**NPIVerify Privacy Policy**

*Last Updated: May 20, 2025*

This Privacy Policy explains how Alertcloud LLC ("we," "us," or "our") collects, uses, discloses, and protects information in connection with NPIVerify, an online tool that enables users to query National Provider Identifier (NPI) numbers to access publicly available information from the National Plan and Provider Enumeration System (NPPES) registry, including Office of Inspector General (OIG), Provider Enrollment, Chain, and Ownership System (PECOS), and state license data ("Service"). By accessing or using the Service, you agree to this Privacy Policy. If you do not agree, you must not use the Service.

**1. Scope of This Policy**

1.1 This Privacy Policy applies to all users of the Service, including those who access the Service under Prepaid or Ongoing subscription plans. It covers information collected through the Service's website, including data processed via cookies or third-party payment processors.

1.2 This policy does not apply to third-party websites linked from the Service (e.g., state-level databases), which have their own privacy policies. You should review those policies before interacting with such sites.

**2. Information We Collect**

Given the Service's purpose of querying public NPI data, we collect minimal personal information. The types of information we may collect include:

2.1 **Information You Provide Directly**:

(a) **Payment Information**: When you purchase a Prepaid or Ongoing Plan, we collect payment details (e.g., credit card number, billing address) through third-party payment processors. We do not store this information directly.

(b) **Account Information**: If you create an account for subscription management, we may collect your email address and a password to authenticate your access.

(c) **Contact Information**: If you contact us (e.g., for support or inquiries), we may collect your name, email address, or other details you provide.

2.2 **Information Collected Automatically**:

(a) **Usage Data**: We collect anonymized data about your interactions with the Service, such as pages visited, NPI queries performed, and error rates, using cookies or similar technologies (see our Cookie Policy (#) for details).

(b) **Device and Log Data**: We may collect technical information, such as your IP address, browser type, operating system, and device identifiers, to ensure security and optimize performance.

2.3 **NPI Query Data**: The NPI numbers you input are used solely to retrieve public data from the NPPES registry and are not stored or linked to your identity unless required for account-specific functionality (e.g., tracking subscription usage).

2.4 **No Sensitive Health Information**: The Service does not collect or process protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), as it handles only public NPI data.

**3. How We Use Your Information**

We use the information we collect to:

3.1 **Provide and Maintain the Service**:

(a) Process NPI queries to deliver OIG, PECOS, and state license information.

(b) Authenticate your account and manage access to Prepaid or Ongoing Plans.

(c) Process payments through third-party payment processors.

3.2 **Improve and Optimize the Service**:

(a) Analyze anonymized usage data to enhance performance, fix errors, and improve user experience.

(b) Monitor and prevent security threats, such as unauthorized access or fraud.

3.3 **Communicate with You**:

(a) Respond to your inquiries, support requests, or complaints.

(b) Send transactional emails related to your subscription (e.g., payment confirmations, renewal notices).

3.4 **Comply with Legal Obligations**:

(a) Fulfill requirements under applicable laws, such as tax reporting or data protection regulations (e.g., GDPR, CCPA).

3.5 We do not use your information for marketing, advertising, or profiling purposes beyond what is necessary to provide the Service.

**4. How We Share Your Information**

We prioritize data minimization and share your information only in the following circumstances:

4.1 **Third-Party Service Providers**:

(a) **Payment Processors**: We share payment information with trusted third-party processors (e.g., Stripe, PayPal) to process transactions for Prepaid or Ongoing Plans. These providers are contractually obligated to protect your data and comply with applicable laws.

(b) **Analytics Providers**: We may use anonymized analytics services (e.g., Google Analytics) to understand usage patterns. These providers receive only non-identifiable data.

(c) **Hosting and Security Providers**: We use cloud or security services to store and protect data, ensuring they adhere to strict data protection standards.

4.2 **Legal and Compliance Purposes**:

(a) We may disclose information if required by law, such as in response to a court order, subpoena, or regulatory request.

(b) We may share information to protect our rights, property, or safety, or that of our users, including to prevent fraud or enforce our Terms and Conditions.

4.3 **Business Transfers**:

(a) If we undergo a merger, acquisition, or sale of assets, your information may be transferred as part of the transaction. We will notify you of any such transfer and any changes to how your data is handled.

