

HIPAA Business Associate Agreement

Association of Washington Cities Employee Benefit Trust

This Business Associate Agreement (“Agreement” or “BAA”) is entered into between [insert name of Business Associate] (“Business Associate”) and the Association of Washington Cities Employee Benefit Trust (“Plan Sponsor”) for and on behalf of the health plans provided under the Health Care Program (collectively, the “Plan” and HIPAA Covered Entity) that are maintained by the Plan Sponsor. The Parties enter into this Agreement to permit Business Associate to create, receive, maintain, and transmit PHI (including EPHI) for and on behalf of the Plan in connection with the services provided by Business Associate pursuant to such other agreement (and any amendments thereto) entered into between the parties (“Other Agreement”). This Agreement shall be effective as of [insert effective date] (the “Effective Date”).

1. Definitions

Capitalized terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in final regulations relating to privacy and security of individually identifiable health information at 45 CFR parts 160, 162, and 164 implementing the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), as amended from time to time.

- (a) **Agent.** “Agent” means an agent as used and defined under the HIPAA Regulations and federal common law.
- (b) **Breach Notification Rule.** “Breach Notification Rule” means the final regulatory provisions set forth at 45 CFR Parts 160 and 164, Subparts A and D.
- (c) **Electronic Protected Health Information or EPHI.** “Electronic Protected Health Information” or “EPHI” means PHI having the same meaning as the term “electronic protected health information” in 45 C.F.R. § 160.103, limited to the EPHI created, received, maintained, or transmitted by Business Associate for or on behalf of the Plan.
- (d) **Electronic Transactions Rule.** “Electronic Transactions Rule” means the federal regulations found at 45 CFR Part 162.
- (e) **HIPAA Regulations.** “HIPAA Regulations” means the Privacy Rule, the Security Rule, and the Electronic Transactions Rule.
- (f) **Information System.** “Information System” means an interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, information, data, applications, communications, and people.
- (g) **Internal Material.** “Internal Material” means Business Associate’s documented internal practices, books, and records, including policies and procedures relating to the use and disclosure of PHI created, received, maintained, or transmitted by Business Associate for or on behalf of the Plan or Plan Sponsor.
- (h) **Other Agreement.** “Other Agreement” means any and all other agreements, if any, entered into between the Plan or Plan Sponsor and Business Associate relating to services of Business Associate concerning the Plan which are in effect as of the Effective Date of this Agreement or which come into effect after the Effective Date of this Agreement.
- (i) **PHI.** PHI means “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, limited to the information created, received, maintained, or transmitted by Business Associate for or on behalf of the Plan or Plan Sponsor.
- (j) **Privacy Rule.** “Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- (k) **Security Rule.** “Security Rule” means the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160 and 164, Subparts A and C.
- (l) **Subcontractor.** “Subcontractor” shall have the same meaning as the term “Subcontractor” in 45 C.F.R. § 160.103, limited to Subcontractors that create, use, transmit, access, disclose, receive, or maintain PHI of the Plan or Plan Sponsor.
- (m) **Unsecured PHI.** “Unsecured PHI” shall have the same meaning as the term “unsecured protected health information” in 45 C.F.R. § 164.402, limited to Unsecured PHI of the Plan or Plan Sponsor

that is created, used, transmitted, disclosed, received, or maintained by Business Associate or its Agents or Subcontractors.

2. Permitted Uses and Disclosures by Business Associate

Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform one or more functions, activities, or services for, or on behalf of, the Plan as specified in the Other Agreement, provided that such use or disclosure would not violate the HIPAA Privacy Rule if done by the Plan or the minimum necessary policies and procedures of the Plan. Business Associate may disclose PHI to, or receive PHI from, another business associate of the Plan to the extent directed to do so by the Plan or the Plan Sponsor. For purposes of this Agreement, the terms “use” or “disclose” include the receipt, creation, transmission, or maintenance of PHI of the Plan to the extent allowed by the HIPAA Regulations.

Additionally, Business Associate may use and disclose PHI received by Business Associate for the proper management and administration of Business Associate or to carry out the legal obligations of Business Associate, but only: (a) if the disclosure is Required by Law; or (b) if Business Associate receives reasonable assurances from the third party to whom the PHI is disclosed that: (i) the PHI will be held confidentially by the third party; (ii) the PHI will be used or further disclosed by the third party only as required by law or for the purpose for which it was disclosed to the third party; and (iii) the third party agrees to notify Business Associate of any Breaches of which the third party becomes aware.

