MEDAI · TOOLDATA SPA

Cómo evaluar un proveedor de IA médica

Preguntas clave para tu clínica u hospital

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

Guía de evaluación para comités de compras, TI y cumplimiento de prestadores de salud en Chile

La incorporación de inteligencia artificial a la práctica clínica es una decisión de alto impacto y alto riesgo: involucra datos de salud —que la **Ley N° 21.719** trata como datos sensibles con régimen reforzado—, la seguridad del paciente y la responsabilidad profesional. Este documento reúne las preguntas que todo comité debería hacer a cualquier proveedor de IA médica antes de firmar.

Cada pregunta incluye un apartado **«Por qué importa»** (para que la uses aunque estés evaluando a otro proveedor) y un apartado **«Cómo responde MedAI»**, para que veas nuestra postura con transparencia. MedAI es un producto de **Tooldata SpA** y se encuentra en **pre-lanzamiento**: lo que describimos es nuestra **arquitectura de referencia** y nuestro **diseño objetivo**; las cifras técnicas son **referenciales** y se ajustan en cada implementación.

> **Cómo usar este checklist.** Llévalo a la mesa de evaluación y pide respuestas por escrito. Una buena señal es que el proveedor pueda entregarte documentación concreta (contrato de encargo, evaluación de impacto, arquitectura de despliegue, política de datos), no solo afirmaciones comerciales.

1. ¿Dónde viven y se procesan los datos clínicos?

Por qué importa. El punto donde se procesan los datos determina tu exposición legal y de seguridad. Si los datos de tus pacientes se envían a una nube pública o a servidores del proveedor en el extranjero, aumenta la superficie de brecha y se activan reglas de transferencia internacional de la Ley 21.719. La soberanía del dato es la primera línea de defensa.

Cómo responde MedAI. MedAI se despliega **en la infraestructura del cliente**, en dos modalidades:

- **On-premise:** en tu servidor o clúster. Los datos clínicos **no salen de tu red**; la inferencia ocurre localmente y puede operar incluso sin salida a internet (**air-gapped**).
- **Nube privada (VPC):** un entorno dedicado y aislado, en la nube que elijas, **bajo tu control**.

En ambos modos los datos permanecen bajo tu control y no se envían a servicios de terceros. Puedes revisar el detalle en nuestra *Arquitectura de referencia de despliegue*, que documenta el perímetro de datos sin egress.

2. ¿Usan mis datos para entrenar sus modelos o los de terceros?

Por qué importa. Muchos servicios de IA reutilizan los datos que reciben para reentrenar modelos comerciales. Con datos de salud, eso es inaceptable: implica un uso para una finalidad distinta a la clínica, sin base de legitimación, y una pérdida de control sobre información sensible de tus pacientes.

Cómo responde MedAI. No. Categóricamente, los datos clínicos de tu institución **no se usan para entrenar** modelos de inteligencia artificial de uso general ni de terceros, y **no se comparten** con terceros fuera de lo pactado. Esta prohibición no es solo una declaración: es una **cláusula del contrato**

de encargo (DPA) y una medida registrada en la evaluación de impacto. Al procesarse en tu infraestructura (on-premise) o en tu entorno dedicado bajo tu control (VPC), además, no existe el canal técnico hacia servicios externos para esa reutilización.

3. ¿Es apoyo a la decisión clínica o diagnóstico autónomo?

Por qué importa. Un sistema que «decide» por sí solo desplaza la responsabilidad profesional y eleva enormemente el riesgo clínico y legal. La pregunta correcta no es «¿qué tan bueno es el algoritmo?», sino «¿quién revisa, valida y firma cada resultado?». Ese diseño define tanto la seguridad del paciente como el encuadre regulatorio.

