata los datos de los pacientes como quieras que traten los tuyos.
2. ¿Estás seguro que quieres acceder a esta Historia Clínica? Piénsalo. Solo debes acceder si es necesario para los fines de tu trabajo.
3. Si estamos ante un sistema de Historia Clínica Electrónica, recuerda: tus accesos a la documentación clínica quedan registrados en el sistema. Se sabe en qué momento y a qué información has accedido. Los accesos son auditados posteriormente.
4. Evitar informar a terceros sobre la salud de tus pacientes, salvo que estos lo hayan consentido o tengas una justificación lícita.
5. Cuando salgas del despacho, asegúrate de cerrar la sesión abierta en tu ordenador. No facilites a nadie tu clave y contraseña; si necesitas un acceso urgente, contacta con el departamento de informática.
6. No envíes información con datos de salud por correo electrónico o por cualquier red pública o inalámbrica de comunicación electrónica; si fuera imprescindible, no olvides cifrar los datos.
7. No tires documentos con datos personales a la papelera; destrúyelos tú mismo o sigue el procedimiento implantado en tu centro.
8. Cuando termines de pasar consulta cierra con llave los armarios y archivadores que contengan documentación clínica.
9. No dejes las historias clínicas a la vista sin su supervisión.
10. No crees tu propia cuenta de ficheros con datos personales de pacientes; consulta siempre antes con el departamento de informática.

De la teoría a la práctica: multas y condenas

Al hilo de los principios abordados, conviene dejar constancia que, tras las multas impuestas recientemente por la Agencia Española de Protección de Datos (AEPD) a *WhatsApp* y *Facebook* por compartir la app de mensajería datos de sus clientes con Facebook sin comunicárselo de forma clara al usuario ni darle opción a ello, cualquier comunicación al paciente de datos de carácter personal vía WhatsApp por parte de la clínica, puede llevar a que se impongan sanciones severas al profesional sanitario o centro que utilice esa vía de comunicación con su paciente sin el expreso consentimiento del mismo y sin informarle de la cesión de datos que WhatsApp hace a Facebook u otras plataformas. Apliquemos aquí el punto 6 del decálogo reseñado:

Punto 6: "No envíes información con datos de salud por correo electrónico o por cualquier red pública o inalámbrica de comunicación electrónica; si fuera imprescindible, no olvides cifrar los datos"

Las consecuencias de no observar estos principios pueden ir más allá de las meras sanciones administrativas, así, recientemente, un juzgado de lo Penal de Pamplona ha condenado a una enfermera a un año de prisión y a seis de inhabilitación absoluta por haber accedido ilegalmente durante dos años al historial clínico de una compañera de trabajo, con la que le unía una enemistad manifiesta. Se le condena a pagar también una multa de 1.440 euros por el delito continuado de revelación de secretos, con la condena, en vía de responsabilidad civil, de indemnizar en 120.000 euros para reparar los daños morales ocasionados a la otra mujer y a su entorno familiar más cercano. Observemos lo que nos dice el punto 2 del decálogo:

Punto 2: "¿Estás seguro que quieres acceder a esta Historia Clínica? Piénsalo. Solo debes acceder si es necesario para los fines de tu trabajo"

Más casos reales: sanción a un médico de Gijón. Fue a causa de arrojar a la vía pública envases de biopsias con datos personales. La AEPD le impuso una multa de 60.101 euros ya que cometió una infracción tipificada como muy grave por la LOPD. Aquí aplicaría el punto 7 del decálogo:

Punto 7: "No tires documentos con datos personales a la papelera; destrúyelos tú mismo o sigue el procedimiento implantado en tu centro"

Otros casos de interés. La AEPD abrió un expediente a un Hospital de Inca por infracción tras filtrar datos personales de pacientes. Asimismo, un Centro Médico de Cartagena fue sancionado por la Agencia con la cifra de 6.000 € por hacer uso de los datos personales de un cliente de la empresa con la cual se había fusionado. La AEPD también denunció a Sanidad, en concreto, un hospital de Cuenca fue apercibido por ceder datos personales e historiales médicos de los pacientes a una clínica privada, sin cifrar la información, pese a tratarse de datos especialmente protegidos, la multa ascendió a un total de 40.001 €. En los tres casos, punto 4 de decálogo:

Punto 4: "Evitar informar a terceros sobre la salud de tus pacientes, salvo que estos lo hayan consentido o tengas una justificación lícita"

Para finalizar, subrayar que el cumplimiento de la normativa sobre tratamiento de datos de carácter personal no es negociable. Como tampoco lo es la fecha del 25 de mayo de 2018 en la que habrá que estar adaptado al Reglamento General de Protección de Datos.