Privacy and Data Use Policy

Introduction

This Privacy and Data Use Policy explains how Delta Dental Plan of Michigan, Inc. and its affiliates and subsidiaries ("Company," "we," "our"), collects, uses, and protects your personal information when you use our services. By accessing or using our website, you agree to the terms outlined in this policy.

This Policy may be updated from time to time to reflect changes in our business, legal, or regulatory obligations. We will not collect additional categories of your personal information or use your personal information already collected for additional purposes without providing you with notice of our intent to do so. If we make material changes to this Policy, we will notify you by posting our updated privacy and data use policy on our website with a new effective date.

Information We Collect

1. **Personal Information**: We collect personal information from applicants, including but not limited to:
    - Contact details (name, email address, phone number)
    - Resume/CV information (work history, education, skills)
    - Any other information you voluntarily provide
    - Information about your health/disability that is relevant to your ability or availability to work or to a reasonable accommodation, to the extent allowed by applicable law or other applicable limitations
    - Information you provide in response to voluntary self-identification for purposes of government mandated statistics, such as race/ethnicity, gender, disability, and veteran status, collected in accordance with applicable law
    - Information revealed during background screenings, including but not limited to your prior employment, education, criminal records, credit history (if applicable).
    - Immigration documentation required by law
2. **Automatically Collected Information**: We may collect certain information automatically when you visit our website, including:
    - General geographic region
    - Browser type
    - Device information
    - Usage data (pages visited, time spent, interactions)
    - Devices and Location Signals
        - Geolocation Country Code: Returns the country code of the geolocation associated with the application.
        - IP Address: Returns the IP address associated with the application
        - VPN and Proxy Detection: Identifies attempts to mask a true country or region using anonymizing networks

        - Device Fingerprinting: Flags repeated submissions originating from the same hardware, browser profile, or virtual machine
        - JA4 Fingerprinting (a technique for creating a fingerprint of a client's TLS/SSL network connection for website security and fraud prevention): returns the JA4 fingerprint associated with the event.
    - Behavioral and Submission Patterns
        - Submission Velocity: Detects unusual application volume or robotic submission speeds indicative of automated mass-apply scripts
        - Session Anomalies: Spots automated or scripted keyboard/mouse movement patterns during the application process
        - Autonomous System Number: Returns the autonomous system number associated with the event.
        - Count of Job Requisitions Applied to: Returns the number of job requisitions applied to by the associated candidate.
        - External Job Application Duration: Returns the number of minutes it took for the candidate to complete the external job application.
3. **Other Information:** We may collect and retain the following additional information generated during the pre-hire or onboarding processes:
    - Data generated by interviewers or recruiters based on their interactions with you or provided by you where allowed under applicable law
    - Data provided by third-party placement firms, applicant matching platforms, recruiters, or job-search websites, where applicable
    - Photograph and images/audio footage captured on CCTV or other video systems when visiting our office or captured in the course of recruitment events or video recruitment interviews

How We Use Your Information

We plan to utilize the information you provide in the following ways:

1. **Application Process**: We use your personal information to process your job application, evaluate your qualifications, and communicate with you during the recruitment process.
2. **Legal Compliance**: We may use your information to comply with legal obligations, such as equal opportunity laws and reporting requirements.
3. **Improving Our Services**: We analyze usage data to improve our website, enhance user experience, and optimize our recruiting process.

If we would like to use your data in a different manner than disclosed in this privacy statement, we will contact you (via the contact information provided to us, such as by mail or email) to ask your permission to use the data in this new way, and to seek your consent to do so.

Data Sharing and Disclosure

We are the sole owner of the information collected on this website. We do not sell, share or rent your information to third parties (marketers) for their own use, unless we first obtain your explicit consent to do so.

In some situations, including those required by law, we may share personal information with organizations affiliated with us, or with unaffiliated third parties to provide services to you on our behalf. We do not allow these third parties to use your information for any purpose other than that requested by us and require them to protect personal information received from us in a manner similar to the protections we offer.

If we should merge with, acquire, or be acquired by another company, personal information provided to us may be transferred to or shared with that organization.

1. **Third Parties**: We may share your information with third parties, including:
    - Service providers (e.g., hosting, analytics)
    - Background check providers
    - Legal authorities (if required by law)
2. **International Transfers**: Your information may be transferred to and processed in the United States or other countries where our service providers are located.

Data Security

Security: We take reasonable measures to protect your personal information from unauthorized access, disclosure, or alteration. We maintain organizational, physical and technical security safeguards for all the personal data we hold. We have protocols, controls and relevant policies, procedures and guidance to maintain these arrangements, taking into account the risks associated with the categories of personal data and the processing we undertake.

Due to the rapidly evolving nature of information technologies, no transmission of data over the internet can ever be fully guaranteed. However, we have appropriate technical, administrative and physical procedures in place to protect personal information from loss, misuse or alteration. We take steps to ensure that access to personal information is limited to individuals who have a business need consistent with the reason the information was provided. We maintain personal information in accordance with industry best practices and the requirements of applicable laws and train our employees on our privacy and security practices.

When we contract with third parties to provide services for us that involve your personal information, we require that they protect your information in a manner similar to the protections we offer.

Any of our websites containing or soliciting nonpublic personal information are SSL encrypted.

Retention: We retain your data only as long as necessary for recruitment and/or employment purposes or as required by law.

Your Rights

1. **Access and Correction**: You have the right to access, correct, or update your personal information. Contact us if you need assistance.
2. **Withdrawal of Consent**: You can withdraw your consent for data processing at any time.

Contact Us

If you have any questions or concerns about this Privacy and Data Use Policy, please contact:

Jim Couch
Vice President, Legal Counsel
jcouch1@deltadentalnc.com

Last updated: 10/27/2026