Cómo responde MedAI. MedAI es un sistema de **apoyo a la decisión clínica**, con arquitectura **human-in-the-loop**. Toda salida es un **borrador** —una epicrisis, un resumen, una propuesta de codificación CIE-10, un apoyo documental— que entra en una cola de revisión y que un **profesional habilitado revisa, edita, valida y firma** antes de finalizarse. MedAI **no emite diagnósticos autónomos** ni reemplaza el juicio médico; la responsabilidad de la decisión permanece siempre en el profesional.

4. ¿Es un dispositivo médico? ¿Tiene o requiere registro sanitario ante el ISP?

Por qué importa. Chile está incorporando el **software como dispositivo médico (SaMD)** al régimen de control sanitario del **Instituto de Salud Pública (ISP)**. Un proveedor que afirme tener un registro que no existe, o que ignore la pregunta, es una señal de alerta. Necesitas un encuadre honesto y trazable de cómo se clasifica la herramienta y quién asume qué.

Cómo responde MedAI. Somos transparentes: MedAI está diseñado como **herramienta de apoyo a la decisión** con validación y firma profesional, y esa arquitectura human-in-the-loop es la que define su encuadre regulatorio. Dado que el régimen SaMD del ISP está **en incorporación**, **evaluamos el alcance de cada caso de uso con asesoría regulatoria** y acompañamos a la institución en lo que corresponda. No afirmamos registros ni certificaciones que no tengamos.

5. ¿Cómo cumplen la Ley N° 21.719 sobre protección de datos?

Por qué importa. La Ley 21.719 entra en **plena vigencia el 1 de diciembre de 2026** (la Ley 19.628 rige hasta esa fecha) y trata los datos de salud como **datos sensibles** con obligaciones reforzadas. Tu institución será la **responsable** del tratamiento y el proveedor, el **encargado**: la ley exige un contrato de encargo escrito y, para tratamientos sensibles a gran escala, una evaluación de impacto previa. Sin estos insumos, la venta se frena —con razón— en el área legal.

Cómo responde MedAI. Entregamos un **paquete de cumplimiento pensado para Chile**:

- **Contrato de encargo (DPA) modelo** conforme a la Ley 21.719: tratamiento solo según instrucciones documentadas, medidas de seguridad, gestión de subencargados y transferencias, notificación de brechas y devolución o destrucción certificada al término.
- **Plantilla de Evaluación de Impacto (EIPD/DPIA)** con matriz de riesgos y medidas de mitigación, para que tu DPO la complete y apruebe con rapidez.
- **Seguridad por diseño** y **soberanía del dato**: al desplegarse en tu infraestructura, se reduce la superficie de exposición.

> El DPA y la EIPD son documentos **modelo** y no constituyen asesoría legal; deben ser revisados y adaptados por un abogado habilitado en Chile antes de su uso o firma.

6. ¿Cómo se integra con mi HIS/EMR, PACS y RIS?

Por qué importa. Una IA que exige rehacer tus flujos o migrar a una plataforma cerrada genera costo, riesgo y dependencia del proveedor. La integración debe apoyarse en **estándares abiertos** y respetar tu ecosistema actual, incluida la interoperabilidad que promueve la **Ley 21.668**.

Cómo responde MedAI. MedAI se **integra, no reemplaza**. Se conecta a tu stack existente mediante estándares médicos establecidos:

Sistema	Estándar de integración
HIS / EMR (sistemas clínicos)	HL7 v2 y **HL7 FHIR**
PACS / RIS (imagenología)	**DICOM** (C-STORE / C-FIND)
Sistemas propios	APIs REST
Identidad / inicio de sesión	SSO con SAML / OIDC

El objetivo es sumarse a tu flujo de trabajo actual. La conectividad y el mapeo de datos se configuran durante la implementación.

7. ¿Hay trazabilidad y auditoría de cada salida?

Por qué importa. En salud, poder reconstruir *quién* produjo o validó un documento, *con qué versión* del sistema y *cuándo*, es esencial para la auditoría clínica, la investigación de incidentes y la notificación de brechas que exige la Ley 21.719. Sin trazabilidad, no hay rendición de cuentas.