3. Obligations and Activities of Business Associate

- (a) Business Associate agrees to not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.
- (b) Business Associate agrees to (i) use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement and to appropriately protect confidentiality, integrity, and availability of EPHI; and (ii) to comply, where applicable, with the Security Rule with respect to EPHI.
- (c) Upon written request from the Plan or Plan Sponsor, Business Associate shall produce such documentation as is reasonably necessary to demonstrate Business Associate's implementation of policies, procedures, and systems that relate to safeguarding PHI to determine whether Business Associate meets the terms of this Agreement, the Other Agreement, and applicable law including HIPAA. Business Associate shall mitigate and prevent, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate, or one of its Subcontractors or Agents in violation of this Agreement, the HIPAA regulations, or other applicable law.
- (d) Business Associate agrees to report to the Plan in writing any use, disclosure, access, or acquisition of the PHI not permitted under this Agreement by Business Associate, a Subcontractor of Business Associate, or an Agent of Business Associate, within five (5) business days of such unauthorized use, disclosure, access, or acquisition. Business Associate agrees to report to the Plan and to the Plan Sponsor any successful Security Incident of which Business Associate becomes aware. Further, Business Associate shall update the Plan with newly discovered information related to any successful Security Incident on a mutually agreed upon schedule until the incident is resolved.
- (e) The Parties acknowledge and agree that unsuccessful Security Incidents include but are not limited to (i) unsuccessful attempts to penetrate computer networks or assets maintained by Business Associate; (ii) immaterial incidents such as “pinging” or “denial of services” attacks, port scans, and unsuccessful log-on attempts; and (iii) any combination of the foregoing, provided no such incident results in unauthorized use, disclosure, access, or acquisition of PHI. The Parties further agree that this Paragraph hereby constitutes notice to the Plan and Plan Sponsor of the ongoing occurrence of unsuccessful Security Incidents, and no further notification is required regarding unsuccessful Security Incidents. Notwithstanding the foregoing, Business Associate agrees to report to the Plan's Privacy Officer in a reasonable manner and upon request, but not more than once in any 12-month period, aggregate information on unsuccessful Security Incidents experienced by Business Associate.

- (f) Business Associate will ensure that any Agent or Subcontractor of Business Associate that creates, receives, maintains, or transmits PHI of the Plan for or on behalf of Business Associate has executed a Business Associate Agreement agreeing to comply with the Security Rule and the same or substantially similar restrictions and conditions that apply through this Agreement to Business Associate with respect to such PHI. Business Associate will provide, upon written request by the Plan Sponsor, a list of any such Agents or Subcontractors of Business Associate. Business Associate will ensure only those who reasonably need to know such PHI in order to perform the services contemplated by the Other Agreement receive such PHI and, in such case, only the minimum amount of such PHI is disclosed as is necessary for such performance.
- (g) Business Associate agrees to provide to the Plan, or to an Individual at the plan's direction, within fifteen (15) calendar days all PHI in a Designated Record Set as necessary for the Plan to respond to an Individual's request for access to PHI pursuant to 45 CFR § 164.524. If the PHI that is maintained electronically in a Designated Record Set in the custody or control of the Business Associate or of a Subcontractor or an Agent of Business Associate, Business Associate will provide such PHI in the electronic form and format requested if it is readily producible in such form and format; if the PHI is not readily producible by Business Associate in the requested form and format, Business Associate will provide the PHI in a readable electronic form as agreed by the Business Associate and Plan.
- (h) Business Associate will document any disclosures of PHI and provide to Plan, or to an Individual at the Plan's direction, within thirty (30) calendar days after written request, information related to such disclosures as would be required for the Plan to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Business Associate shall maintain documentation of such disclosures for at least six (6) years following the date of the most recent disclosure.
- (i) Business Associate will make any amendment(s) to PHI in a Designated Record Set that the Plan directs or agrees to pursuant to 45 CFR § 164.526 at the request of the Plan or an Individual, within fifteen (15) calendar days after receipt of written instructions to do so.
- (j) Business Associate shall honor any restriction on use or disclosure of PHI or request for confidential communications as agreed to by the Plan pursuant to 45 CFR § 164.522.
- (k) Business Associate agrees to make its Internal Materials relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of the Plan available to the Plan or, at the request of the Plan, to the Secretary or other regulatory official as directed by the Plan, in a time and manner requested by the Plan or official, for the purpose of determining the Plan's or Business Associate's compliance with the HIPAA Regulations.
- (l) Business Associate agrees to implement administrative, physical, and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI that it creates, receives, maintains or transmits on behalf of the Plan as required by the Security Rule. Business Associate will ensure that any Agent and Subcontractor to whom Business Associate provides EPHI agrees to implement reasonable and appropriate administrative, physical and technical safeguards to reasonably and appropriately protect the confidentiality, integrity and availability of such EPHI. Business Associate agrees to comply with Sections 164.306, 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations with respect to all EPHI.
- (m) In conducting any electronic transaction that is subject to the Electronic Transactions Rule on behalf of the Plan, Business Associate agrees to comply with all requirements of the Electronic Transactions Rule that would apply to the Plan if the Plan were conducting the transaction itself. Business Associate agrees to ensure that any Agent or Subcontractor of Business Associate that conducts standard transactions with PHI of the Plan will comply with all of the requirements with the Electronic Transactions Rule that would apply to the Plan if the Plan were conducting the transaction itself.
- (n) Business Associate shall not disclose PHI to any member of its workforce unless Business Associate has advised such person of Business Associate's privacy and security obligations under this Agreement, including the consequences for violation of such obligations. Business Associate shall take appropriate disciplinary action against any member of its workforce who uses or discloses PHI in violation of this Agreement and applicable law.

