En Teker Salud S.A.S. (en adelante, "la Plataforma"), reconocemos la importancia de la información y estamos comprometidos con la protección de la privacidad de sus datos personales. Este Aviso de Privacidad tiene como objetivo informarle sobre cómo recopilamos, utilizamos, almacenamos, protegemos y, en ciertas circunstancias, compartimos su información personal, así como sus derechos en relación con estos datos. Nos regimos estrictamente por las disposiciones de la **Ley 1581 de 2012 (Ley de protección de datos personales)**, el **Decreto 1377 de 2013**, el **Decreto Reglamentario 1075 de 2015** (que desarrolla el Decreto 1377 de 2013), y el principio de **Responsabilidad Demostrada.**

1. Identidad y Domicilio del responsable Teker Salud S.A.S. es el titular de los derechos patrimoniales del software Teker o Tekerapp, es una plataforma dedicada a ofrecer servicios de salud a través de la tecnología. Nuestro domicilio se encuentra en Colombia.

2. Compromiso con la Seguridad, Privacidad y Responsabilidad Demostrada de la Información La Plataforma Teker Salud S.A.S. garantiza la **confidencialidad, integridad, disponibilidad y privacidad** de la información de sus grupos de interés (directivos, empleados/as, profesionales, empresas aliadas y clientes). Contamos con una **Política de Seguridad de la Información (SGSI)** y un **Manual de Gestión de Riesgos** que establecen los requerimientos y controles necesarios para proteger sus datos.

En cumplimiento del principio de **Responsabilidad Demostrada,** tal como lo establece la Superintendencia de Industria y Comercio (SIC), Teker Salud S.A.S. ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema está alineado con estándares internacionales como ISO 27001 e ISO 22301, y la legislación colombiana de protección de datos, incluyendo la Ley 1581 de 2012 y el Decreto 1377 de 2013, así como regulaciones como GDPR y HIPAA. Este marco integral permite:

- **Demostrar la gestión proactiva y sistemática de los riesgos** asociados al tratamiento de sus datos personales.
- Contar con un **Comité de Gestión de Riesgos** y roles claramente definidos, como el Responsable de Seguridad de la Informática y el Responsable de la Privacidad de la Información, que supervisan y dirigen las actividades de gestión de riesgos y seguridad de la información.

- Asegurar la **mejora continua** del sistema de gestión de riesgos y de la política de seguridad de la información, con revisiones periódicas y actualizaciones para adaptarse a cambios en el entorno o lecciones aprendidas de incidentes.
- Establecer **procedimientos claros** para el reporte y gestión de incidentes de seguridad.

3. Datos Personales que Recopilamos Recopilamos información necesaria para la prestación de nuestros servicios de teleconsulta y gestión de citas médicas. Esta información puede incluir:

- **Datos de identificación y contacto:** Nombres, apellidos, número de identificación, nacionalidad, números de teléfono (incluido WhatsApp para notificaciones), correos electrónicos.
- **Datos de salud y sensibles:** Información de la historia clínica (parametrizable y dinámica), soportes y exámenes previos del paciente, formulaciones de medicamentos, procedimientos e incapacidades, datos de interconsultas, datos de monitoreo a pacientes, y la clasificación en modelos de riesgo para catalogar grupos de pacientes y asignar atenciones.
- **Datos transaccionales y de pago:** Estos datos no quedan en nuestro sistema si no directamente en las plataformas de pago seguras como WOMPI-EPAYCO y otras plataformas de pago.
- **Datos de uso y técnicos:** Información sobre el acceso a sistemas de información, redes informáticas y aplicaciones especializadas de la plataforma, incluyendo el uso de nuestra herramienta de videoconferencia Zoom Workplace la cual está integrada con nuestra plataforma.

4. Finalidades del Tratamiento de sus Datos Personales Sus datos personales son tratados con las siguientes finalidades principales, de acuerdo con el principio de finalidad establecido en la Ley 1581 de 2012:

- **Prestación de servicios de salud:** Agendamiento, reprogramación y cancelación de citas con médicos generales, especialistas, psicólogos y nutricionistas.

- **Gestión de la atención médica:** Diligenciamiento y gestión de la historia clínica, formulación de medicamentos, procedimientos e incapacidades, revisión de soportes y exámenes previos y solicitud y tramite de interconsultas.
- **Comunicación y soporte:** Envío de notificaciones por WhatsApp y correo electrónico, y gestión de la comunicación, antes, durante y posterior a las teleconsultas (incluyendo alternativas en caso de problemas de conectividad, como llamadas por audio en Zoom o al teléfono suministrado).
- **Gestión de pagos:** Facilitar los pagos por los servicios prestados a través de plataformas seguras.
- **Monitoreo y mejora del paciente:** Posibilidad de realizar el monitoreo a pacientes y aplicar modelos de inteligencia artificial para prevenir hospitalizaciones y remisiones a urgencias.
- **Gestión institucional:** Ofrecer opciones a aliados como facturación mensual, y soporte a la habilitación médica de aliados.
- **Cumplimiento normativo y de seguridad:** Adherencia a las leyes y regulaciones aplicables, gestión de riesgos de seguridad de la información, detección y respuesta a incidentes cibernéticos.