Cómo responde MedAI. La **trazabilidad es un principio de diseño**. Cada salida queda registrada con su **autoría (autor y validador), la versión del modelo y de la plantilla utilizadas y la marca de tiempo**. El orquestador de MedAI mantiene registros de auditoría y versionado de todas las salidas dentro del perímetro del cliente, de modo que siempre sea posible saber qué versión generó cada resultado y quién lo firmó.

8. ¿Qué medidas de seguridad tienen: cifrado, control de acceso, SSO?

Por qué importa. Los controles de seguridad concretos —no las etiquetas— son los que protegen los datos sensibles. Debes exigir cifrado, control de acceso por rol, autenticación federada y principio de mínimo privilegio, y verificar cómo se implementan en tu despliegue.

Cómo responde MedAI. MedAI está **diseñado conforme a controles de seguridad reconocidos** y aplica seguridad por diseño:

- **Cifrado** en tránsito (TLS) y en reposo (AES).
- **Control de acceso por rol (RBAC)** con **SSO (SAML/OIDC)** federado a tu IdP (AD/Entra/Keycloak) y principio de mínimo privilegio.
- **Segregación de entornos**; sin egress en modo air-gapped.
- **Registros de auditoría**, versionado, retención configurable y enmascaramiento/anonimización donde aplique.
- **Respaldos, plan de recuperación y rollback** por versión.

> Sobre certificaciones: somos precisos. MedAI está **diseñado conforme a / alineado con** los controles habituales de gestión de seguridad de la información; una **certificación ISO 27001 está en nuestro roadmap (en diseño)**. No afirmamos certificaciones (ISO 27001, HIPAA, SOC 2) que no tengamos.

9. ¿Qué pasa con mis datos si termino el contrato?

Por qué importa. La reversibilidad evita el bloqueo por dependencia (*vendor lock-in*) y protege la continuidad clínica. Debes saber, antes de firmar, cómo recuperas o conservas tus datos, en qué formatos y con qué garantías de eliminación por parte del proveedor.

Cómo responde MedAI. En un despliegue **on-premise o en tu VPC privada**, los datos clínicos **nunca salieron de tu infraestructura**: ya están bajo tu control, así que no hay que «devolverlos». Al término del contrato, MedAI **deja de operar** en tu entorno y se retiran el software y los modelos; tus datos, registros e informes **permanecen en tus sistemas**. El DPA contempla, además, **devolución**

o destrucción certificada de cualquier dato tratado por cuenta tuya. El detalle de reversibilidad, formatos de exportación y desinstalación queda establecido en el contrato de servicio.

10. Soporte, actualizaciones controladas y responsabilidad legal

Por qué importa. Una actualización silenciosa puede cambiar el comportamiento de un sistema clínico sin que lo apruebes, con impacto en la seguridad del paciente. Necesitas control sobre los cambios, un soporte con niveles definidos y claridad sobre **qué entidad responde legalmente** ante tu institución.

Cómo responde MedAI. Las actualizaciones de modelos y plantillas son **controladas y versionadas**: no hay cambios silenciosos en producción. En despliegues on-premise o air-gapped se entregan como **paquetes firmados** (con verificación de firma antes de aplicar) que tu organización aprueba e instala, con capacidad de **revertir** a la versión anterior. El soporte y los niveles de servicio se definen **por contrato**, según el dimensionamiento y la arquitectura de alta disponibilidad acordados. Legalmente responde una **entidad chilena identificable, Tooldata SpA (RUT 76.963.629-3)**, lo que facilita la jurisdicción y la relación contractual.

11. ¿Cómo validan el desempeño antes de pasar a producción?

Por qué importa. Las métricas de marketing o de otros contextos no predicen el desempeño en *tu* población, con *tus* casos y flujos. La validación debe hacerse con tus propios datos y con criterios de aceptación acordados por escrito, y el sistema debería entrar en producción solo si los cumple.

