Protección de Datos: una obligación ineludible para sanitarios

Manuel Gil Verdú

Colegiado 7415 del ICAV (Col. Abogados de Valencia)
Director de Prodat Valencia - Consultoría en materia de protección de datos personales del ICOFCV

En la práctica sanitaria, cada fisioterapeuta maneja a diario una enorme cantidad de información personal y clínica de sus pacientes. Son datos especialmente sensibles que merecen -y exigen- el máximo nivel de protección. No se trata solo de cumplir una formalidad legal, sino de garantizar la **confianza** y el **derecho fundamental a la privacidad** de cada persona que entra en la consulta.

A continuación, detallaré **aspectos clave a tener en cuenta.**

Cumplir la normativa: una obligación legal y ética

El Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) establecen las normas que todos debemos cumplir.

El derecho a la protección de datos permite a cada persona tener control sobre su información: quién la trata, con qué finalidad y durante cuánto tiempo.

Es un derecho fundamental que permite a la persona tener control sobre sus datos personales, decidiendo quién puede acceder a ellos y con qué fines. Por eso, todo fisioterapeuta debe cumplir la normativa de protección de datos personales, tanto si trabaja como autónomo como si dirige una clínica o empresa. En el desempeño de su actividad diaria, recaba información personal y trata información personal de pacientes y, en su caso, de empleados, colaboradores y proveedores.

Esto implica, entre otras obligaciones:

- Contar con una **base jurídica** que legitime el tratamiento (generalmente, el consentimiento del paciente).
- **Informar adecuadamente** sobre qué datos se recogen, con qué finalidad y quién los gestiona.
- Adoptar **medidas de seguridad técnicas y organizativas** que garanticen la confidencialidad, integridad y disponibilidad de los datos -muy importante-.
- **Garantizar y atender los derechos** de los pacientes (acceso, rectificación, supresión, limitación, portabilidad y oposición).

Consentimiento informado y consentimiento de datos: no son lo mismo

Un error frecuente es confundir ambos conceptos. De hecho, la Agencia Española de Protección de Datos (AEPD) recomienda separarlos en documentos distintos:

- El **consentimiento para el tratamiento de datos personales** (art. 6.1.a del RGPD) autoriza al fisioterapeuta a recopilar y usar los datos del paciente.
- El **consentimiento informado sanitario** (Ley 41/2002, de Autonomía del Paciente) se refiere a la aceptación de un procedimiento clínico o terapéutico.

Además, el consentimiento de datos relativos a la salud debe ser explícito y por escrito, pues se trata de datos sensibles, especialmente protegidos y que, tras la publicación del RGPD, son considerados una categoría especial de datos personales, por lo que exigen un mayor nivel de protección.

El autónomo debe informar a los interesados sobre: datos identificativos del responsable del tratamiento y, en su caso, del encargado del tratamiento y el DPD; tipos de datos que se recogerá; finalidad del tratamiento; base legitimadora del tratamiento; (si los datos serán cedidos a terceros; si se efectuarán transferencias internacionales de datos; plazo de conservación de los datos; y cómo ejercer los derechos ARCO y el derecho a reclamar ante la AEPD.

Cómo aplicar la protección de datos en tu día a día profesional

El cumplimiento de la normativa también implica una gestión activa y responsable de la información que se maneja en la práctica diaria. Cada fisioterapeuta, ya sea autónomo o parte de una clínica, debe asegurarse de que los procedimientos internos, la documentación y las herramientas tecnológicas estén alineados con las exigencias legales. En este sentido, existen una serie de elementos esenciales que conviene revisar periódicamente para garantizar la seguridad y confidencialidad de los datos de los pacientes:

- **Historia clínica:** el fisioterapeuta tiene la obligación de elaborarla, custodiarla e implantar medidas de seguridad que eviten su extravío o el acceso por terceros. Puede conservarse durante todo el tiempo en que se preste asistencia sanitaria y, como mínimo, cinco años desde la fecha de alta del proceso asistencial. Puede mantenerse más tiempo si se usa con fines estadísticos o de investigación.

