

— GUÍA GRATUITA · MEDICINA ESTÉTICA

¿Tu clínica aplica bien *la Ley de IA y el RGPD?*

Autodiagnóstico en 3 reglas: qué revisar, cómo puntuarte y qué hacer en los próximos 30 días.

3 reglas

16 puntos de control

Plan de 30 días



Qué cambió *el 2 de agosto de 2026*

Desde esa fecha rigen obligaciones de **gobernanza y transparencia** de la Ley Europea de IA en el ámbito médico. Si tu clínica usa IA para atender, agendar, hacer seguimiento o gestionar datos de pacientes, esta guía te ayuda a comprobar tres cosas básicas.

1

El médico decide

La IA asiste. La responsabilidad final sigue siendo de un profesional.

2

Informa al paciente

Debe saber cuándo la IA tiene un papel relevante en su atención.

3

Protege los datos

Los datos de pacientes no van a cualquier herramienta de IA.

Cómo usar esta guía

- Reúne a quien gestione la dirección, la recepción y la parte médica. Son 15 minutos.
- En cada punto marca una opción: **Sí** (lo cumplimos y podemos demostrarlo), **No** o **No lo sé**.
- Si no lo sabes, cuenta como **No**: lo que no puedes demostrar es lo primero que hay que revisar.
- Al final suma tus “No” y consulta el resultado en la última página.

☐ Sí ☐ No ☐ No lo sé

Por qué importa más allá de la ley

Quien automatiza sin estas bases no ahorra tiempo: **acumula riesgo**. Automatizar bien es automatizar conforme a la ley y al RGPD, con un proceso que puedas explicar a tus pacientes y a una inspección.

1

El médico *sigue siendo el responsable final*

Idea clave: la IA asiste, no decide. Cualquier decisión clínica pasa por un profesional identificado.

PUNTO DE CONTROL	SÍ	NO	NO SÉ
1.1 Hay un profesional sanitario identificado como responsable final de cada decisión clínica.	☐	☐	☐
1.2 La IA no emite diagnósticos, indicaciones ni pautas de tratamiento sin validación de un profesional.	☐	☐	☐
1.3 Las respuestas automáticas se limitan a información general y logística (horarios, citas); lo clínico se deriva a una persona.	☐	☐	☐
1.4 Existe un procedimiento escrito para que el equipo corrija o anule lo que haga la IA.	☐	☐	☐
1.5 El equipo sabe qué puede y qué no puede hacer la IA en la clínica.	☐	☐	☐

2

Informa *al paciente*

Idea clave: el paciente debe saber cuándo la IA tiene un papel relevante en su atención, y poder hablar con una persona.

PUNTO DE CONTROL	SÍ	NO	NO SÉ
2.1 El paciente sabe que habla con un asistente de IA: aviso visible al inicio de la conversación.	☐	☐	☐
2.2 Puede pedir hablar con una persona en cualquier momento.	☐	☐	☐
2.3 La información de privacidad que recibe el paciente menciona el uso de IA.	☐	☐	☐
2.4 El aviso aparece en todos los canales: WhatsApp, web, llamadas automáticas y correo.	☐	☐	☐
2.5 Queda constancia de cuándo y cómo se informó al paciente.	☐	☐	☐

3

Protege los datos *de tus pacientes*

Idea clave: no metas datos de pacientes en una IA generativa sin aprobación. Subir historias clínicas o fotos a un ChatGPT de consumo puede ser una brecha de RGPD.

PUNTO DE CONTROL	SÍ	NO	NO SÉ
3.1 Nadie del equipo pega datos de pacientes (nombres, historias, fotos) en herramientas de IA generativa de consumo.	☐	☐	☐
3.2 Las herramientas de IA que tocan datos de pacientes están aprobadas por la dirección.	☐	☐	☐
3.3 Hay contrato con cada proveedor que trata datos, con cláusula de no entrenamiento con vuestros datos.	☐	☐	☐
3.4 Las fotos de antes y después se tratan como datos especialmente protegidos, con consentimiento específico del paciente.	☐	☐	☐
3.5 Sabéis dónde se almacenan los datos y quién tiene acceso a ellos.	☐	☐	☐
3.6 Hay un registro actualizado de las herramientas de IA que se usan en la clínica.	☐	☐	☐

Lo correcto con las fotos de pacientes

- **Contrato empresarial** con el proveedor (no cuentas personales de consumo).
- **Cláusula de no entrenamiento:** lo que subes no sirve para entrenar sus modelos.
- **Consentimiento del paciente** para ese uso concreto.

Recuerda: hacerlo bien cuesta menos que hacerlo mal una sola vez. Una brecha con datos de pacientes cuesta confianza, reputación y posibles sanciones.

Cuenta tus “No” y “No lo sé”

Suma las respuestas “No” y “No lo sé” de los 16 puntos. Es una referencia orientativa para priorizar, no una auditoría legal.

0 – 2
Buen punto de partida

Mantén la revisión cada trimestre y documenta cómo lo demuestras.

3 – 7
Hay huecos que cerrar

Prioriza la regla donde más “No” sumes. Empieza por la 3 si hay datos de pacientes.

8 – 16
Prioridad alta

Pausa los usos de IA con datos de pacientes hasta tener aprobación, contrato y aviso.

Plan de 30 días

Semana 1	Inventario. Lista qué herramientas de IA se usan, quién las usa y con qué datos (punto 3.6).
Semana 2	Transparencia. Añade el aviso de IA en todos los canales y actualiza la información de privacidad (reglas 2.1 a 2.5).
Semana 3	Datos. Revisa contratos con proveedores, cláusula de no entrenamiento y consentimientos de fotos (3.2 a 3.5).
Semana 4	Equipo. Forma al equipo en qué puede y qué no puede hacer la IA y documenta el procedimiento de corrección (regla 1).

2 ago 2026

Obligaciones de gobernanza y transparencia.

Dic 2027

Sistemas de alto riesgo.

Ago 2028

Dispositivos médicos.

Guárdala y *sígueme*

Cada semana, una pieza nueva sobre automatización en clínicas de medicina estética: @fidelitia.tech

FIDELITIA

Aviso: documento informativo y orientativo; no constituye asesoramiento jurídico. Revisa tu caso con tu delegado de protección de datos o con un abogado especializado. Fuente de las fechas y obligaciones: Médicos y Pacientes (OMC), “La Ley Europea de IA ya cambia la práctica médica: qué deben hacer los médicos desde agosto de 2026” (medicosypacientes.com).