Cómo responde MedAI. Durante la implementación validamos el desempeño **con tus propios datos y casos**, definiendo **en conjunto las métricas de aceptación** (por ejemplo, concordancia con el criterio del especialista o precisión de codificación). MedAI entra en producción **únicamente cuando cumple los umbrales acordados**, y mantenemos un reporte periódico de desempeño. Los borradores se generan de forma **conservadora**, pensados para no omitir información que el profesional deba revisar; en todos los casos, la salida es un borrador que requiere validación y firma médica. No atribuimos a MedAI un «perfil de detección» ni afirmamos hallazgos automáticos: la lectura definitiva la hace el profesional.

12. ¿Quién está detrás? Equipo y trazabilidad del proveedor

Por qué importa. Confías datos de salud y un proceso clínico a una organización, no solo a un software. Debes poder identificar la **entidad legal**, su jurisdicción, sus responsables y su cadena de proveedores (subencargados), y verificar que la documentación técnica y legal exista y sea coherente.

Cómo responde MedAI. MedAI es un producto de **Tooldata SpA**, sociedad chilena con **RUT 76.963.629-3** y domicilio en Concón, Región de Valparaíso. Ponemos a tu disposición la documentación que permite hacer *due diligence*: **arquitectura de referencia, guía de dimensionamiento, DPA modelo, plantilla EIPD** y política de datos, incluida la lista de **subencargados** con su ubicación y garantías (en el producto on-premise/VPC, los datos clínicos no se transfieren fuera de tu infraestructura). Al estar en **pre-lanzamiento**, somos explícitos sobre qué componentes son diseño objetivo y qué cifras son referenciales, en lugar de exhibir tracción o clientes que aún no corresponden.

En resumen

Un buen proveedor de IA médica debería poder responder estas doce preguntas **por escrito** y respaldarlas con documentos. Como referencia rápida:

#	Pregunta	Respuesta de MedAI
1	¿Dónde se procesan los datos?	On-premise o VPC privada; bajo tu control
2	¿Entrenan con mis datos?	No; prohibido por contrato

#	Pregunta	Respuesta de MedAI
3	¿Apoyo o diagnóstico autónomo?	Apoyo con firma profesional (human-in-the-loop)
4	¿Dispositivo médico / ISP?	Encuadre honesto; SaMD en evaluación con asesoría
5	¿Ley 21.719?	DPA + EIPD + seguridad por diseño
6	¿Integración?	DICOM, HL7/FHIR, REST, SSO; no reemplaza
7	¿Trazabilidad?	Autoría, versión y marca de tiempo por salida
8	¿Seguridad?	Cifrado, RBAC + SSO; ISO 27001 en roadmap
9	¿Fin del contrato?	Reversibilidad; tus datos permanecen contigo
10	¿Soporte y actualizaciones?	Controladas y firmadas; responde Tooldata SpA
11	¿Validación?	Con tus datos y umbrales de aceptación acordados
12	¿Quién está detrás?	Tooldata SpA (Chile), con documentación verificable

Próximos pasos

Si estás evaluando IA médica —a MedAI o a cualquier otro proveedor— te recomendamos pedir estos tres documentos antes de decidir:

1. El **contrato de encargo (DPA)** conforme a la Ley 21.719.
2. La **evaluación de impacto (EIPD/DPIA)** o su plantilla.
3. La **arquitectura de despliegue** y la política de datos.

En MedAI podemos entregarte nuestro **DPA y la plantilla EIPD**, y coordinar una **demostración** adaptada a tu institución. Escríbenos y con gusto avanzamos.

Documento de evaluación para prestadores de salud en Chile. Julio de 2026. MedAI (Tooldata SpA) se encuentra en pre-lanzamiento; la arquitectura descrita corresponde al diseño de referencia y las cifras técnicas son referenciales. El DPA y la EIPD son documentos modelo y no constituyen asesoría legal.