- **Contratos con proveedores:** si el profesional o clínica contrata un servicio que suponga el acceso a datos personales (software, gestoría, almacenamiento en la nube, etc.), es obligatorio firmar un contrato de encargo de tratamiento que detalle las responsabilidades y medidas de seguridad.

- **Registro de Actividades de Tratamiento (RAT)**: los profesionales deben documentar qué datos se tratan, con qué finalidad y qué medidas de seguridad se aplican.

- **Medidas de seguridad:** contraseñas robustas, copias de seguridad cifradas, antivirus actualizados, control de accesos, auditorías periódicas y revisión de usuarios inactivos, entre otras.

Si tienes clínica propia...

Cuando el fisioterapeuta gestiona una clínica o centro sanitario, las obligaciones en materia de protección de datos se amplían. En este contexto, los centros sanitarios deben atender, entre otros, los siguientes requisitos adicionales:

- **Cartelería informativa visible** sobre protección de datos y videovigilancia (si la hubiera).

- **Política de privacidad y hojas informativas** en salas de tratamiento.

- **Delegado de Protección de Datos (DPD):** obligatorio si el centro realiza tratamientos de datos a gran escala o de forma sistemática, salvo que el profesional ejerza su actividad a título individual.

Situaciones de riesgo más habituales

El cumplimiento no se limita a la teoría. Existen riesgos reales que pueden provocar brechas de seguridad o sanciones si no se gestionan adecuadamente.

- **Filtraciones o descuidos**: por ejemplo, si un tercero que accede accidentalmente a datos clínicos al ver un mensaje en el móvil del fisioterapeuta con información de un paciente.
- **Redes sociales:** para publicar imágenes o vídeos de pacientes debe existir consentimiento expreso, generalmente por escrito, de forma que el profesional pueda probar fehacientemente que obtuvo el consentimiento del paciente para la captación y difusión. El documento debe indicar la finalidad (divulgación o promoción) y el la red social donde se publicará.
- **Mensajería y WhatsApp**: si se usan para comunicarse con pacientes, debe existir consentimiento y aplicarse precauciones: evitar enviar información sensible, mantener el dispositivo protegido y no compartir mensajes.
- **Grabaciones: el artículo 7 de la Ley 41/2002** prohíbe grabar audio o vídeo dentro de las áreas asistenciales sin el consentimiento expreso del paciente.

Qué hacer ante una brecha de seguridad

Si se produce un incidente de seguridad que pueda exponer los datos de los pacientes (por ejemplo, una pérdida de historiales, un robo de dispositivo o un acceso indebido), el profesional debe **notificarlo a la AEPD y, en su caso, a los afectados en un plazo máximo de 72 horas** desde que tenga constancia del hecho. La notificación debe incluir una descripción del incidente y las medidas correctoras adoptadas.

En el caso de datos de salud, esta obligación cobra especial importancia porque si los datos robados o filtrados no estaban debidamente cifrados, su conocimiento por parte de terceros no autorizados puede poner en riesgo los derechos fundamentales de los interesados.

Cámaras de videovigilancia: dónde sí y dónde no

Las cámaras de videovigilancia pueden instalarse con fines de seguridad, siempre que se informe de su instalación mediante un cartel informativo visible.

El paciente puede solicitar información sobre quien es el responsable de la instalación, de las finalidades de las cámaras, tiempo en el que se mantienen las grabaciones, ejercer sus derechos.

En cuanto a su ubicación, suelen colocarse en accesos, pasillos, o zona comunes, pero **nunca dentro de las salas de tratamiento o consulta**, donde se vulneraría la intimidad de los pacientes.

Para finalizar, subrayar que los autónomos, trabajen solos y/o gestionen una clínica, que no cumplan con sus obligaciones de protección de datos están expuestos a recibir sanciones de la AEPD. Pero más allá de evitarlas, cumplir con la normativa es una forma de profesionalizar el trabajo del fisioterapeuta y reforzar la confianza de los pacientes.