iamática

CHECKLIST · DATOS Y RGPD

10 preguntas para cualquier proveedor de IA

Antes de que conteste una sola llamada de tus pacientes. Si no te responde a las 10 por escrito, no lo instales.

> **Por qué importa.** Lo que un paciente cuenta por teléfono suele incluir datos de salud, una categoría especial según el artículo 9 del RGPD. Y la responsable del tratamiento sigue siendo tu clínica, aunque el sistema sea de otro.

1 ¿Dónde están los servidores? ¿Dentro de la UE?

Lo que esperas: nombre de cada proveedor y la región donde se guardan los datos.

Lo que te ha respondido:

2 ¿Hay transferencias fuera del Espacio Económico Europeo? ¿Con qué garantías?

Lo que esperas: si las hay, con decisión de adecuación o cláusulas contractuales tipo (arts. 44–46 RGPD).

Lo que te ha respondido:

3 ¿Firmamos un contrato de encargado del tratamiento?

Lo que esperas: sí, por escrito y antes de empezar, con el contenido del art. 28 RGPD.

Lo que te ha respondido:

4 ¿Qué subencargados usas: voz, inteligencia artificial, telefonía?

Lo que esperas: una lista con nombres y el compromiso de avisarte antes de cambiarla (art. 28.2).

Lo que te ha respondido:

5 ¿Se graban las llamadas? ¿Quién puede escucharlas?

Lo que esperas: qué se graba o transcribe, quién accede y cómo se avisa al paciente al empezar.

Lo que te ha respondido:

Señales de alarma

- [ ] «Eso no hace falta, los datos son anónimos.» La voz y el teléfono del paciente no lo son.
- [ ] No hay contrato de encargado o te lo mandan «más adelante».
- [ ] No sabe decirte dónde están los servidores.

iamática

CHECKLIST · DATOS Y RGPD

Las 5 que más se olvidan

Son las que marcan la diferencia entre un proveedor serio y uno que improvisa.

6 **¿Cuánto tiempo se guardan los datos y cómo se borran?**

Lo que esperas: un plazo concreto para grabaciones y transcripciones, y borrado automático al cumplirse.

Lo que te ha respondido:

7 **¿Se usan los datos de mis pacientes para entrenar modelos?**

Lo que esperas: no, y que lo diga el contrato.

Lo que te ha respondido:

8 **¿El agente avisa al paciente de que habla con una IA?**

Lo que esperas: sí, al empezar la llamada. Es obligatorio desde el 2 de agosto de 2026 (art. 50.1 del Reglamento de IA).

Lo que te ha respondido:

9 **¿Qué pasa con los datos si dejo el servicio?**

Lo que esperas: te los devuelve o los borra, a tu elección, y lo certifica (art. 28.3.g RGPD).

Lo que te ha respondido:

10 **¿Qué medidas de seguridad tienes y qué haces si hay una brecha?**

Lo que esperas: cifrado y control de accesos, y aviso a tu clínica sin demora para que puedas notificar a la AEPD en 72 horas (arts. 32 y 33).

Lo que te ha respondido:

> Esto es información general, no asesoramiento legal. Revísalo con tu delegado de protección de datos o tu asesor, y pregúntale si tu clínica necesita una evaluación de impacto (art. 35 RGPD).

Nosotros respondemos a las 10 por escrito.
Y te las enseñamos en la auditoría gratis, antes de instalar nada.

iamatica.com/#auditoria