4.4 We do not sell, rent, or share your personal information with third parties for marketing or advertising purposes.

**5. Cookies and Similar Technologies**

5.1 We use cookies and similar technologies to provide essential functionality, improve performance, and store preferences (e.g., consent settings). For details, including types of cookies and how to manage them, see our Cookie Policy (#).
5.2 Strictly necessary cookies are required for the Service to function and cannot be disabled. You may opt out of non-essential cookies (e.g., performance cookies) via browser settings or our consent mechanism, where applicable.

**6. Data Retention**

6.1 We retain information only for as long as necessary to fulfill the purposes outlined in this policy or as required by law:
(a) **Payment Information**: Processed by third-party payment processors and not stored by us, except as needed for transaction records (e.g., up to 7 years for tax purposes).
(b) **Account Information**: Retained for the duration of your active subscription and up to 1 year after account closure to address disputes or legal requirements.
(c) **Usage and Device Data**: Anonymized data may be retained for up to 2 years for analytics; identifiable data (e.g., IP addresses for security logs) is deleted within 90 days unless required for legal purposes.
(d) **Contact Information**: Retained until your inquiry is resolved, unless ongoing communication is needed.
6.2 NPI query data is not stored beyond the session unless required for subscription usage tracking, in which case it is anonymized or deleted after 30 days.
6.3 We securely delete or anonymize data when it is no longer needed, using industry-standard methods.

**7. Data Security**

7.1 We implement reasonable technical and organizational measures to protect your information, including:
(a) Encryption of payment data and account credentials during transmission and storage.
(b) Secure servers and access controls to prevent unauthorized access.
(c) Regular security assessments to identify and address vulnerabilities.
7.2 Despite our efforts, no system is completely secure. We cannot guarantee absolute security, and you use the Service at your own risk. You are responsible for maintaining the confidentiality of your account credentials.

**8. Your Data Protection Rights**

Depending on your location, you may have rights under data protection laws, such as GDPR (European Economic Area) or CCPA (California). These may include:
8.1 **Access**: Request a copy of the personal information we hold about you.
8.2 **Rectification**: Request correction of inaccurate or incomplete information.
8.3 **Deletion**: Request deletion of your personal information, subject to legal retention obligations.
8.4 **Restriction**: Request restriction of processing in certain circumstances.
8.5 **Data Portability**: Request transfer of your information to another provider in a structured format.
8.6 **Objection**: Object to processing based on legitimate interests (e.g., analytics).

8.7 **Opt-Out of Sales**: Under CCPA, opt out of the sale of personal information. We do not sell your information.
8.8 To exercise these rights, contact us at the details provided in Section 11. We will respond within 30 days (or as required by law, e.g., 45 days under CCPA). We may require identity verification to process your request.
8.9 If you are in the EEA, you may also lodge a complaint with your local data protection authority.

**9. International Data Transfers**

9.1 The Service is operated from the United States, and your information may be processed on servers located in the US or other jurisdictions. If you are located outside the US (e.g., in the EEA), your data may be transferred to countries with different data protection standards.
9.2 We ensure appropriate safeguards for international transfers, such as Standard Contractual Clauses (SCCs) under GDPR, to protect your information. Contact us for details on our transfer mechanisms.

**10. Children's Privacy**

10.1 The Service is not intended for use by individuals under 18 years of age. We do not knowingly collect personal information from children. If we learn that we have collected such information, we will promptly delete it. Contact us if you believe we have inadvertently collected data from a child.

**11. Contact Information**

11.1 For questions, concerns, or requests regarding this Privacy Policy, including exercising your data protection rights, please contact us at:
Alertcloud LLC
Email: info@alertcloud.com

11.2 We will respond to inquiries as soon as reasonably practicable, typically within 30 days for data protection requests.

**12. Updates to This Privacy Policy**

12.1 We may update this Privacy Policy at any time to reflect changes in our practices, legal requirements, or Service functionality. The updated policy will be posted on the Service with the revised "Last Updated" date.
12.2 Your continued use of the Service after changes are posted constitutes your acceptance of the revised Privacy Policy. You are responsible for periodically reviewing this policy.

**13. Compliance with Laws**

13.1 This Privacy Policy is designed to comply with applicable data protection laws, including but not limited to:
(a) **GDPR**: For EEA users, ensuring lawful processing, transparency, and user rights.
(b) **CCPA**: For California residents, providing opt-out rights and transparency about personal information.
(c) **HIPAA**: While the Service does not process PHI, we ensure public NPI data is handled responsibly to avoid misuse.

13.2 If you are located in a jurisdiction with specific data protection requirements, you may have additional rights. Contact us to exercise these rights or learn more.