MEDAI · TOOLDATA SPA

Matriz de responsabilidades — Ley 21.719

Reparto responsable / encargado en el tratamiento de datos de salud

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

Reparto de obligaciones de protección de datos en el despliegue de MedAI

Documento modelo / orientativo preparado por Tooldata SpA (MedAI) para el oficial de cumplimiento o DPO de la institución de salud. Destila los Anexos y cláusulas del Contrato de Encargo (DPA) modelo conforme a la Ley N° 21.719. No constituye asesoría legal.

1. Por qué existe la distinción Responsable / Encargado

La **Ley N° 21.719** sobre protección de datos personales entra en **plena vigencia el 1 de diciembre de 2026** y trata los **datos de salud como datos personales sensibles**, sujetos a un régimen reforzado. La ley distingue dos roles con obligaciones y responsabilidades distintas:

- **Responsable del tratamiento — la clínica u hospital.** Es quien **decide los fines y los medios** del tratamiento: para qué se tratan los datos de sus pacientes, con qué base de legitimación y bajo qué condiciones. La **responsabilidad legal frente al titular y frente a la Agencia de Protección de Datos Personales recae en el Responsable.**
- **Encargado del tratamiento — Tooldata SpA (MedAI).** Trata datos **por cuenta y según las instrucciones documentadas del Responsable**, exclusivamente para prestar el servicio. No define fines propios ni usa los datos para finalidades distintas (por ejemplo, entrenar modelos de uso general).

Esta relación se formaliza en un **contrato de encargo (DPA)**, exigido por la ley cuando un proveedor trata datos por cuenta de la institución. En consecuencia, la regla de lectura de toda esta matriz es:

> **La obligación legal ante el titular y la Agencia es del Responsable; el Encargado presta apoyo, herramientas, información y trazabilidad para que el Responsable pueda cumplirla.**

El modo de despliegue refuerza este reparto. MedAI se despliega **on-premise** o en **VPC privada** del Responsable, de modo que los datos clínicos permanecen **bajo el control del Responsable**. En **on-premise**, además, **los datos no salen de la infraestructura ni de la red del Responsable** (con capacidad de operación air-gapped). El acceso del Encargado se limita a las actividades de soporte, mantenimiento y actualización expresamente autorizadas.

Cómo leer la matriz

Marca	Significado
R	**Responsable de ejecutar** la obligación; sobre esta parte recae el deber legal ante el titular y la Agencia.
A	**Apoya**: aporta herramientas, información, asistencia técnica o trazabilidad, bajo instrucción del Responsable.

Marca	Significado
—	No aplica a esa parte.

En seguridad, registro y subencargados ambas partes ejecutan tareas propias de su rol, por lo que aparece **R** en ambas columnas.

2. Matriz de responsabilidades

Obligación / actividad (Ley 21.719)	Responsable (clínica / hospital)	Encargado (MedAI / Tooldata)	Notas
Base de licitud y consentimiento	**R** — determina y acredita la base de legitimación, incluido el régimen de datos sensibles de salud	**—** — no fija la base; trata solo según instrucciones documentadas	DPA cl. 3 y 12. El Encargado advierte al Responsable si, a su juicio, una instrucción infringe la ley (cl. 3.2).
Información a los titulares	**R** — deber de informar a pacientes y profesionales	**A** — aporta la descripción del tratamiento (Anexo I) y de la lógica de MedAI	Insumo para los avisos de privacidad. El contacto con el titular es siempre del Responsable.
Atención de derechos (acceso, rectificación, cancelación / supresión, oposición, portabilidad, bloqueo)	**R** — recibe y resuelve las solicitudes frente al titular	**A** — asiste con medidas técnicas; si el titular lo contacta, lo deriva al Responsable sin responder directamente	DPA cl. 7.1. MedAI facilita búsqueda, exportación, rectificación, bloqueo y borrado, con trazabilidad de cada acción.
Evaluación de impacto (EIPD)	**R** — es titular y aprueba la EIPD; decide la consulta previa a la Agencia	**A** — aporta la plantilla EIPD e información de su ámbito	DPA cl. 7.2 + plantilla EIPD. Obligatoria en tratamiento de datos sensibles a gran escala o de alto riesgo.
Medidas de seguridad	**R** — controles organizativos y de su infraestructura (gestión de accesos, personal, entorno on-premise / VPC)	**R** — medidas técnicas del producto (Anexo II): cifrado en tránsito y reposo, control de acceso por rol, SSO, registros de auditoría	Responsabilidad compartida por diseño. DPA cl. 5 y Anexo II. Nivel de seguridad adecuado al riesgo.
Notificación de brechas (a la Agencia y a los titulares)	**R** — notifica a la Agencia y, cuando proceda, a los titulares, dentro del plazo legal	**A** — notifica al Responsable sin dilación indebida, con los datos disponibles de la vulneración	DPA cl. 8. Plazo referencial de 72 h (verificar con la norma vigente).
Registro de actividades de tratamiento	**R** — mantiene su registro en calidad de Responsable	**R** — mantiene su registro de los tratamientos efectuados por cuenta del Responsable	DPA cl. 11.1. Cada parte lleva el registro correspondiente a su rol.
Transferencias internacionales	**R** — decide y autoriza las transferencias y exige garantías adecuadas	**A** — no transfiere sin instrucción; impone garantías equivalentes a subencargados	DPA cl. 9. On-premise: los datos clínicos no salen de la red del Responsable; VPC: permanecen en un entorno dedicado bajo su control. El subencargado de correo (Re-