- (o) Business Associate agrees to determine the minimum necessary type and amount of PHI required to perform its services and will comply with any regulations promulgated under HIPAA concerning minimum necessary rules.
- (p) Business Associate, following the discovery of a Breach of Unsecured PHI of the Plan, shall notify the Plan and Plan Sponsor of such breach. Business Associate shall provide initial notice without unreasonable delay, and in no case later than five (5) business days after Discovery of the Breach of Unsecured PHI by Business Associate or Discovery of the Breach of Unsecured PHI by a Subcontractor or Agent of Business Associate. Business Associate will require its Subcontractors and Agents to provide initial notice to the Plan of a Discovery of a Breach of Unsecured PHI at the same time its Subcontractors and Agents notify the Business Associate. Furthermore, without unreasonable delay and prior to any breach notification deadline that may apply under federal or state law, Business Associate shall provide the Plan with any additional information required under this Paragraph (p) in a timeframe and form as mutually agreed to by the parties.
 - (1) Notice to the Plan required by this Paragraph (p) shall include: (i) to the extent possible, the names of the individual(s) whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired, used or disclosed during the Breach; (ii) a brief description of what happened including the date of the Breach and the date of the discovery of the Breach, if known; (iii) a description of the types of Unsecured PHI that were involved in the Breach; (iv) a brief description of what Business Associate is doing or will be doing to investigate the Breach, to mitigate harm to the individual(s), and to protect against further Breaches; and (v) any other information that the Plan or Plan Sponsor determines it needs to include in notifications to the individual(s) under 45 CFR § 164.404(c).
 - (2) After receipt of notice, from any source, of a Breach involving Unsecured PHI used, disclosed, maintained, or otherwise possessed by Business Associate or a Subcontractor or Agent of Business Associate, the Plan or Plan Sponsor, exercising reasonable discretion, may delegate to Business Associate the responsibility for providing all legally required notifications to Individuals, the Secretary, state attorneys' general, the media, or others on behalf of the Plan. In the event such delegation has been made, Business Associate (1) shall provide a copy of the notification letter to be sent to Individuals and other required recipients for the Plan's review and approval prior to sending; (2) upon approval by the Plan, shall provide the notifications in accordance with the notification requirements set forth in the Breach Notification Rule and applicable state law; (3) shall pay for the reasonable and actual costs associated with those notifications, any remediation or mitigation as directed by the Plan, and the Plan's or Plan Sponsor's legal fees associated with the incident; and (4) shall provide signed, written documentation including a copy of Business Associates Breach notification risk analysis, confirming that all such requirements have been met for the Plan's records.
- (q) Business Associate shall not use or disclose genetic information of the Plan in violation of 45 C.F.R. §164.502(a)(5) or sell PHI (directly or indirectly receive remuneration in exchange for any PHI) of the Plan in violation of 45 C.F.R. §164.502(a)(5). Business Associate must obtain the required authorizations or confirm that the Plan Entity has obtained the required authorizations for any use or disclosure of PHI for Marketing, as that term is defined in 45 C.F.R. §164.501, or for fundraising communication purposes, as described in 45 C.F.R. §164.514.
- (r) To the extent that Business Associate is to carry out any of the Plan's obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that would apply to the Plan in the performance of such obligations.
- (s) Business Associate will, in its performance of the functions, activities, services, and operations specified in this Agreement, make reasonable efforts to use, to disclose, and to request only the minimum amount of PHI reasonably necessary to accomplish the intended purpose of the use, disclosure, or request, except that Business Associate will not be obligated to comply with this minimum-necessary limitation if neither Business Associate nor the Plan is required to limit its use, disclosure, or request to the minimum necessary under the HIPAA Regulations. Business Associate and the Plan acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with the HIPAA Regulations.

