MEDAI · TOOLDATA SPA

Plantilla de Evaluación de Impacto (EIPD)

Para el despliegue de MedAI — conforme a la Ley 21.719

Activo de confianza · MedAI en pre-lanzamiento · julio de 2026

Plantilla para el despliegue de MedAI — Ley N° 21.719 (Chile)

⚠ **PLANTILLA — NO ES ASESORÍA LEGAL.** La EIPD es una obligación del **Responsable** (la institución de salud) cuando trata datos sensibles a gran escala o en tratamientos de alto riesgo. Esta plantilla es un insumo que MedAI/Tooldata aporta para acelerarla; **debe ser completada, validada y aprobada por el Responsable** (con su DPO/asesoría legal) y ajustada al texto vigente de la Ley N° 21.719 y a las guías de la Agencia de Protección de Datos Personales. Los campos […] deben completarse.

0. Identificación

- **Responsable del tratamiento:** [institución de salud]
- **Proyecto:** Despliegue de MedAI — [módulo: lenguaje clínico / imagenología / ambos]
- **DPO / responsable de la EIPD:** [•]
- **Fecha / versión:** [•]
- **Modalidad de despliegue:** [on-premise / VPC privada / híbrido]

1. Necesidad de la EIPD

Marcar los criterios que apliquen (justifican realizar la EIPD):

- ☐ Tratamiento de **datos sensibles de salud** a gran escala.
- ☐ Uso de tecnologías de **inteligencia artificial** sobre datos personales.
- ☐ Tratamiento que puede generar un **alto riesgo** para los derechos de los titulares.
- ☐ Observación o evaluación sistemática de personas.

2. Descripción sistemática del tratamiento

- **Finalidad:** apoyo a la documentación clínica (epicrisis, resúmenes), codificación CIE-10 y/o apoyo a la lectura de imágenes, con **validación y firma de un profesional** (human-in-the-loop).
- **Flujo de datos:** [origen (HIS/EMR/PACS) → MedAI (en infraestructura del Responsable) → borrador → revisión profesional → registro en la ficha/sistema]. Describir si hay alguna salida de datos fuera de la infraestructura del Responsable (en on-premise/VPC, **no la hay**).
- **Categorías de datos:** identificación; **datos de salud (sensibles)**; imágenes (si aplica); registros de auditoría.
- **Categorías de titulares:** pacientes; profesionales de salud.
- **Volumen estimado:** [•] (p. ej. egresos/mes, estudios/mes).
- **Encargado:** Tooldata SpA (ver DPA). **Subencargados:** ver Anexo III del DPA.
- **Plazo de conservación:** [según ficha clínica — referencialmente 15 años — y políticas internas].

3. Base de legitimación y proporcionalidad

- **Base de legitimación:** [excepción de tratamiento necesario para la salud por profesionales sujetos a secreto / consentimiento explícito / otra]. Justificar.
- **Necesidad y minimización:** se tratan solo los datos necesarios para la finalidad; describir medidas de minimización y por qué la IA es proporcionada al objetivo.
- **Información a los titulares:** [cómo se informa a pacientes/profesionales].

4. Identificación y evaluación de riesgos

Para cada riesgo, estimar **probabilidad** e **impacto** (Bajo/Medio/Alto) y el nivel de riesgo inherente.

#	Riesgo para los derechos de los titulares	Prob.	Impacto	Riesgo inherente
R1	Acceso no autorizado a datos de salud	[ ]	Alto	[ ]
R2	Vulneración/brecha de seguridad con exfiltración	[ ]	Alto	[ ]
R3	Uso de datos para fines distintos (p. ej. entrenamiento)	Baja	Alto	[ ]
R4	Reidentificación a partir de datos tratados	[ ]	[ ]	[ ]
R5	Error en el borrador asistido por IA con impacto clínico	[ ]	Alto	[ ]
R6	Falta de trazabilidad/autoría de las salidas	[ ]	Medio	[ ]
R7	Transferencia internacional sin garantías	Baja	Alto	[ ]
R8	Conservación más allá de lo necesario	[ ]	Medio	[ ]

5. Medidas de mitigación

Riesgo	Medidas (MedAI + organizativas del Responsable)	Riesgo residual
R1	Control de acceso por rol, SSO (SAML/OIDC), principio de necesidad de conocer	[ ]
R2	Cifrado en tránsito/reposo, segregación, registros de auditoría, plan de respuesta a incidentes	[ ]
R3	Política contractual de **no entrenamiento** con datos del cliente; despliegue on-premise/VPC	[ ]

Riesgo	Medidas (MedAI + organizativas del Responsable)	Riesgo residual
R4	Minimización, enmascaramiento/ anonimización donde aplique	[ ]
R5	**Human-in-the-loop**: validación y firma profesional obligatoria; el borrador no es diagnóstico	[ ]
R6	Trazabilidad, versionado y registro de autor/validador en cada salida	[ ]
R7	Datos clínicos no salen de la infraestructura (on-premise/VPC); DPA y garantías para subencargados	[ ]
R8	Retención configurable y borrado/ destrucción certificada al término	[ ]

6. Riesgo residual y decisión

- **Riesgo residual global:** [Bajo / Medio / Alto].
- **¿Requiere consulta previa a la Agencia?** [Sí / No] — justificar.
- **Decisión:** [Aprobar / Aprobar con condiciones / No aprobar].

7. Consulta y aprobación

- **Consulta a interesados / áreas (TI, clínica, legal, DPO):** [resumen].
- **Aprobado por:** [DPO / responsable] — Fecha: [•].
- **Revisión programada:** [periodicidad o hito que la gatilla, p. ej. cambio de alcance].

8. Plan de acción

Acción	Responsable	Plazo	Estado
[•]	[•]	[•]	[•]

Plantilla aportada por Tooldata (MedAI) como insumo. La titularidad y aprobación de la EIPD corresponden al Responsable. Última actualización: junio de 2026. Sujeta a revisión legal.