Exhibit C
HEALTH CARE PLAN CONSULTING AND MANAGEMENT SERVICES AGREEMENT FOR PREMIUM ASSISTANCE PROGRAM

DATA AND INFORMATION SECURITY ADDENDUM

THIS DATA AND INFORMATION SECURITY ADDENDUM ("Addendum") forms part of that certain [*insert the name of the agreement*] ("Agreement") made by and between [PLACEHOLDER FOR VENDOR NAME][PLACEHOLDER FOR LEGAL ENTITY TYPE AND JURISDICTION OF FORMATION] ("**Consultant**"), whose principal place of business is [PLACEHOLDER FOR PRINCIPAL PLACE OF BUSINESS] and the Commonwealth of Pennsylvania, Public School Employees' Retirement Board ("**Board**"), whose principal place of business is 5 North 5th Street, Harrisburg, Pennsylvania 17101 and sets forth additional terms and conditions with respect to data and information security applicable to the Agreement.

RECITALS:

WHEREAS, Board and Consultant acknowledge that in relation to the provision of services under the Agreement for the [Health Options Program][Premium Assistance Program], the Agreement will or may require (i) Board to disclose certain data and information to Consultant, (ii) Consultant to accept, collect and/or use that data and information and (iii) Consultant to create data and information; and

WHEREAS, Board and Consultant desire to agree to protect and provide for the privacy and confidentiality of all such data and information.

NOW THEREFORE, in consideration of the foregoing recitals, which are incorporated herein, and the mutual promises and undertakings hereinafter set forth, and the exchange of data and information pursuant to the Agreement and this Addendum, the parties hereto agree as follows:

1. Definitions. As used in this Addendum:

(a) "Act" means the Breach of Personal Information Notification Act, Act of Dec. 22, 2005, P.L. 474, No. 94, 73 P.S. Section 2301, et. seq., as amended and enacted in the Commonwealth of Pennsylvania, including as amended by the Act of Nov. 3, 2022, P.L.2139, No. 151.

(b) "Applicable Standards" has the meaning specified in Section 2 (a) hereof.

(c) "Authorized Person" means a Consultant's employee, Consultant and any other individual or entity acting for Consultant who has (i) Board authorization and (ii) a specific need for access to Board Confidential Information to perform Consultant's services for Board. Consultant shall be deemed in control of all Authorized Persons.

(d) "Cloud Computing Services" means any computing service managed infrastructure regardless of deployment model (public, private, or hybrid) or type, such as, but not limited to, software-as-a-service (SaaS) for web-based applications, infrastructure-as-a-service (IaaS) for Internet-based access to storage and computing power, or platform-as-a-service (PaaS) that gives developers the tools to build and host Web applications, that is procured through and hosted by or within a third-party vendor, licensor, contractor, or supplier ("Service Organization") or its subcontractor(s) (commonly referred to as "Subservice Organizations"). This term includes

solutions deployed through traditional hosting methods and without the use of NIST Cloud capabilities (i.e., rapid elasticity, resource pooling, measured service, broad network access, and on demand self-service).

(e) "Cloud Use Case Review" means an established process to ensure the procurement and/or implementation of any Cloud Computing Service is aligned with Board overall business and intellectual technology vision, strategy, goals, and policies. This term includes representation and review from all domains to pro-actively identify, manage, and mitigate risk, if any, with the Cloud Computing Service being considered. The foregoing process requires that the Service Organization (third-party vendor, licensor, contractor, or supplier), must complete the Cloud Services Requirements (CSR) document provided by Board that is specific to the Cloud Computing Service being considered. Any procurement or use of a Cloud Computing Service requires an approved cloud use case.

(f) "CONUS" means any state in the Continental United States and Hawaii.

(g) "Documentation" means all documentation related to the Services, including, if applicable, a SOW.

(h) "ISP" has the meaning specified in Section 3 (a) hereof.

