CITIOMED

Política de Protección de Datos Personales de Salud

Tratamiento de datos personales sensibles bajo la LOPDP (Ecuador)

Versión 1.0
Fecha de entrada en vigor: 18 de abril de 2026
Quito — Ecuador

1. Objeto y ámbito de aplicación

La presente Política de Protección de Datos Personales (en adelante, la "Política") establece los principios, controles y garantías que Citiomed aplica al tratamiento de los datos personales sensibles relacionados con la salud de los pacientes atendidos por las clínicas y profesionales de la salud que utilizan la plataforma.

Esta Política complementa la Política de Privacidad general del servicio y se emite en cumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador (en adelante, "LOPDP"), su Reglamento General y demás normativa aplicable.

2. Responsable del tratamiento y Delegado de Protección de Datos

Responsable del tratamiento: Citiomed (nombre comercial), 0603997305001, con domicilio en Quito, Ecuador.

Delegado de Protección de Datos (DPD): Contactable a través del correo info@citiomed.com. El DPD es el punto de contacto para cualquier consulta relacionada con el tratamiento de datos personales y para el ejercicio de los derechos del Titular.

Cuando la clínica o profesional de la salud actúe como Responsable del tratamiento, Citiomed operará como Encargado del tratamiento en virtud del correspondiente Acuerdo de Encargo, y se compromete a tratar los datos conforme a las instrucciones documentadas del Responsable.

3. Clasificación de los datos de salud como sensibles

De conformidad con el artículo 4 de la LOPDP, los datos relativos a la salud son considerados datos personales sensibles, dado que revelan información sobre el estado de salud físico o mental, presente o futuro, de una persona natural, incluida la prestación de servicios de atención sanitaria.

En particular, Citiomed considera dato sensible, entre otros:

- Motivo de consulta médica o especialidad solicitada.
- Antecedentes clínicos compartidos por el paciente con la clínica.
- Información sobre tratamientos, medicación y procedimientos.
- Cualquier dato contenido en los mensajes intercambiados con el asistente conversacional que permita inferir condiciones de salud.

4. Base legal: consentimiento explícito (Art. 26 LOPDP)

El tratamiento de datos personales sensibles de salud se realiza exclusivamente sobre la base del consentimiento expreso, libre, específico, informado e inequívoco del Titular o de su representante legal, otorgado de forma previa al inicio del tratamiento.

El consentimiento se obtiene a través de mecanismos verificables, incluyendo la aceptación explícita en el primer contacto del paciente con el asistente conversacional de WhatsApp Business y, en su caso, en la plataforma web de la clínica.

El Titular podrá revocar su consentimiento en cualquier momento, sin efectos retroactivos, escribiendo a info@citiomed.com o a la clínica tratante. La revocación no afectará la licitud del tratamiento realizado con anterioridad.

5. Principios rectores del tratamiento

Citiomed aplica los siguientes principios al tratamiento de datos de salud:

- **Licitud, lealtad y transparencia:** todo tratamiento se realiza con fundamento legal y de forma transparente para el Titular.
- **Finalidad:** los datos se recopilan con fines determinados, explícitos y legítimos, y no se tratan posteriormente de manera incompatible con dichos fines.
- **Minimización:** únicamente se recopilan los datos estrictamente necesarios para la finalidad declarada.
- **Exactitud:** los datos se mantienen exactos y actualizados; se adoptan medidas razonables para suprimir o rectificar los inexactos.
- **Limitación del plazo de conservación:** los datos se conservan solo durante el tiempo necesario para cumplir la finalidad.
- **Integridad y confidencialidad:** se garantiza la protección frente al tratamiento no autorizado o ilícito y frente a la pérdida, destrucción o daño accidentales.
- **Responsabilidad proactiva:** se documentan las medidas adoptadas para cumplir la LOPDP.

6. Acceso restringido (Arts. 30 a 32 LOPDP)

El acceso a los datos personales de salud está restringido a profesionales de la salud y al personal administrativo bajo su supervisión directa que requiera dicho acceso para el cumplimiento de sus funciones, siempre sujetos al deber de secreto profesional.

Citiomed implementa un modelo de control de acceso basado en roles (RBAC) con los siguientes perfiles y principios:

- Administrador de clínica: acceso al conjunto de datos de la clínica que administra; no puede acceder a datos de otras clínicas.
- Profesional de la salud (médico): acceso únicamente a los datos de los pacientes asignados a su agenda.
- Recepcionista: acceso a los datos estrictamente necesarios para la gestión de turnos y comunicación con pacientes.
- Super Administrador (personal de Citiomed): acceso excepcional con fines de soporte y mantenimiento, sujeto a registro de auditoría, cláusula de confidencialidad y revisión periódica.

Cualquier acceso a los datos por parte del personal de Citiomed queda registrado en bitácoras de auditoría para su revisión posterior.

7. Decisiones automatizadas e intervención humana (Art. 20 LOPDP)

El Titular tiene derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar.

El asistente conversacional de Citiomed utiliza procesamiento automatizado únicamente para tareas operativas (agendamiento, confirmación y recordatorio de citas, respuesta a preguntas frecuentes) y no para emitir diagnósticos, recomendaciones terapéuticas ni decisiones de naturaleza médica. En todo caso, el paciente puede en cualquier momento:

- Solicitar la intervención humana de un profesional de la clínica.
- Expresar su punto de vista e impugnar la decisión automatizada.
- Solicitar una revisión humana de cualquier respuesta recibida del asistente conversacional.

