BUILDWICK SOLUTIONS, INC.

VORTEX CONTACT INTELLIGENCE PLATFORM

Privacy Policy

How we collect, use, protect, and share your information

Last Updated: February 28, 2026

Oakridge, North Carolina, United States
contact@buildwicksolutions.com

Privacy Policy

Buildwick Solutions, Inc. (“Buildwick,” “we,” “us,” or “our”) operates the Vortex Contact Intelligence Platform (the “Platform” or “Service”). This Privacy Policy describes how we collect, use, store, share, and protect information about you when you access or use our Platform, and explains your rights and choices with respect to that information.

By accessing or using Vortex, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with the practices described herein, please do not use the Service. This Privacy Policy does not create any contractual or other legal rights beyond those established by applicable law.

1.1 Information We Collect

We collect information in several ways: directly from you, automatically through your use of the Platform, and from third-party sources.

A. Account and Registration Information

When you create an account or onboard your organization onto Vortex, we may collect:

- Full legal name and job title
- Business email address and phone number
- Organization name, address, and industry type (e.g., dental practice)
- Login credentials (passwords are hashed and are not stored in plaintext)
- Billing contact information and subscription plan details
- Practice identifiers for healthcare organizations

B. Communications and Call Data

As a contact intelligence platform, the core functionality of Vortex involves processing real-time communications. We may collect:

- Inbound and outbound call recordings and audio data
- Real-time and post-call transcripts generated by our AI engine
- SMS messages sent and received through the Platform
- Voicemail recordings and transcriptions
- Call metadata including timestamps, duration, caller ID, and disposition codes
- AI-generated annotations including sentiment scores, call summaries, detected topics, and outcome classifications

For healthcare clients, call content may contain Protected Health Information (PHI) as defined under HIPAA. Such data is handled in accordance with our HIPAA compliance practices and the terms of any executed Business Associate Agreement (BAA).

C. Insurance and Claims Data

Vortex’s Revenue Cycle Management (RCM) module may collect and process:

- Patient demographic information submitted by your practice
- Insurance eligibility verification results received from payers and partner interfaces
- Claim submission data, procedure codes, and remittance information
- Denial reasons, appeal records, and resubmission histories

D. Usage and Technical Data

We automatically collect certain technical information to operate, improve, and secure the Platform:

- IP address, browser type, and operating system
- Device identifiers and session tokens
- Pages visited, features used, and interaction timestamps
- Error logs and performance metrics
- Referring URLs and search queries that led you to the Platform

E. Billing and Payment Information

All payment processing is handled by our third-party payment processor. We do not store full credit card numbers, CVV codes, or bank account numbers on our servers. We receive and store only:

- The last four digits of your payment method
- Card expiration date and billing address
- Payment processor customer and subscription identifiers for account management
- Invoice history and payment status records

F. Cookies and Tracking Technologies

When you visit our website or use the Platform, we may use cookies, web beacons, pixel tags, and similar tracking technologies to collect information about your browsing behavior. These technologies help us analyze trends, administer the site, track user navigation, and gather aggregate demographic information. You may control the use of cookies through your browser settings. Please note that disabling cookies may affect certain features of the Platform.

G. Information from Third Parties

We may receive information about you from:

- Insurance payers and clearinghouses during eligibility and claims transactions
- Authentication providers used to verify your identity
- Marketing and analytics platforms used to understand how users discover Vortex

1.2 How We Use Your Information

A. Service Delivery

- To authenticate users and provide secure access to the Platform
- To process insurance eligibility checks, claim submissions, and remittance reconciliation
- To transcribe and analyze calls using our AI engine for agent performance and patient engagement insights
- To route inbound communications to the appropriate agents or departments
- To send SMS appointment reminders, follow-ups, and service notifications on behalf of your practice

B. AI and Analytics

- To generate sentiment analysis, treatment discussion summaries, and call outcome classifications
- To power denial risk scores displayed during insurance verification
- To surface business intelligence in Admin and SuperAdmin dashboards
- To improve our AI models using de-identified, aggregated data only (raw PHI is not used for model training unless separately authorized under a BAA)

C. Billing and Account Management

- To process subscription payments and issue invoices via our payment processor
- To send payment receipts, renewal notices, and billing alerts
- To manage subscription changes and cancellations

D. Security and Compliance

- To monitor for unauthorized access, fraud, or misuse of the Platform
- To maintain audit logs in support of HIPAA and our internal security policies
- To comply with applicable laws, regulations, and lawful government requests
- To enforce our Terms and Conditions and other policies

E. Communications and Support

- To respond to your support tickets, questions, and feature requests
- To send product updates, maintenance notices, and security alerts
- To send marketing communications where you have opted in or where permitted by applicable law

1.3 How We Share Your Information

We do not sell your personal data to third parties. We share information only in the following limited circumstances:

A. Service Providers

We engage third-party vendors to help operate the Platform. These providers are given access only to the data reasonably necessary for their specific function and are bound by data processing agreements. Categories of service providers include:

- Cloud infrastructure, storage, and authentication services
- Payment processing and subscription management services
- Insurance eligibility verification and electronic claim submission partners
- SMS and telephony infrastructure providers
- AI-powered call analysis services

B. Healthcare-Specific Disclosures

For covered entities and their business associates under HIPAA, we may share PHI only as permitted or required by the HIPAA Privacy Rule, including with payers and clearinghouses for the purpose of treatment, payment, or healthcare operations, and as directed by the covered entity under the terms of an executed Business Associate Agreement (BAA).