(i) "Industry Standards" means any of the following: (i) National Institute of Standards and Technology (NIST) 800 Series; (ii) NIST Cybersecurity Framework; and (iii) ISO 27001/2, the successor thereto or their generally recognized equivalents.

(j) "Multi-Factor Authentication" means the use of two or more of the authentication methods listed below. Two-factor employs two of the methods. Three-factor employs one each of all three methods:

(i) something you know (e.g. PIN, password, shared information);
(ii) something you possess (e.g. token, smart card, digital certificate); and
(iii) something you are (biometrics - e.g. fingerprint, voice, iris, face

(k) "Board Confidential Information" means Board Data that is not Public Data, including information containing personally identifiable information (commonly referred to as "PII"), "personal information" as defined in the Act, protected health information (commonly referred to as "PHI"), and electronic protected health information (commonly referred to as "ePHI") as defined in regulations issued by the United States Department of Health and Human Services, investment portfolio information and trade secrets. Trade secrets include limited partnership agreements, side letters, private placement memoranda and similar information.

(l) "Board Data" means any data or information that Consultant creates, obtains, accesses, receives from Board or on behalf of the [Health Options Program] [Premium Assistance Program], hosts or uses in the course of its performance of the Agreement.

(m)"Public Data" means any specific data or information, regardless of form or format, that Board has actively and intentionally disclosed, disseminated, or made available to the public.

(n) "Security Breach" has the meaning specified in Section 4 (b)(i) hereof.

(o) "Services" means the services described in the Agreement, and if applicable, any SOW.

(p) "SOW" means a statement of work made in relation to Services.

2. Data Security.

(a) Compliance. Consultant shall comply with and ensure that Services are provided under the Agreement in compliance with the requirements set forth in the following subparagraphs (i), (ii) and (iii) (individually and collectively referred to herein as the "Applicable Standards"):

(i) the Information Technology ("IT") standards and policies issued by the Commonwealth of Pennsylvania Governor's Office of Administration, Office for Information Technology (OA/OIT), as amended or restated and successor standard and policy (located at: http://www.oa.pa.gov/Policies/Pages/itp.aspx, and any replacement or successor site (referred to herein as the "COPA IT Site" and the standards and policies thereon the "COPA IT Standards"), including the accessibility standards set out in IT Bulletin ACC001, IT Accessibility Policy[1];

(ii) any applicable laws or regulations including:

(A) CJIS and CHRIA for criminal history data;
(B) HIPAA for health-related data;
(C) IRS Pub 1075 and SSA for federal protected data;
(D) PCI-DSS for financial data; and
(E) The Act;

(iii) Industry Standards (as defined above in Section 1(h)).

(b) Data Protection. To the extent that Consultant's obligations under the Agreement involve creating, accessing, transmitting, maintaining, accepting, hosting or using Board Data, Consultant shall preserve the confidentiality, integrity and availability of Board Data by implementing and maintaining administrative, technical and physical controls that conform to Applicable Standards. Consultant shall implement security controls that provide a level of security consistent with accepted information security standards which are commensurate with the sensitivity of the Board Data to be protected.

(c) Data Use and Access. Consultant shall use Board Data only and exclusively to support the performance of Services and not for any other purpose. With the exception of Public Data, absent Board prior written consent or as required by law, Consultant shall not disclose to or allow access to Board Data by any person, other than an Authorized Person in connection with the performance of Services and Board authorized employees and agents who have a need to know to perform their services for Board. If such disclosure is required by law, Consultant shall notify Board in writing before such disclosure, unless such notification is prohibited by law.

(d) Access to Board Specific Systems, Data and Services. Consultant shall limit

[1] The COPA IT Site includes Information Technology Policy, Security Policy Requirements for Third Party Vendors, Number OPD-SECOOOB. OPD-SEC000B is useful in navigating the COPA IT Standards.

access to Board-specific systems, data and services, and provide access only, to Authorized Persons located within CONUS.

