BUILDWICK SOLUTIONS, INC.

VORTEX CONTACT INTELLIGENCE PLATFORM

Compliance and Security

Security architecture, compliance posture, and shared responsibilities

Last Updated: February 28, 2026

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

Compliance and Security

Buildwick Solutions, Inc. is committed to maintaining a security and compliance program designed to protect the confidentiality, integrity, and availability of data processed through the Vortex Platform. This section describes our compliance posture and the shared responsibilities between Buildwick and our customers.

The information provided in this document is for general informational purposes and describes Buildwick's current security and compliance practices. It does not constitute a warranty, guarantee, or contractual commitment. Buildwick's obligations to customers are governed solely by the applicable executed agreements, including the Terms and Conditions, Business Associate Agreement (if applicable), and any subscription agreement.

4.1 Security Program Overview

Our information security program is built on a defense-in-depth approach that combines technical controls, operational safeguards, and governance policies.

Data Security

- Encryption at rest: Industry-standard encryption is applied to stored data including databases, backups, and object storage
- Encryption in transit: Industry-standard encryption protocols are enforced for data moving between clients, our servers, and third-party APIs
- Data classification policies are applied to differentiate handling of PHI, PII, and general business data

Identity and Access Management

- Authentication is managed through a dedicated identity provider with multi-factor authentication enforcement for administrative roles
- Role-based access control with four defined tiers: SuperAdmin, Admin, Agent, and Read-Only
- Principle of least privilege is applied — users access only the data and functions required for their role
- Access is reviewed quarterly and revoked promptly upon employee termination
- Session management with automatic timeout after a period of inactivity

Monitoring and Incident Response

- Automated security event monitoring through dedicated monitoring and audit logging services
- Anomaly detection configured to alert on unusual login patterns, bulk data access, or API abuse
- Comprehensive audit logging of administrative actions, data access events, and authentication attempts
- Incident response plan reviewed and tested periodically, with defined roles and escalation paths
- Breach notification procedures designed to align with HIPAA Breach Notification Rule requirements
- Mean time to detect (MTTD) and mean time to respond (MTTR) tracked as security KPIs

4.2 HIPAA Compliance

Vortex is designed to support healthcare organizations subject to HIPAA and its implementing regulations, including the Privacy Rule, Security Rule, and Breach Notification Rule. A detailed description of our HIPAA Compliance Program is available as a separate document. Key highlights include:

- Buildwick enters into Business Associate Agreements (BAAs) with Covered Entities that use the Platform to create, receive, maintain, or transmit PHI
- Administrative, physical, and technical safeguards are implemented consistent with the HIPAA Security Rule
- Workforce members receive HIPAA training upon onboarding and annually
- Risk analyses are conducted at least annually and upon material changes
- Breach notification procedures are maintained in alignment with 45 CFR Part 164, Subpart D

To request a BAA, contact contact@buildwicksolutions.com with the subject line “BAA Request.”

4.3 Industry Compliance Alignment

Our security practices are designed in alignment with industry-recognized trust and assurance frameworks addressing security, availability, confidentiality, and processing integrity. We continuously evaluate and seek to enhance our compliance posture. Customers requiring compliance documentation may contact us to discuss our current assessments and controls.

This alignment is described for informational purposes only and does not constitute a representation that Buildwick has achieved any specific third-party certification or attestation unless expressly stated.

4.4 Insurance Claims and Clearinghouse Compliance

Vortex’s RCM module transmits electronic healthcare transactions that are subject to HIPAA’s Electronic Transactions and Code Sets Standards (45 CFR Part 162):

- Eligibility Verification: Transmitted through certified healthcare transaction partners
- Claims Submission: Transmitted through certified electronic clearinghouse partners
- Remittance Advice: Received and parsed from payer electronic remittance files
- Claim Status: Used to check outstanding claim status with payers

Transaction data is logged and retained for audit purposes. Buildwick endeavors to ensure that all electronic transactions are transmitted in accordance with applicable standards adopted by HHS, but does not guarantee the accuracy or completeness of data provided by third-party payers or clearinghouses.