C. Legal and Regulatory Disclosures

We may disclose your information where we believe in good faith that such disclosure is reasonably necessary to comply with applicable law, regulation, legal process, or enforceable governmental request; to protect the rights, property, or safety of Buildwick, our users, or the public; or to detect, investigate, or address fraud, security incidents, or technical issues.

D. Business Transfers

In the event of a merger, acquisition, reorganization, or sale of assets, your information may be transferred to the successor entity. We will use reasonable efforts to ensure the successor entity is bound by privacy protections that are materially consistent with this Policy.

1.4 Data Retention

We retain your data for as long as your account is active or as reasonably needed to provide services, comply with our legal obligations, resolve disputes, and enforce our agreements. General retention guidelines include:

- **Account and contact data:** Duration of the account plus up to 3 years after termination.
- **Call recordings and transcripts:** Up to 7 years in support of HIPAA audit requirements (unless a different period is specified in your BAA).
- **Insurance verification and claims records:** Up to 7 years in alignment with CMS and HIPAA record retention guidance.
- **Billing records:** Up to 7 years to satisfy tax and financial compliance obligations.
- **Usage logs and analytics:** Up to 24 months, then aggregated or deleted.
- **SMS consent records:** Minimum of 5 years in support of TCPA record-keeping requirements.

Upon account termination, we will delete or anonymize your data within 90 days, except where longer retention is required by law, regulation, or an executed BAA.

1.5 Data Security

We employ commercially reasonable administrative, technical, and physical safeguards designed to protect your information, including:

- Encryption at rest using industry-standard algorithms for stored data
- Encryption in transit using industry-standard protocols for data transmitted between your browser, our servers, and third-party APIs
- Role-based access control limiting data access to personnel with a legitimate business need
- Multi-factor authentication enforced for platform administrator accounts
- Regular penetration testing and vulnerability assessments conducted by qualified third parties
- Automated intrusion detection and security event monitoring
- Employee security training conducted annually and upon onboarding

No method of electronic transmission or storage is completely secure. While we strive to use commercially reasonable means to protect your information, we cannot guarantee its absolute security. In the event of a data breach affecting your information, we will provide notification as required by applicable law and any executed BAA.

1.6 Your Rights and Choices

Depending on your location and applicable law, you may have certain rights regarding your personal information, which may include:

- **Access:** Request a copy of the personal data we hold about you.
- **Correction:** Request correction of inaccurate or incomplete data.
- **Deletion:** Request deletion of your personal data, subject to legal and contractual retention requirements.
- **Portability:** Request your data in a structured, machine-readable format.
- **Objection:** Object to processing of your data for marketing purposes.
- **Restriction:** Request restriction of processing in certain circumstances.
- **Do Not Sell:** Buildwick does not sell personal information. If applicable law grants you the right to opt out of the sale of personal data, you may exercise that right by contacting us.

To exercise any of these rights, please contact us at contact@buildwicksolutions.com. We will respond within 30 days or as otherwise required by applicable law. Certain rights may not apply where we process data on behalf of a covered entity under HIPAA; in such cases, requests should be directed to the covered entity.

1.7 California Privacy Rights (CCPA/CPRA)

If you are a California resident, you may have additional rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). These may include: the right to know what personal information is collected, used, and disclosed; the right to request deletion of personal information; the right to opt out of the sale or sharing of personal information (Buildwick does not sell personal data); the right to non-discrimination for exercising privacy rights; and the right to correct inaccurate personal information. To submit a request, contact us at contact@buildwicksolutions.com.

1.8 International Data Transfers

Vortex is operated in the United States. If you access the Platform from outside the United States, your information may be transferred to, stored, and processed in the United States. By using the Platform, you acknowledge this transfer. We implement safeguards as appropriate for any international data transfers in accordance with applicable data protection laws.

1.9 Children’s Privacy

Vortex is a B2B enterprise platform not directed at children under 13 (or under 16 in certain jurisdictions). We do not knowingly collect personal information from children. If we become aware that a child has provided us with personal information, we will take steps to delete it. If you believe a child has provided personal information through the Platform, please contact us.

1.10 Changes to This Policy

We may update this Privacy Policy from time to time. We will endeavor to notify you of material changes by email or by posting a notice within the Platform at least 30 days before the effective date of the change. Your continued use of the Platform after the effective date constitutes your acknowledgment of the revised Policy.

1.11 Contact

For privacy-related inquiries, data subject requests, or to report a potential privacy concern:

- **Email:** contact@buildwicksolutions.com
- **Mailing Address:** Oakridge, North Carolina, US

For HIPAA-specific inquiries, include “HIPAA” in your subject line.