(e) Data Hosting. Consultant shall only host, store, or backup Board Data in physical locations within the CONUS.

(f) Multi-Factor Authentication. For services or applications exposed to the Internet, where sensitive data or information is stored, accessed, processed or transmitted, Consultant shall provide Multi-Factor Authentication for user authentication to the web application via workstation and mobile browsers. If a service is provided via mobile application, Consultant shall cause that application to be protected by Multi-Factor Authentication.

(g) Data Backup. If appropriate to protect the integrity and availability of Board Data in accordance with accepted industry practice, Consultant shall maintain (and cause any third-party hosting company that it uses to maintain) a means to backup and recover Board Data if that Board Data is lost, corrupted or destroyed. Consultant shall store backups offline to prevent modification or encryption by ransomware or other malicious software. Board shall have the right to establish backup security for Board Data and to keep backup Board Data and Board Data files in its possession or control in Board sole discretion.

(h) Return of Board Data. Upon Board request, Consultant shall ensure that Board can retrieve Board Data in the event Consultant is unable to continue providing Services for any reason or as a result of the termination of the Agreement. In the event of a termination and upon Board request, Consultant shall provide Board Data in a mutually acceptable format.

(i) Effect of Termination on Board Data Retention. Upon the first to occur of the termination of the Agreement for any reason or notice of such termination having been given, the provisions of this Subparagraph shall apply notwithstanding anything contained in the Agreement or this Addendum to the contrary. Unless otherwise directed by Board in writing, Consultant shall maintain Board Data and continue to extend the protections of the Agreement and this Addendum to such Board Data for a period of six (6) months at which point it shall return, and then upon Board written direction destroy, all Board Data received from Board (or created or received by Consultant on behalf of Board) regardless of form, and shall retain no copies of Board Data. Consultant shall certify in writing to Board that these actions have been completed within thirty (30) days after receipt of Board direction to destroy. If return or destruction of Board Data is not feasible, Consultant shall (i) promptly inform Board that the return or destruction, as applicable, is not feasible, (ii) continue to extend the protections of the Agreement and this Addendum to such Board Data and (iii) limit further use of Board Data to those purposes that make the return or destruction of Board Data infeasible.

(j) Destruction of Board Data. Subject to Subparagraph (i) above, Consultant shall erase, destroy, and/or render unrecoverable all Board Data in Consultant's possession or control that is no longer required for the performance of Services. Upon Board request, Consultant shall certify in writing that these actions have been completed within seven (7) days of Board request.

3. Consultant Security.

(a) Information Security Program. Consultant represents, acknowledges and agrees that Consultant has in place and will continue to maintain a formal information security program ("ISP") with written policies and procedures consistent with Industry Standards and reasonably

designed to protect the confidentiality and integrity of Board Data when such Board Data is in the possession or control of Consultant. The ISP shall include administrative, technical, and physical safeguards. The safeguards shall appropriately: (i) relate to the type of data and information concerned, (ii) be reasonably designed to maintain the integrity, confidentiality, and availability of the data and information; (iii) protect against anticipated threats or hazards to the security or integrity of the data and information; (iv) protect against unauthorized access to or use of the data and information that could result in substantial harm or inconvenience to Board; (v) provide for secure disposal of the data and information; and (vi) prescribe actions to be taken in the event that a security incident occurs or is suspected to have occurred.

(b) Consultant Personnel. Consultant hereby agrees that it shall only use Authorized Persons who are highly qualified in performing under the Agreement and have passed a background check. Consultant shall use the background check required under the COPA IT Standards for individuals described therein and for all others, a background check that is recognized under industry standards as appropriate to address the security concerns that apply to the specific individual and the services to be provided by the individual under the Agreement.