4. Obligations of the Plan

- (a) The Plan shall provide Business Associate with its notice of privacy practices that the Plan produces in accordance with 45 CFR § 164.520, including the limitations found in such notice, as well as any changes to such notice.
- (b) The Plan shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures.
- (c) The Plan shall notify Business Associate of any restriction to the use or disclosure of PHI that the Plan has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
- (d) The Plan shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Regulations if made by the Plan.

5. Term and Termination

- (a) **Term.** This Agreement shall be effective as of the Effective Date specified above and shall terminate on the earlier of (i) the date on which the Other Agreement(s) terminates; or (ii) the date of termination of this Agreement for cause or otherwise. Notwithstanding the foregoing, (1) the protections of this Agreement will remain in place until all of the PHI provided by the Plan to Business Associate, its Agents and Subcontractors or created or received by Business Associate, its Agents and Subcontractors on behalf of the Plan, is destroyed or returned to the Plan, or (2) if it is infeasible to return or destroy such PHI, the protections of this Agreement shall be extended to such PHI in accordance with the termination provisions in this Section 5.
- (b) **Termination for Cause.** Upon the Plan's determination that Business Associate violated a material term of this Agreement, the Plan and/or Plan Sponsor shall notify Business Associate in writing of such violation and take one of the following actions:
 - (1) **Curable Breach.** If the Plan determines that the breach or violation is curable, the Plan shall provide an opportunity for Business Associate to cure the breach or end the violation within a reasonable time period set by the Plan, which shall not exceed thirty (30) calendar days. If the breach or violation is not cured or ended within the time set by the Plan, the Plan and/or Plan Sponsor may: (i) immediately terminate this Agreement and any Other Agreement(s); or (ii) suspend performance by the Plan and/or Plan Sponsor under the Other Agreement(s) until such breach or violation is cured.
 - (2) **Incurable Breach.** If the Plan determines that the breach or violation is not curable, the Plan and/or Plan Sponsor shall immediately terminate this Agreement and any Other Agreement(s).
 - (3) **Alternative Actions.** If the Plan determines that neither a termination of the Agreement or a cure of the breach is feasible, the Plan may take other appropriate actions to remedy, correct or mitigate such breach, including reporting the violation to the Secretary.
 - (4) **Termination for Material Breach of Security Rule.** In addition to the termination for cause procedures listed above, the Plan and/or Plan Sponsor may immediately terminate this Agreement and any Other Agreement(s) if the Plan determines that Business Associate has violated a material term of this Agreement concerning the Security Rule.
- (c) **Effect of Termination.**
 - (1) Except as otherwise provided below, upon termination of this Agreement for any reason, Business Associate shall return or destroy all PHI within thirty (30) calendar days after termination of the Agreement. This provision shall also apply to PHI that is in the possession of Subcontractors or Agents of Business Associate. Business Associate shall retain no copies of the PHI.
 - (2) If Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall, within thirty (30) calendar days after termination of this Agreement, provide to the Plan written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI (including PHI held by Agents or Subcontractors of Business Associate) and limit further uses and disclosures of

such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate or its Agents or Subcontractors maintain such PHI.

- (3) With respect to PHI that is retained in accordance with this Paragraph (c), for the convenience of the Plan and Plan Sponsor and to ensure uninterrupted access to the PHI subject to this Agreement, Business Associate shall cause retention of all such PHI for a period of at least six (6) years following termination of this Agreement (the "Retention Period"). During such Retention Period, Business Associate shall continue to comply with its obligations under the HIPAA Regulations, including but not limited to the Individual rights relating to such PHI. In addition, during such Retention Period, the Plan or Plan Sponsor may request Business Associate to provide a copy of any or all such PHI of the Plan, or direct that any or all such PHI be copied and transferred to another business associate of the Plan, provided Business Associate and the Plan or Plan Sponsor mutually agree as to form and timing of any such copy or transfer of PHI. Upon conclusion of the Retention Period, Business Associate shall cause all retained PHI to be returned or destroyed in accordance with this Paragraph (c).

