

Checklist RGPD para clínicas dentales

Una lista de verificación práctica para revisar los puntos de protección de datos más habituales en el día a día de una clínica dental. Márcalos según los vayas repasando.

Consentimiento informado

- ☐ Existe un modelo de consentimiento informado por tipo de tratamiento, firmado antes de empezar.
- ☐ El paciente puede revocar el consentimiento en cualquier momento y queda constancia de ello.
- ☐ Los consentimientos se guardan asociados a la historia clínica del paciente, no sueltos.

Historia clínica

- ☐ El acceso a las historias clínicas está limitado al personal que las necesita para su trabajo.
- ☐ Los datos de salud se almacenan cifrados, tanto en reposo como en tránsito.
- ☐ Existe un plazo de conservación definido y se revisa periódicamente qué historias han caducado.

Encargados de tratamiento

- ☐ Hay un contrato de encargado de tratamiento firmado con cada proveedor externo que trata datos de pacientes en tu nombre (software, laboratorio, gestoría, mensajería).
- ☐ Se ha comprobado que esos proveedores ofrecen garantías suficientes de seguridad.

Derechos ARCO-POL

- ☐ Existe un procedimiento claro para atender solicitudes de acceso, rectificación, cancelación, oposición, portabilidad y limitación del tratamiento.
- ☐ Las solicitudes se responden dentro del plazo legal (un mes, ampliable a tres).

Registro de actividades de tratamiento

- ☐ La clínica mantiene un registro actualizado de qué datos trata, con qué finalidad y durante cuánto tiempo.

Medidas de seguridad

- ☐ Cada usuario del software tiene su propio acceso, con contraseña individual — nadie comparte cuenta.
- ☐ Hay copias de seguridad periódicas y se ha comprobado alguna vez que se pueden restaurar.
- ☐ El acceso a los sistemas se revoca en cuanto alguien deja de trabajar en la clínica.

Notificación de brechas de seguridad

[] Existe un procedimiento para detectar y notificar una brecha de seguridad a la AEPD en menos de 72 horas si procede.

Delegado de Protección de Datos (DPO)

[] Se ha valorado si la clínica está obligada a designar un DPO (tratamiento a gran escala de datos de salud es uno de los supuestos habituales en el sector sanitario).

Auditoría de accesos

[] El software de gestión registra quién accede a cada historia clínica y cuándo, de forma que se pueda auditar ante una incidencia o una inspección.

Guía orientativa, no sustituye asesoramiento legal — cortesía de NuvaClin (nuvaclin.es).