(c) Acceptance of Acceptable Use Policy. Consultant shall ensure that all Consultant personnel, including employees and Consultants, who access or could access Board network as a part of performing under the Agreement, have agreed to Board Acceptable Use Policy as found in Management Directive 205.34, as it may be amended from time to time and any successor thereto (the current version being located at: https://www.oa.pa.gov/Policies/md/Documents/205_34.pdf) before such access.

(d) Security Awareness Training. Consultant shall ensure that its employees, agents, contractors, subcontractors are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with Applicable Standards.

4. Documentation and Required Notification.

(a) Security Incident Handling. As part of the ISP, Consultant represents, acknowledges and agrees that Consultant has in place and will continue to maintain a documented security incident management process. The security incident management process shall: (i) provide for the timely detection of security incidents and responses thereto; and (ii) require the recordation of the applicable facts of each security incident and responses thereto, including the application or non-application of the security incident management process, escalation procedures and the responsibilities of each affected party.

(b) Notice to Board and Response of Security Breach.

(i) Consultant shall notify by telephone Board Chief Information Security Officer at (717) 720-4699 and Deputy Executive Director for Administration at (717) 720-4825 and by e-mail Board at RA-PSISO@pa.gov:

(A) as soon as reasonably practicable and in any event within twenty-four (24) hours of first having knowledge or reasonable suspicion of:

(1) an unauthorized access or acquisition of Board Data;

(2) a loss, alteration, theft or corruption of Board Data;

(3) any event that creates a substantial risk to the confidentiality, integrity or availability of Board Data;

(4) a breach of any of Consultant's security obligations under this Addendum;

(5) the occurrence of an event described in clauses (1), (2), or (3) (without reference to Board Data) involving data or information other than Board Data if Consultant has not reasonably determined that such event will not be an event described in clause (1), (2) or (3); or

(6) any other event requiring notification under applicable law, including the Act (each of the events described in clauses (1) – (5) and this clause (6)) is hereinafter referred to as a "Security Breach"), and

(B) within ten (10) days of having a suspicion that a Security Breach may have occurred unless after investigation appropriate to the suspicion during such ten (10) day period, Consultant has reasonably concluded that no Security Breach occurred.

Board shall provide updated contact information to Consultant within ten (10) business days of any change to the Board contact information set forth in this Subparagraph (i).

(ii) In the event of a Security Breach and as soon as practicable after first having knowledge of the Security Breach, Consultant shall:

(A) preserve forensic evidence and eliminate the cause of the risk or breach within Consultant's reasonable control; and

(B) undertake a thorough forensic investigation of any compromise or improper use and provide to Board all information necessary to enable Board to fully understand the nature and extent of the compromise or improper use to the extent known.

(iii) To the extent that the Security Breach is attributable to the actions or failure to act by Consultant or Authorized Persons or breach of this Addendum by Consultant or Authorized Persons, Consultant shall: (A) be liable for the cost of informing all such affected individuals in accordance with applicable law and (B) indemnify, hold harmless and defend Board and its trustees, officers, and employees from and against any and all liabilities, claims, damages, losses, expenses, costs or other harm related to such Security Breach. As used herein, an "affected individual" shall include any individual who would be entitled to notice under the Act, if such individual was a resident of the Commonwealth of Pennsylvania. Consultant hereby agrees that it is doing business in the Commonwealth of Pennsylvania.

(c) Security Incident Investigations. Consultant hereby agrees to cooperate with Board in investigating a security incident, as declared by Board in Board sole discretion, and provide the names and contact information, of at least two (2) security contacts who shall respond to Board in a timely manner, dependent on criticality, in the event that Board must investigate a security incident. The current security contacts are:

Contact Names: _____ _____
Phone Numbers: _____ _____
Email Addresses: _____ _____

Consultant shall provide updated contact information to Board within ten (10) business days of any change to the currently applicable security contact information provided to Board.

5. Maintenance of Safeguards.

(a) Consultant shall maintain and follow Applicable Standards with respect to any of Board' Confidential Information in Consultant's possession or control and protect such information against any loss, alteration, theft or corruption.

