Security Practices

Effective Date: 1st Feb 2025
Last Updated: 25th Feb 2025

1. Our Commitment to Security

At **thirdvoice.ai**, we prioritize the security and privacy of our users. We implement industry-leading practices to protect sensitive data and maintain the highest standards of information security.

2. Data Protection Measures

- **Encryption**: All data is encrypted both in transit (using TLS 1.2+) and at rest (using AES-256).
- **Access Controls**: We enforce strict access policies, ensuring only authorized personnel can access sensitive data.
- **Data Minimization**: We only collect the necessary information for our services—such as patient preferences and clinic data.

3. Compliance Standards

- **SOC 2 Compliance (In Progress)**: We are actively working toward SOC 2 Type II certification to ensure our processes meet rigorous security and privacy standards.
- **Data Privacy Regulations**: We comply with relevant privacy laws, including the **General Data Protection Regulation (GDPR)** and **California Consumer Privacy Act (CCPA)** where applicable.

4. Infrastructure Security

- **Secure Cloud Hosting**: Our platform is hosted on secure, SOC 2-compliant infrastructure.
- **Monitoring & Logging**: We continuously monitor our systems to detect and respond to potential threats.
- **Incident Response**: In case of a security event, we have a comprehensive incident response plan to mitigate and resolve issues swiftly.

5. Third-Party Security

We work with trusted third-party services that align with our security practices:

- **Google Analytics**: Usage tracking with anonymized data where applicable.
- **VAPI**: Secure AI voice processing.
- **Kolla**: Identity verification and fraud prevention.
- **Twilio**: Encrypted communication services.

6. User Data Protection

- **Patient Data**: We do not store voice recordings. Patient information is used solely for appointment scheduling.
- **Clinic Data**: Access to clinic dashboards is limited to authorized users.

7. Responsible Disclosure

We welcome reports of potential security vulnerabilities. If you identify a security issue, please contact us at: **support@thirdvoice.ai**