Privacy Policy

Effective Date: November 15, 2024

Sybatech, Inc., operating as Codepal ("we," "us," or "our"), is committed to protecting the privacy and security of our customers' data. This Privacy Policy explains how we collect, use, disclose, and protect the information provided to us, particularly in compliance with regulations for health-based and non-public data.

All data processed by our software is hosted within the **Azure Government Cloud GCC**, ensuring compliance with stringent security and privacy requirements for Federal entities and their partners, and non-Federal entities and businesses working with sensitive data.

---

1. Scope of Policy

This Privacy Policy applies to all data collected, stored, or processed by Sybatech, Inc. dba Codepal, including but not limited to:

- Personal data collected from customers, users, and partners.
- Health-based data or Protected Health Information (PHI).
- Non-public data, including sensitive information related to government and private entities.

---

2. Information We Collect

2.1 Personal Data

We collect information that identifies you as an individual, such as:

- Name
- Email address
- Telephone number
- Job title or role

2.2 Usage Data

We collect data automatically when you interact with our systems, including:

- IP address
- Browser type

- Log files
- Usage patterns

2.3 Health-Based Data

We may process **Protected Health Information (PHI)** on behalf of our clients who use our software in compliance with the **Health Insurance Portability and Accountability Act (HIPAA)**. PHI may include but is not limited to:

- Patient names and identifiers
- Health-related details (e.g., medical records)

2.4 Non-Public Data

We handle non-public, sensitive information from our customers, particularly government agencies, which may include but not limited to:

- Inspection results
- Regulatory compliance reports
- Internal operational data

---

3. How We Use Your Information

We use the data we collect for the following purposes:

- To provide, maintain, and enhance our software services.
- To support and troubleshoot customer needs.
- To meet regulatory and compliance requirements.
- To notify users of changes to our services or policies.
- To analyze usage trends and improve our systems.

---

4. Protecting Health-Based Data

In compliance with HIPAA, we ensure:

- **Safeguards:** We employ administrative, technical, and physical safeguards to protect PHI against unauthorized access, alteration, or disclosure.
- **Data Use Limitations:** PHI will only be used or disclosed as permitted under Business Associate Agreements (BAAs) with covered entities.
- **Subcontractor Compliance:** Subcontractors with access to PHI must adhere to HIPAA requirements.

- **Breach Notification:** In the event of a data breach involving PHI, we will notify affected clients promptly and comply with applicable laws regarding breach notifications.

---

5. Protecting Non-Public Data

Given our reliance on the **Azure Government Cloud GCC**:

- **Data Isolation:** All customer data is housed in the Azure Government Cloud GCC, ensuring compliance with U.S. federal, state, and local data protection regulations.
- **Restricted Access:** Access to non-public data is limited to authorized personnel with roles that require access.
- **Encryption:** Data is encrypted both in transit and at rest using industry-standard protocols.
- **Audit Logging:** Comprehensive logging and monitoring tools are in place to track data access and usage.

---

6. Disclosure of Information

We do not sell or share personal data with third parties except in the following circumstances:

- **With Service Providers:** Data may be shared with trusted vendors who perform services on our behalf, subject to strict confidentiality obligations.
- **As Required by Law:** We may disclose data to comply with legal obligations, such as court orders or government requests.
- **In Business Transactions:** In the event of a merger or acquisition, data may be transferred to the new entity with continued adherence to this Privacy Policy.

---

7. Security Measures

We take extensive measures to protect the information entrusted to us, including:

- Using the advanced security features of Azure Government Cloud GCC.
- Implementing multi-layer authentication and role-based access controls.
- Conducting regular security audits and assessments.

Despite our efforts, no system can be 100% secure. Users are encouraged to take precautions when transmitting sensitive data.

---

8. Your Data Protection Rights

Depending on your location, you may have the following rights:

- **Access:** Request access to personal data we hold about you.
- **Correction:** Request corrections to inaccurate or incomplete information.
- **Deletion:** Request deletion of your personal data, subject to applicable legal obligations.
- **Restriction:** Request restrictions on how your data is processed.

---

9. Data Retention

We retain personal and non-public data only as long as necessary to fulfill the purposes outlined in this policy or comply with legal obligations.

---

10. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices or applicable regulations. Updates will be posted on our website, and significant changes will be communicated to users directly.

---

11. Contact Us

If you have questions about this Privacy Policy or our data practices, please contact us:

- **Email:** privacy@codepaltoolkit.com
- **Address:** Sybatech, Inc. dba Codepal, P.O. Box 9047, Springfield, Illinois 62791-9047
