Delta Dental of Colorado
Vendor Compliance Requirements

Delta Dental of Colorado (hereinafter "*DDCO*") is committed to establishing and observing high standards of ethical conduct in business and operational practices. As members of DDCO's working community, we depend on one another to, as a team, meet the high standards of honesty, integrity, and diligence that we expect of ourselves and that our members and their families expect of us. This packet is a resource for our contractors and vendors to ensure that you are aware of the compliance obligations related to your work and services performed with and for DDCO. Your company will receive relevant questionnaires and requests for auditing regularly to recertify your understanding of your compliance obligations.

We value you as members of our community and hold you to the same high standards of ethics and compliance as our employees and other team members. As recipients of federal health care program funds, including Medicare and Medicaid, DDCO is required by law to notify employees, affiliates, contractors, and vendors of their requirement to comply with the federal and state False Claims Acts, which are intended to prevent and detect fraud, waste, and abuse in the federal health care programs.

Compliance Hotline

DDCO is committed to meeting the highest standards for honesty and integrity in all business practices. DDCO's employees, affiliates, contractors, members, and vendors who do business with DDCO can report compliance concerns using the Compliance Hotline. All reports will be treated with appropriate confidentiality and may be made anonymously. The Hotline is available 24 hours a day, seven 7 days a week, toll-free at 833-430-0255 or online at ddpco.ethicspoint.com. We depend on each member of the community to do the right thing and to raise questions as they come up. Ethical conduct and compliance are everyone's job, and each of us can make a difference.

Data Privacy Attestation

As a vendor or contractor to DDCO, you may receive certain financial, personal, or other sensitive information about DDCO or its participants and beneficiaries. If you have access to this information, DDCO expects all vendors to comply with the following.

By signing this Attestation, you hereby represent, warrant, and certify to DDCO that your organization is compliant with the following Items 1-24, and will remain so during the term of its relationship with DDCO and to the extent applicable or appropriate, thereafter, except as specifically indicated on the last page of this Attestation.

1. **Accessibility Compliance:** Vendor is, and will remain, compliant with all applicable federal civil rights laws, including Section 1557 of the Affordable Care Act (Section 1557). Vendor will not discriminate on the basis of race, color, national origin (including limited English proficiency and primary language), age, disability, gender, veteran-status or sex. Vendor agrees to provide individuals with the following in a timely manner and free of charge: Reasonable modifications and free appropriate auxiliary aids and services to people with disabilities to communicate effectively with Vendor, such as qualified sign language interpreters and written information in other formats (large print, audio, accessible electronic formats, etc.); and free language-assistance services — such as qualified

Delta Dental of Colorado
6465 Greenwood Plaza Blvd., Suite 900
Centennial, CO 80111-8902

Telephone: 303-741-9300, 1-800-233-0860
Fax: 303-741-9338
Web: deltadentalco.com

interpreters and information written in other languages — to people whose primary language is not English.

2. **DDPA Standards:** Vendor has received and shall comply with applicable Delta Dental Plans Association (DDPA) Standards.

3. **Access Control Policy.** Vendor has, and shall maintain, an effective process to ensure that access to its company resources and information is only provided to authorized users and shall proactively review and monitor the access controls to ensure compliance with need to know, need to use, and least privilege principles.

4. **Patch Management Policy**. Vendor has, and shall maintain and periodically review and update, written processes and methodology to maintain hardware and software regularly. The most secure, stable software updates provided by reliable sources will be promptly applied to Vendor's systems to fix software bugs and cover security holes.

5. **Data Retention Policy**. Vendor has, and shall maintain and periodically review and update, a written data and records management policy for meeting legal and business data archival requirements. Among other things, Vendor's data retention policy outlines the retention period for each data type, including any sensitive data, DDPA Confidential Information, Personally Identifiable Information, and Protected Health Information.

6. **Data Encryption**. Vendor has implemented, and will maintain, industry-standards technological solutions to effectively encrypt data in transit and at rest. All DDCO's sensitive data at the file and database levels, including backups and logs, and files stored on the external storage devices, will be encrypted using security algorithms that comply with Vendor's encryption policy. Additionally, Vendor will encrypt all sensitive data in transit, whether in the local area network or on the internet.

7. **Log Security**. Vendor will at all times protect logging facilities and log information against tampering and unauthorized access. Additionally, Vendor will allocate enough storage capacity for the log file to avoid being exceeded, resulting in either the failure to record events or overwriting past recorded events.

8. **Network Segregation**. Vendor has implemented, and will maintain, a process to separate critical network elements from the internet and other less sensitive networks and control traffic flow between various subnets based on granular policies. In addition, Vendor must adopt physical or virtual technologies to appropriately segregate DDCO’s critical data and network from Vendor operations and Vendor’s other customers.

9. **IT Risk Management Policy**. Vendor has implemented, and shall maintain, a comprehensive IT risk management policy to govern how its employees and agents use and interact with data and technology by identifying information and technology assets and assessing potential risks. Vendor will allocate the required budget to maintain the IT risk within an acceptable risk threshold.

10. **Awareness, Training, and Education**. Vendor has implemented, and will maintain, an effective procedure to educate its staff, third-party vendors, and anyone else with access to Vendor's systems, including customer resources and data, with up-to-date security knowledge and best practices tailored to the staff job function on a periodic basis, not less frequently than annually. In addition, the training content will be regularly reviewed and updated with new topics as needed to maintain consistency with industry standards. The training program will require personnel to acknowledge they have received and understand the content being delivered.