Obligación / actividad (Ley 21.719)	Responsable (clínica / hospital)	Encargado (MedAI / Tooldata)	Notas
			send, EE.UU.) trata solo notificaciones del formulario del sitio web, no datos clínicos del producto.
Retención y supresión al término	**R** — define la política de retención (referencia: ficha clínica, Ley 20.584) y elige devolución o destrucción	**A** — ejecuta y certifica la devolución o destrucción; ofrece retención configurable	DPA cl. 10. En on-premise / VPC los datos ya están bajo control del Responsable; se retiran software y modelos al término.
Subencargados / subprocesadores	**R** — autoriza la lista (Anexo III) y puede oponerse a cambios por motivos fundados	**R** — contrata con obligaciones equivalentes, informa incorporaciones o sustituciones y responde por sus subencargados	DPA cl. 6 y Anexo III.
Auditoría y trazabilidad	**R** — ejerce el derecho de auditoría y la supervisión del cumplimiento	**A** — facilita auditorías e inspecciones; mantiene trazabilidad, versionado y registro de autoría / validación	DPA cl. 11.2. Cada salida de MedAI queda registrada con autor, validador y versión que la generó.

3. Cómo apoya MedAI cada grupo de obligaciones

El reparto anterior no deja al Responsable solo frente a sus deberes: MedAI está diseñado para **aportar los insumos y controles** que facilitan el cumplimiento.

- **Contrato como base del encargo — DPA modelo.** Sustenta las filas de base de licitud, instrucciones, seguridad, brechas, transferencias, subencargados, retención y auditoría. Define que el tratamiento se realiza **solo según instrucciones documentadas** del Responsable y fija la política de **no uso de los datos del cliente para entrenar modelos de uso general**.
- **Deberes de evaluación — plantilla EIPD.** MedAI entrega una **plantilla de Evaluación de Impacto** con descripción del tratamiento, base de legitimación, matriz de riesgos y medidas de mitigación, como insumo para que el Responsable la complete, valide y apruebe. La **titularidad y la aprobación de la EIPD son del Responsable**.
- **Seguridad por diseño.** Cifrado en tránsito y en reposo, control de acceso por rol, SSO (SAML / OIDC), segregación de datos y actualizaciones controladas y versionadas (incluidas actualizaciones firmadas para entornos air-gapped). El **despliegue on-premise / VPC** mantiene los datos bajo el control del Responsable y reduce la superficie de exposición.
- **Trazabilidad y auditoría.** Registros de auditoría y **versionado de cada salida**, con autoría y validación, para sostener las obligaciones de registro, atención de derechos y auditoría, y para acreditar qué versión del modelo o plantilla generó cada resultado.
- **Atención de derechos y brechas.** Funciones de búsqueda, exportación, rectificación, bloqueo y borrado que asisten al Responsable en la atención de solicitudes; y un flujo de notificación al Responsable **sin dilación indebida** ante una vulneración, para que este cumpla su deber de notificación a la Agencia y a los titulares.

Nota sobre la responsabilidad clínica. Esta matriz cubre la protección de datos (Ley 21.719). La **responsabilidad clínica es distinta y permanece siempre en el profesional de salud**: toda

salida de MedAI es un **borrador de apoyo** que un profesional habilitado revisa, edita, valida y firma (human-in-the-loop). MedAI **no emite diagnóstico autónomo** ni reemplaza el juicio médico.

4. Aviso

Este es un **documento modelo y orientativo**; **no constituye asesoría legal**. Sintetiza el Contrato de Encargo (DPA) y la plantilla EIPD de MedAI y debe leerse junto con ellos. El reparto de responsabilidades **se concreta y adapta en el contrato de servicio** de cada institución, y debe ser **revisado por un abogado habilitado en Chile** y ajustado al texto vigente de la **Ley N° 21.719**, su reglamento y las instrucciones de la **Agencia de Protección de Datos Personales**. Las referencias a plazos (p. ej. 72 horas) y a la normativa aplicable (Ley 20.584 sobre derechos del paciente y ficha clínica; Ley 21.668 sobre interoperabilidad; régimen del ISP para software como dispositivo médico) deben verificarse con la norma vigente al momento de su uso.

Documento modelo preparado por Tooldata SpA (MedAI). Julio de 2026. Sujeto a revisión legal.