5. Transferencia y transmisión de Datos Personales Teker Salud S.A.S. podrá compartir sus datos personales con terceros para cumplir con las finalidades descritas, siempre bajo estrictas medidas de seguridad y acuerdos de confidencialidad, en concordancia con el principio de acceso y circulación restringida de la Ley 1581 de 2012. Esto incluye:

- **Proveedores de servicios tecnológicos:** Como Maxapex para servidores externos y la plataforma Zoom Workplace para videoconferencias, garantizando su uso, seguridad, integridad y robustez. La organización cuenta con un Firewall de aplicaciones de Vercel (WAF). Exigimos a nuestros proveedores de servicios en la nube que acrediten su conocimiento y cumplimiento de la normatividad legal existente en seguridad de la información y que cuenten con medidas de control que eviten ataques contra la seguridad.
- **Plataformas de pago:** Para procesar sus transacciones de manera segura.

- **APIs de terceros:** Para la recepción de servicios, asignación de consultas y remisión de la Historia Clínica, según sea necesario para la funcionalidad de la Plataforma.
- **Autoridades competentes:** Cuando sea requerido por ley o para cumplir con obligaciones legales. Todos los proveedores y contratos de prestación de servicios deben cumplir con acuerdos de niveles de servicio (SLA) para disponibilidad, confidencialidad e integridad de la información, incluyendo cláusulas de confidencialidad y la posibilidad de auditorías aleatorias por parte de la Plataforma. Los proveedores de servicios en la nube deben demostrar que cuentan con un plan de contingencia y continuidad del negocio.

6. Medidas de Seguridad Implementadas Para proteger sus datos personales y en demostración de nuestro compromiso con el principio de **Responsabilidad Demostrada**, Teker Salud S.A.S. ha implementado un robusto Sistema de Gestión de Seguridad de la Información (SGSI) y un Manual de Gestión de Riesgos, que incluyen:

- **Cumplimiento normativo:** Adhesión a estándares internacionales como ISO 27001 e ISO 22301, y a la legislación colombiana de protección de datos (Ley 1581 de 2012, Decreto 1377 de 2013 y Decreto Reglamentario 1075 de 2015), así como regulaciones como GDPR y HIPAA.
- **Cifrado de datos:** La información sensible o personal circula por las redes de manera cifrada (HTTPS) y se utilizan mecanismos de cifrado para el envío y recepción de información clasificada como confidencial o sensible. También se cifrará la información en equipos de cómputo que almacenen datos confidenciales o de menores de edad.
- **Control de acceso:** Contraseñas fuertes (mínimo 8 caracteres con combinación de mayúsculas, minúsculas, números y caracteres especiales), autenticación de doble o múltiple factor para servicios críticos, y cuentas personales e intransferibles. Las sesiones se bloquean automáticamente tras inactividad y los usuarios son responsables de bloquear su estación de trabajo al retirarse. Se garantiza que las contraseñas de usuarios privilegiados sean actualizadas o bloqueadas inmediatamente después del retiro del empleado o contratista.
- **Protección contra malware y ciberataques:** Todos los equipos de usuario cuentan con protección antimalware (antivirus), se cuenta con procedimientos para la

identificación y análisis de incidentes de ciberseguridad. Se restringe la navegación en sitios de mala reputación y soluciones EDR actualizadas.

- **Gestión proactiva de vulnerabilidades:** Se cuenta con gestión de vulnerabilidades a nivel de computadoras y a nivel de servidores. Se asegura que los **sistemas operativos, soluciones de (antivirus) y navegadores** estén debidamente **actualizados y parchados** frente a vulnerabilidades de seguridad.
- **Desarrollo seguro:** Se aplican metodologías de desarrollo seguro durante todo el ciclo de vida del software, incluyendo análisis de vulnerabilidades antes de pasar a producción. Los ambientes de desarrollo, pruebas y producción están lógica y físicamente separados. Se exige a terceros acuerdos de propiedad intelectual, confidencialidad, certificación de seguridad en el proceso de desarrollo, y pruebas de seguridad.
- **Copias de seguridad y recuperación:** Se realizan copias de seguridad periódicas de datos, aplicaciones y configuraciones, con pruebas regulares de restauración en ambientes controlados para garantizar la disponibilidad y recuperación de la información ante incidentes o desastres. Se cuenta con un "Plan de Contingencia" y un "Plan de Recuperación ante Desastres (DRP)" para asegurar la continuidad de las operaciones críticas.
- **Seguridad física y ambiental:** Controles para prevenir el acceso no autorizado a las instalaciones, y proteger la documentación física y dispositivos de almacenamiento removibles de riesgos de acceso no autorizado, pérdida y daño. Se validan condiciones ambientales y se protegen centros de cableado.
- **Gestión de incidentes:** Procedimientos claros para el reporte y gestión de cualquier incidente de seguridad de la información a soporte@teker.co.
- **Capacitación:** Programas de concienciación, capacitación y sensibilización periódicos para todos los empleados sobre políticas y procedimientos de seguridad y privacidad de la información.

7. Derechos del Titular Como titular de sus datos personales, usted tiene el derecho de ejercer los derechos de **Acceso, Rectificación, Cancelación u Oposición (Derechos ARCO)** respecto del tratamiento de sus datos. Estos derechos están respaldados por la **Ley 1581 de 2012** y el **Decreto 1377 de 2013**.

Para ejercer cualquiera de estos derechos, o si tiene preguntas sobre este Aviso de Privacidad, puede contactarnos a través de los canales de comunicación indicados y la Plataforma contará con mecanismos de confirmación.

8. Cambios en el Aviso de Privacidad Este Aviso de Privacidad puede ser actualizado periódicamente para reflejar cambios en nuestros servicios, la criticidad de la información, el entorno de riesgos o las lecciones aprendidas de incidentes. La política de seguridad de la información se revisa continuamente. Cualquier cambio significativo será comunicado oportunamente a través de nuestros canales de comunicación o directamente en nuestra web.