11. **Background Checks**. Vendor has implemented, and will maintain, a process to verify that an individual with access to Vendor's systems and data is who they claim to be. Vendor will check and confirm the validity of all job candidates' criminal records, education, employment history, and other activities from their past before offering any job to a candidate. If needed, the process will be repeated periodically during staff employment, particularly for those individuals dealing with customers' sensitive data.

12. **Business Continuity and Disaster Recovery:** Vendor has, and will maintain, documented Business Continuity and Disaster Recovery plans. Such plans shall be reviewed, tested and updated regularly.

13. **Incident Responsibilities**. Vendor has, and will maintain, an outline of management responsibilities and procedures to ensure a quick, effective and orderly response to information security incidents, including logging, monitoring, detecting, handling forensic evidence, and analyzing information security incidents. Additionally, Vendor will allocate competent personnel to handle information security incidents. If Vendor becomes aware of any actual known cyber incident or security breach that may have affected DDCO's information stored on Vendor's systems, Vendor must notify DDCO within 48 hours.

14. **Penetration Test**. Vendor will run penetration testing annually by independent experts contracted for this purpose. Vendor will promptly address the potential vulnerabilities with prioritization based on severity and keep its IT risk at the acceptable level defined by Vendor's risk management policy. Additionally, Vendor will share the report with DDCO upon request.

15. **Email Security**. Vendor has implemented, and will maintain, an anti-malware and security solution for all on-premises and cloud email systems to protect sensitive data in email messages from spam, phishing, business email compromise, malware delivery, system takeover and other types of email security threats.

16. **Malware**. Vendor agrees to use industry accepted practices to ensure that any data transmitted to or received by DDCO does not contain any malicious code, viruses, worms, Trojan horses, attacker tools or programs that could compromise the confidentiality, integrity, or availability of data, applications, or services.

17. **Third Party Security Management**. Vendor has, and will maintain and periodically review and update, a documented third-party risk management framework to maintain and implement policies and procedures for managing Vendor's service providers including proper due diligence prior to engagement and ongoing monitoring throughout the relationship. Should any third party used to service DDCO be found deficient in their ability to carry out the services or in violation of any privacy, security or contractual requirements agreed to by Vendor in favor of DDCO (including without limitation the services contract and this agreement), Vendor will immediately remove such third party from DDCO services, and terminate all access by such third party to DDCO's data, until the deficiency or violation is mitigated to the satisfaction of DDCO as confirmed by DDCO in writing. All such service providers will agree in writing to substantially similar compliance and security terms as those agreed to by Vendor.

18. **Security Audits.** Vendor's services to DDCO will be audited by an independent auditor annually, and the result must be shared with DDCO on an annual basis. Vendor will provide a copy of its Service Organization Controls (SOC) 2 Type 2 audit or HITRUST certification and reports (or similar security evaluation as DDCO deems reasonably sufficient) to DDCO annually.

19. **Prohibitions**. Vendor understands that it is prohibited from, and agrees not to engage in any of the following: (i) selling DDCO's data; (ii) retaining, using, or disclosing DDCO's data for a commercial purpose other than providing the Services; (iii) retaining, using, or disclosing DDCO's data in any manner that is not in furtherance of the services provided by Vendor to DDCO or expressly permitted by DDCO in writing; (iv) transmitting, offshoring, or accessing any DDCO data outside of the United States without DDCO's prior written consent; and (v) using any DDCO data in connection with, or providing any DDCO data to, any AI Technologies without DDCO's prior written consent. As used herein, "*AI Technologies*" means deep learning, machine learning, and other artificial intelligence technologies, including any and all (a) proprietary algorithms, software or systems that make use of or employ neural networks, statistical learning algorithms (like linear and logistic regression, support vector machines, random forests, k-means clustering), or reinforcement learning, and (b) proprietary embodied artificial intelligence and related hardware or equipment.

20. **Insurance Coverage**. Vendor has, and shall maintain, appropriate insurance coverage appropriate to the nature of its business, including cyber liability insurance with coverage.

21. **Additional Agreements**. Upon DDCO's request, Vendor will provide DDCO with copies of its policies, certifications, and all other information reasonably necessary to demonstrate that its operations and controls are compliant with contractual requirements as set forth in the services contract and herein. This may include but is not limited to an annual attestation. Cooperation shall be timely.

22. **Right to Audit**. Upon at least thirty (30) calendar days prior written notice and in a manner which does not unreasonably interfere with Vendor's business operations, Vendor agrees to grant DDCO or, upon DDCO's election, a third party on DDCO's behalf, permission to perform an assessment, audit, examination or review (in person or remotely, in DDCO's discretion) of all controls in Vendor's physical and virtual environment concerning all DDCO data being handled or services being provided to DDCO by Vendor. Vendor shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports DDCO data.

23. **Corrective Actions**: Vendor agrees to comply timely and fully with any mutually agreed upon Corrective Action Plans and mitigation efforts.

[Attestation Signature Page Follows]

By my signature below, I hereby certify to DDCO that my organization is fully compliant with items 1-23 as listed in this Attestation, except as specifically indicated below. I also certify that my responses to the enclosed Questionnaires are true, correct and complete. I understand that DDCO is relying on these representations and warranties, and the truth of my responses.

Organization Name:	
Name of Person Completing Attestation:	
Title of Person Completing Attestation:	
Signature:	
Date:	
Exceptions to Attestations: ***Indicate any exceptions by reference to the Item Number or confirm NONE.***	