(b) At Board request, Consultant shall provide Board with copies of its information security policies, processes, and procedures. Consultant shall notify Board within ten (10) business days of any changes to its policies, processes or procedures that relate to the security of Board Data in Consultant's possession or control.

6. Information Security Audit.

(a) Board Right to Review ISP and Onsite Assessment. Board shall have the right to review Consultant's ISP at any time that Consultant is subject to the terms of this Addendum. During the performance of the Services, on an ongoing basis annually and immediately in the event of a Security Breach, Board, including its professional advisors and auditors, at its own expense, shall be entitled to perform, or to have performed, an on-site assessment of Consultant's ISP. Consultant hereby agrees that the assessment scope will address the services provided to Board, including related people, process and technology.

(b) System and Organization Controls (SOC) Reporting. Board shall have the right to review Consultant's ISP through Consultant's annual submission to Board of its current SOC report(s) as required to be provided under this Addendum. Consultants shall submit: (i) a SOC 1 Type II report, if hosting financial information; (ii) a SOC 2 Type II report, if hosting, handling or processing Board Confidential Information; and (iii) a SOC for Cybersecurity Report if any of the following conditions exist: (A) reoccurring findings in SOC 1-Type II or SOC 2-Type II reports; (B) a cybersecurity incident or security breach has occurred; (C) cybersecurity incidents or breaches are not being detected, prevented, reported, and/or mitigated in a timely manner (as determined by Board); (D) cybersecurity incidents or breaches are not being properly managed by Consultant; (E) uncertainty that Consultant has an effective cybersecurity risk management program; (F) Consultant has been engaged in a merger or acquisition during the term of the Agreement; or (G) Consultant has restructured its service offerings and/or business model. Any report required to be provided hereunder shall document an assessment conducted by a qualified, independent third party. The assessment scope must address the services provided to Board, including related people, process and technology.

(c) Assessment Questionnaire. Annually, Consultant hereby agrees to complete, within forty-five (45 days) of receipt of Board request, an assessment questionnaire provided by Board regarding Consultant's ISP, including artifacts for a subset of controls.

7. Software Development Security. In the event that Consultant conducts

application software development for Board, Consultant shall: (a) either make source codes available for review by Board or shall conduct source code scanning using a commercial security tool; (b) cause scans to be conducted annually and at any time significant code changes are made; (c) make scan reports available to Board within two (2) weeks of execution; (d) disclose remediation timelines for high, medium and low risk security code defects; and (e) perform scans before code is implemented in production. Consultant hereby agrees that high risk security code defects may not be implemented in production without written approval from either Board Executive Director or a Deputy Executive Director.

8. Cloud Computing Services. Consultants shall meet the following requirements to the extent that Consultant provides Cloud Computing Services:

(a) Cloud Use Case (CUC) Review. Consultant shall coordinate with Board to complete the Cloud Services Requirements (CSR) as part of the CUC review process. Consultant hereby agrees that CUC review and approval is required prior to procurement or use of any Cloud Computing Service.

(b) Monitoring and Audit Logging. Consultant shall ensure system monitoring and security audit logging is enabled and accessible to the Board Chief Information Security Officer or designee. Consultant shall:(i) provide monitoring (in addition, Board recommends verbose logging); (ii) provide software with ability to correlate events and create security alerts; and (iii) maintain reports that are easily accessible and in a readable format online for a minimum of 90 days and archived for a minimum of one (1) year.

(c) Data Segmentation / Boundary Protection. Consultant shall provide a network/architecture diagram showing what technical controls are performing the network segmentation. If solution spans more than one hosting environment (such as integration to Board managed environments, or across multiple hosting providers), Consultant shall provide details on what solution components and data are deployed in which environment and (i) include border gateway, perimeter and/or network firewall, web application firewall, VPN tunnels, security zone access as applicable to the solution; (ii) describe data encryption methods at rest and in transit across environments; and (iii) include the direction of connectivity (specify whether initiated inbound, outbound, or both) and specifications for API calls, protocols, etc. Consultant shall describe how data segregation (physically or logically) of Board data from non-Board data is guaranteed and maintain the diagram as long as Consultant is subject to the terms of this Addendum and provide updates if changes occur.