4.5 Payment Security

Vortex does not store, process, or transmit cardholder data directly. All payment processing is delegated to a third-party payment processor. Our integration uses a tokenization model, meaning sensitive card data does not reside on Buildwick’s systems. Buildwick does not make any representations regarding the payment processor’s certifications or compliance status; customers should review the payment processor’s own security documentation.

4.6 Vendor and Subprocessor Management

We maintain a list of third-party subprocessors that may access Customer Data. Subprocessors are subject to: contractual data processing agreements or BAAs (for HIPAA-applicable processors), security assessment prior to onboarding, and periodic review of their compliance status.

Buildwick uses commercially reasonable efforts to select subprocessors that maintain appropriate security controls, but does not guarantee the security practices or compliance status of any third-party subprocessor. Buildwick's liability for subprocessor actions is governed by the applicable executed agreements.

4.7 Business Continuity and Disaster Recovery

Buildwick maintains business continuity and disaster recovery capabilities designed to support the following targets:

- **Recovery Time Objective (RTO):** Targeted at 4 hours for core Platform services.
- **Recovery Point Objective (RPO):** Targeted at 1 hour — maximum anticipated data loss in a disaster scenario.
- Database backups are performed at regular intervals with point-in-time recovery enabled
- Redundant deployment across multiple availability zones for critical services
- Disaster recovery plan tested periodically via tabletop exercises
- **Platform uptime target:** 99.9% monthly availability (excluding planned maintenance windows).
- Planned maintenance is communicated to customers at least 72 hours in advance via email and in-app notification

The RTO, RPO, and uptime targets stated above are goals, not guarantees. Actual recovery times and uptime may vary depending on the nature and scope of the incident. Buildwick's obligations regarding service availability are governed solely by the applicable executed agreements.

4.8 Employee and Organizational Security

- Background checks are conducted on employees with access to production systems or customer data
- Security awareness training is completed upon onboarding and annually
- Acceptable use policies and confidentiality agreements are signed by employees
- Access is revoked promptly upon employee departure through automated offboarding workflows
- Security policies are reviewed and updated at least annually or upon material changes

4.9 Customer Responsibilities

While Buildwick implements security controls at the platform level, customers retain responsibility for:

- Managing their own user accounts, access levels, and timely offboarding of former employees
- Obtaining and maintaining required patient consents for SMS and recording under HIPAA, TCPA, and applicable state laws
- Configuring role-based access appropriately within their Vortex account
- Executing a BAA with Buildwick prior to inputting PHI into the Platform
- Complying with all applicable laws and regulations governing their practice and communications
- Maintaining the security of their own devices and networks used to access Vortex

- Reporting suspected security incidents to contact@buildwicksolutions.com promptly
- Ensuring compliance with 10DLC registration and carrier requirements for their SMS campaigns

Buildwick disclaims any liability arising from a customer's failure to fulfill the responsibilities described in this section.

4.10 Reporting Security Concerns

We encourage responsible disclosure of security vulnerabilities. If you discover a potential security issue in the Vortex Platform, please contact us at:

- **Security Email:** contact@buildwicksolutions.com
- **Subject Line:** "Security Vulnerability Report"
- Please include: description of the vulnerability, steps to reproduce, and potential impact

We will endeavor to acknowledge your report within 2 business days and provide an update within 10 business days. We ask that you not publicly disclose vulnerabilities until we have had reasonable time to investigate and remediate. Buildwick does not currently offer a bug bounty program.

4.11 Compliance Governance and Review

- Security and compliance policies are reviewed and updated at least annually
- Risk assessments are conducted at least annually and following material changes to the Platform or threat landscape
- A designated Privacy Officer and Security Officer are responsible for overseeing compliance
- An internal compliance committee meets quarterly to review security metrics, incidents, and regulatory developments
- Customer-facing compliance documentation is updated to reflect material changes within a reasonable timeframe

4.12 Disclaimer

The security and compliance practices described in this document represent Buildwick's current approach as of the date indicated above. Security practices are subject to change as threats evolve and technology advances. No security program can guarantee the prevention of all unauthorized access or data breaches. Buildwick's contractual obligations to customers are governed solely by the applicable executed agreements, and this document does not create or modify any such obligations.