8. Transferencia internacional de datos (Art. 55 LOPDP)

Determinados proveedores de infraestructura y servicios utilizados por Citiomed se encuentran ubicados fuera del Ecuador, incluyendo:

- Supabase Inc. / Amazon Web Services, Inc. (almacenamiento de base de datos y funciones de backend).

- Meta Platforms, Inc. (plataforma de WhatsApp Business).
- OpenAI, OpCo, LLC (procesamiento de texto mediante modelos de lenguaje).

Estas transferencias internacionales se amparan en cláusulas contractuales estándar, compromisos de confidencialidad, cifrado en tránsito y en reposo, así como en el consentimiento informado del Titular, en los términos del artículo 55 de la LOPDP.

Cuando el Titular interactúa con el asistente conversacional, se le informa previamente que el contenido del mensaje podrá ser procesado por un modelo de lenguaje operado por un proveedor ubicado fuera del Ecuador, exclusivamente para generar la respuesta y sin que dicho contenido sea utilizado para entrenar modelos de uso general.

9. Medidas técnicas y organizativas de seguridad

Citiomed aplica, como mínimo, las siguientes medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos de salud:

9.1 Medidas técnicas

- Cifrado en tránsito mediante TLS 1.2 o superior.
- Cifrado en reposo en la base de datos y en los respaldos.
- Separación lógica de datos por tenant (clínica/establecimiento).
- Control de acceso basado en roles (RBAC), con políticas de seguridad a nivel de fila (Row Level Security) cuando aplica.
- Autenticación multifactor para personal administrativo.
- Gestión de secretos y claves mediante bóvedas especializadas.
- Monitoreo de eventos de seguridad y alertas automatizadas.
- Copias de respaldo automatizadas con pruebas periódicas de restauración.

9.2 Medidas organizativas

- Políticas internas de seguridad de la información y gestión de accesos.
- Acuerdos de confidencialidad con todo el personal y proveedores.
- Capacitación periódica en protección de datos y seguridad de la información.
- Procedimientos para la gestión de incidentes y continuidad del servicio.
- Revisión periódica de los controles de acceso y de los registros de auditoría.

10. Evaluación de Impacto en Protección de Datos (EIPD)

Dado que el tratamiento de datos de salud supone un alto riesgo para los derechos y libertades de los Titulares, Citiomed ha realizado una Evaluación de Impacto en Protección de Datos (EIPD) en la que se identifican:

- Los flujos de datos y categorías de datos tratados.
- Las finalidades y base legal del tratamiento.
- Los riesgos para los derechos y libertades de los Titulares, incluyendo accesos no autorizados, transferencias internacionales y uso de modelos de lenguaje.
- Las medidas técnicas y organizativas implementadas para mitigar dichos riesgos.
- Los indicadores de control y el plan de revisión periódica.

La EIPD es revisada cuando se introducen cambios significativos en el servicio y se mantiene a disposición de la autoridad de control cuando sea requerida.

11. Derechos ARCO ampliados para datos sensibles

Además de los derechos reconocidos en la Política de Privacidad general, cuando se trate de datos sensibles de salud, el Titular podrá:

- Solicitar información detallada sobre los terceros a quienes se han comunicado sus datos y sobre las transferencias internacionales realizadas.
- Solicitar la eliminación inmediata de mensajes específicos intercambiados con el asistente conversacional que contengan información sensible.
- Exigir la restricción del tratamiento mientras se resuelve una solicitud de rectificación u oposición.
- Solicitar la intervención humana y la explicación de cualquier lógica automatizada aplicada a sus datos.

Las solicitudes se atenderán en los plazos establecidos por la LOPDP, de forma gratuita, salvo en los supuestos de solicitudes manifiestamente infundadas o excesivas.

12. Conservación de datos de salud

Los datos de salud se conservan durante el tiempo necesario para la atención del paciente y para el cumplimiento de las obligaciones legales aplicables en materia sanitaria, tributaria y probatoria. Transcurrido dicho plazo, los datos se bloquean y, posteriormente, se suprimen o anonimizan de manera irreversible.

13. Gestión de incidentes y notificación de brechas

Citiomed cuenta con un procedimiento documentado para la detección, contención, evaluación y respuesta a incidentes de seguridad. En caso de producirse una vulneración de datos personales susceptible de generar un riesgo para los derechos y libertades de los Titulares:

- Se notificará a la autoridad de control en los plazos previstos por la LOPDP, con el contenido mínimo exigido.
- Cuando el riesgo sea alto, se comunicará la brecha a los Titulares afectados sin dilación indebida, utilizando un lenguaje claro y sencillo.
- Se implementarán las medidas correctivas necesarias y se documentará la gestión del incidente.

14. Supervisión y revisión de la Política

El DPD supervisa la aplicación de la presente Política, coordina la atención de las solicitudes de los Titulares y reporta periódicamente al órgano de gobierno de Citiomed sobre el estado de cumplimiento.

Esta Política se revisa al menos anualmente y cuando existan cambios normativos, tecnológicos u organizativos que puedan afectar el tratamiento de datos de salud.

15. Canales de contacto y ejercicio de derechos

El Titular puede ejercer sus derechos o formular consultas al DPD a través de:

- Correo electrónico: info@citiomed.com
- Sitio web: https://www.citiomed.com
- Dirección postal: [Dirección por completar], Quito, Ecuador

Adicionalmente, el Titular tiene derecho a presentar una reclamación ante la Superintendencia de Protección de Datos Personales del Ecuador si considera que el tratamiento de sus datos no se ajusta a la normativa vigente.

Documento emitido por Citiomed — Versión 1.0 — 18 de abril de 2026.