(d) Exploit and Malware Protection. Consultant shall provide security controls required to identify attacks, identify changes to files, protect against malware, protect user web services, data loss prevention (DLP) and to perform forensic analysis. Consultant shall provide: (i) file Integrity Monitoring Controls; (ii) Anti-Malware and Antivirus Controls; (iii) Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) Controls; (iv) Data Loss Prevention (DLP) Controls; (v) Forensic Controls; and (vi) Advanced Persistent Threat (APT) Controls.

(e) Encryption. Consultant shall enable industry standard strong encryption for all records involved with Software as a Service (SaaS) cloud services. Consultant shall provide technical controls with strong encryption to protect Data in Transit and Data at Rest.

(f) Identity & Access Management. Consultant shall provide technical controls for

authenticating users, provisioning and deprovisioning users, identity interaction and nonrepudiation needs for administrators, internet users and internal users. Multi-Factor Authentication (MFA) shall be implemented by the Consultant for users requiring direct access to any Board application from outside the Commonwealth of Pennsylvania network. Where possible, the Commonwealth of Pennsylvania's MFA solution shall be utilized."

(g) Vulnerability Assessment. Consultant shall ensure all cloud applications are securely coded, vetted and scanned. Consultant shall: (i) conduct a third-party independent vulnerability assessment annually or sooner if due to compliance regulations or other requirements, or upon a major change to the solution; (ii) provide vulnerability assessment results to Board on an annual basis during the period the Consultant is subject to the terms of this Addendum; (iii) identify and validate vulnerabilities required for remediation; and iv) ensure patching is up to date.

(h) Data Protection / Recovery. Upon Board request, Consultant shall provide a business continuity plan that addresses:

(i) Data/Database Recovery;
(ii) Application Recovery;
(iii) Operating System Recovery; and
(iv) Infrastructure Recovery.

In connection therewith, Consultant shall describe:

(A) its capability to do a complete restoration in the event of a disaster;
(B) what tests are performed as part of its disaster recovery plan; and
(C) its capability to provide services during a pandemic event.

(i) Inventory. Consultant shall ensure a complete, accurate and up-to-date inventory of Board deployed resources within the cloud infrastructure and must be made available for review by Board upon request

9. Compliance with Applicable Federal, State and Local Laws. Consultant shall comply with all applicable federal, state, and local laws concerning data protection and privacy when handling Board Data.

10. Enforcing Compliance. Consultant shall enforce and be responsible for compliance by all its personnel and contractors with the provisions of this Addendum and all other confidentiality obligations owed to Board.

11. Accommodation of Additional Protections. Consultant hereby agrees to comply with such additional protections as Board shall reasonably request.

12. Termination. If Board determines that the Consultant has breached any provision of this Addendum, such breach shall constitute a material breach of the Agreement and shall provide grounds for immediate termination of the Agreement by Board pursuant to the Agreement.

13. Indemnification. Consultant hereby agrees to indemnify, hold harmless and defend Board from and against all claims, losses, liabilities, damages, judgments, costs and other

expenses, including Board's costs and attorney fees, incurred as a result of, or arising directly or indirectly out of or in connection with Consultant's failure to meet any of its obligations under this Addendum; and any claims, demands, awards, judgments, actions and proceedings made by any person or organization arising out of or in any way connected with Consultant's performance under this Addendum. Consultant hereby agrees that any limitations on Consultant's liability, regardless of conflicting language elsewhere in the Agreement, shall not apply to claims related to Consultant's breach of this Addendum.