6. Miscellaneous

- (a) **Regulatory References.** A reference in this Agreement to a section in the HIPAA Regulations means the section as in effect or as amended, and for which compliance is required.
- (b) **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time for the Plan to comply with the requirements of the HIPAA Regulations and the Health Insurance Portability and Accountability Act, Public Law 104-191, as amended. In addition, Business Associate agrees that, as of the compliance date of any amendments to the HIPAA Regulations, it will conform its practices to comply with amended requirements applicable to Business Associate.
- (c) **Survival.** The respective rights and obligations of Business Associate under Sections 2(p), 5(c), 6(c) and 6(l) of this Agreement shall survive the termination of this Agreement.
- (d) **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Plan to comply with the HIPAA Regulations and other applicable law. The section and paragraph headings of this Agreement are for the convenience of the reader only, and are not intended to act as a limitation of the scope or meaning of the sections and paragraphs themselves.
- (e) **Relationship of Parties; No Third-Party Beneficiaries.** The relationship between the Plan or Plan Sponsor and Business Associate will solely be that of independent contractors engaged in the operation of their own respective businesses. Business Associate is not an Agent of Plan or Plan Sponsor. Subcontractors and Agents of Business Associate are not Agents of the Plan or Plan Sponsor. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Business Associate, the Plan, and the Plan Sponsor and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.
- (f) **Assignment.** This Agreement shall not be assigned or otherwise transferred by a party without the prior written consent of the other parties, which consent shall not be unreasonably withheld; provided no such consent shall be required for either party's assignment or transfer of this Agreement in connection with a sale or transfer of all or substantially all of the business or assets of the assigning party.
- (g) **Severability and Waiver.** The invalidity of any term or provision of this Agreement will not affect the validity of any other provision. Waiver by any party of strict performances of any provision of this Agreement will not be a waiver of or prejudice any party's right to require strict performance of the same provision in the future or of any other provision of this Agreement.
- (h) **Notices.** Any notices permitted or required by this Agreement will be addressed as follows or to such other address as either party may provide to the other:

If to Plan or Plan Sponsor:

Association of Washington Cities Employee Benefit Trust

Attn: [Name]

1076 Franklin Street SE

Olympia, WA 98501

[email]

If to Business Associate:

[Insert Business Associate physical/email address]

- (i) **Counterparts.** This Agreement may be executed in multiple counterparts, all of which together will constitute one agreement, even though all parties do not sign the same counterpart.
- (j) **Other Agreement(s).** Notwithstanding any provision of the Other Agreement(s) to the contrary, to the extent of any inconsistency between any Other Agreement(s) and this Agreement, the provisions of this Agreement shall prevail.
- (k) **Supersedes Prior Business Associate Agreement.** This Agreement supersedes any other Business Associate Agreement currently in effect among or between the Parties, or affiliates of the Parties, to this Agreement.
- (l) **Indemnification.** Business Associate shall indemnify, hold harmless, and defend the Plan and Plan Sponsor from and against any and all civil monetary penalties and damages, as well as sums payable pursuant to resolution or settlement agreements, caused in whole or in part by Business Associate's failure to comply with HIPAA or this Agreement, including but not limited to timely performance of functions or activities delegated to Business Associate by the Plan, to the extent Business Associate's failure caused or contributed to liability of the Plan or the Plan Sponsor for such penalties, damages or other amounts payable. Failures by any Agent or Subcontractor of the Business Associate shall be deemed a failure by Business Associate for purposes of this provision. Business Associate shall reimburse the Plan or Plan Sponsor, as applicable, for any investigative and mitigation costs, as well as any attorneys' fees and costs including with respect to administrative enforcement proceedings, pretrial and trial, appeal and petition for review and certiorari, and any bankruptcy proceedings, in proportion to the extent to which Business Associate's failure caused or contributed to the claims or allegations against the Plan or Plan Sponsor giving rise to the activities and proceedings causing the Plan or Plan Sponsor to incur the fees and costs.

IN WITNESS WHEREOF, the parties have caused this Business Associate Agreement to be executed on their behalf by their duly authorized representatives' signatures as of the dates set forth below.

Covered entity
Association of Washington Cities Employee Benefit Trust, for and on behalf of the health plans provided under the Health Care Program

Business associate
[Insert Business Associate name]

Signed

Signed

Printed name

Printed name

Title

Title

Date

Date