14. Intellectual Property Infringement Indemnification. Consultant hereby agrees to indemnify, defend and hold Board harmless from any and all claims brought against Board alleging that the Services and/or Documentation or Board use of the Services and/or Documentation constitutes a misappropriation or infringement of intellectual property ("IP") of any third party. Consultant hereby agrees to be responsible for all costs or expenses, to include reasonable attorneys' fees awarded or resulting from any claim. Board shall, after receiving notice of a claim, advise Consultant of such notification. Limitations on Consultant's liability, regardless of conflicting language elsewhere in any Agreement, shall not apply to claims related to Consultant's misappropriation or infringement of another's intellectual property.

15. Consultant Liability Insurance. Consultant shall procure, and maintain for the duration of the Agreement and for such other period of time that Consultant is obligated under this Addendum to protect Board Data and Board system and services, insurance against claims and damages which may arise from or in connection with the performance of its work to include IP infringement and privacy or data breaches coverage. Coverage shall have limits of no less than $5,000,000.00 per occurrence and $10,000,000.00 aggregate.

16. Survival; Order of Precedence. Notwithstanding anything contained herein or the Agreement to the contrary, Consultant hereby acknowledges and agrees that the obligations imposed on Consultant under this Addendum shall (i) apply during the term of the Agreement, (ii) survive the termination of the Agreement for such other period of time as may be necessary to effectuate the intended purpose of protecting Board Data and Board systems and services, and (iii) in the event of any conflict with any term of the Agreement, the terms of this Addendum shall govern and take precedence.

17. Entire Agreement. The Agreement, including any exhibits and/or schedules thereto, and this Addendum contain the entire understanding of the parties hereto with respect to the subject matter hereof and supersedes all prior agreements, oral or written, and all other communications between the parties hereto relating to such subject matter.

18. Notices. Except as provided in Section 4(b)(i) above, as to matters requiring notice covered by this Addendum, Board and Consultant agree that the notice provisions in the Agreement shall apply.

19. Miscellaneous. The section headings contained in this Addendum are for convenience of reference purposes only and shall not affect the meaning or interpretation of this Addendum. If a conflict occurs between any obligation imposed on Consultant under this Addendum or the Agreement, the stricter requirement shall apply. Wherever from the context it appears appropriate, each term stated in either the singular or the plural shall include the singular and the plural. Usage of the term "including" in this Addendum shall be deemed to be followed by the phrase "without limitation" and shall be regarded as a reference to nonexclusive and non-characterizing illustrations. No waiver of any provision hereof or of any right or remedy

hereunder shall be effective unless in writing and signed by the party against whom such waiver is sought to be enforced. A waiver is effective only in the specific instance and for the specific purpose for which it is given and shall not be deemed a waiver of any subsequent breach or default. No delay in exercising, failure to exercise, course of dealing with respect to, or partial exercise of any right or remedy shall constitute a waiver of an other right or remedy, or future exercise thereof. This Addendum may be executed in any number of counterparts. Separate counterparts, each of which when so executed and delivered, shall be deemed to be an original and all of which taken together shall constitute but one and the same instrument. PDF copies of signatures and electronic signatures shall be deemed originals. Consultant may not assign any of its rights, duties or obligations under this Addendum without Board prior written consent. This Addendum and the obligations hereunder shall be interpreted, construed, and enforced in accordance with the laws of the Commonwealth of Pennsylvania, without reference to any conflict of laws rules. If any term, covenant, or condition of this Addendum or the application thereof to any person or circumstance shall, to any extent, be invalid or unenforceable, the remainder of this Addendum, or the application of such term, covenant, or condition to persons or circumstances other than to those to which is held invalid or unenforceable, shall not be affected thereby, and each term, covenant, or condition of this Addendum shall be valid and be enforced to the fullest extent permitted by law. Except to the extent that Board has agreed otherwise in writing, Board and the Consultant hereby acknowledge and agree that Board has all right, title and interest in and to Board Data.