Washington Health Benefit Exchange

RFP HBE 18-007 Addendum No. 1

July 6, 2018

TO: Potential Bidders for RFP HBE 18-007 and Other Interested Parties
FROM: Erin Hamilton, RFP Coordinator
SUBJECT: Addendum No. 1 to RFP HBE 18-007 for "*Full Service Enrollment Centers*"

PURPOSE: The purpose of this addendum is:
1) To amend specific sections of the RFP, including Exhibits; and
2) To provide responses to questions submitted by potential bidders by the July 3, 2018 deadline.

ATTACHMENTS:
Exhibit A – Vendor Questions and WAHBE Responses
Exhibit D – Revised Data Security & Reporting Requirements

RFP HBE 18-007 is hereby amended as set forth below. Any material not specifically referenced below remains in full force and effect.

1) RFP Exhibit A – Certifications and Assurances, the last paragraph is hereby amended as follows:

   FROM:

   We (**Check one**) ☐ **are /** ☐ **are not** submitting proposed alternate Contract language or exceptions (see Section 4.2.1.9).

   TO:

   We (**Check one**) ☐ **are /** ☐ **are not** submitting proposed alternate Contract language or exceptions (see Exhibit D – Item B.15.).

2) RFP Exhibit B – Sample Contract, Exhibit D – Data Security Requirements, is hereby removed in its entirety and replaced with the attached Exhibit D – Revised Data Security & Reporting Requirements.

   The following items have been added to the Exhibit:

   - **Section 1.d.** "Security Incident means a warning that there may be or has been a threat to information or computer security including, but not limited to: unauthorized access; data or security breach; service attacks; malicious code; and unauthorized disclosure or misuse of confidential information".
   - **Section 4.** "The terms of this Exhibit shall apply to Contractor and any Subcontractors who use systems, network, data and/or documentation that is housed or managed by Contractors on behalf of, or in the performance of services, for WAHBE. For purposes of this Exhibit, they shall be collectively referred to as "Exchange Data"".
   - **Section 6.d.** "Reviews shall be conducted in accordance with the US Department of Commerce National Institute of Standards and Technology (NIST) Technical Guide to Information Security Testing and Assessment (Special Publication (SP) 800-115)".

   The following Definition from Section 1 has been deleted from the Exhibit:

   - "WAHBE data: use of systems, network, data and documentation that are housed or managed for WAHBE".

3) WAHBE responses to bidder questions submitted by the July 3, 2018 deadline are provided as Exhibit C to this Addendum.

Please contact the RFP Coordinator at contracts@WAHBExchange.org if there are any questions concerning this Addendum.

Respectfully,

Erin Hamilton, CPPB
RFP Coordinator

EXHIBIT A
VENDOR QUESTIONS AND WAHBE RESPONSES

Question #	Document Name	Section # & Title	Page or Paragraph#	Question	WAHBE RESPONSE
1	RFP HBE 18-007	Section 2.4. WAHBE Support for Enrollment Centers	2.4.6.	Can we use some of the funds offered to hire extra help during the 3 main months of open enrollment; and then use the balance for advertising or for compensating current staff or the business for their year-round WAH and SEP work?	No. Per RFP Section 2.4.6, WAHBE will provide funding for Enrollment Center operational costs, as follows: • 2.4.6.1. – Administrative Staff Costs (during OE only) • 2.4.6.2. – Signage (purchased prior to OE) • 2.4.6.3. – Advertising and Marketing (purchased prior to or during OE) • 2.4.6.4. – Operational overhead (year-round) Funds may not be used to compensate brokers or licensed insurance agents. WAHBE will only cover costs that are over and above a Vendor's normal business operating expenses. Compensation for current staff would be considered normal operating expenses, except for any additional administrative time needed to cover peak periods or extended hours during Open Enrollment. WAHBE does not anticipate the volume of requests for Enrollment Center assistance outside open enrollment to be significant enough to require additional staff or extended hours. Therefore, WAHBE will only allow funds to be used to cover extra (non-licensed) help during Open Enrollment. Advertising and marketing expenses can be requested leading up to and during open enrollment only.
2	RFP HBE 18-007	Section 1. Introduction	1.5. Vendor Information and Eligibility	We are aware that we can't apply jointly with another organization this year, is there an issue if we list another organization as affiliates with our agency? We don't want to compete with them but use them as "overflow" if needed and use their Spanish speaking agents that we can refer over.	WAHBE will accept one Proposal per Vendor, per Enrollment Center. The Apparently Successful Vendor(s) will be solely responsible for any Subcontractors used and the terms and conditions within the Contract. A Subcontractor could be a paid or unpaid organization conducting activities on behalf of the contracted Enrollment Center organization.

3	N/A (general question)			Is there a limited number of enrollment center locations that will be awarded this year?	Yes. WAHBE intends to award up to one Enrollment Center Contract per area. Per RFP Section 1.3., WAHBE will accept applications for all geographic areas of Washington State except Spokane and Federal Way.
4	N/A (general question)			Will there be affiliates in addition to brokers and navigators that will be listed in the press release?	No. WAHBE will only be contracting with Enrollment Centers this year. There will not be affiliates listed in the press release.
5	N/A (general question)			Can Enrollment Centers also be a Navigator Lead organization?	Yes.
6	Exhibit D – Response Template	Section I. Cost Proposal (Scored)	Signature Block	Every time I click on the signature section it automatically scrolls up to the beginning of the application without allowing me to insert the name and date. Do you have suggestions for how I can correct this?	All Vendors will need to print the response template and the signatory will need to handwrite his/her signature, name, Vendor name, and date. The template must then be uploaded and submitted to WAHBE in electronic format.

EXHIBIT D – REVISED DATA SECURITY & REPORTING REQUIREMENTS

WAHBE's duty is to protect the confidentiality and security of client, proprietary, account, and all other business information. To execute these responsibilities, this exhibit sets forth the requirements for Contractors and Sub-contractors who access, obtain, repackage, and/or distribute WAHBE Information. These requirements are in addition to WAHBE policies, standards, and other contractual terms and conditions. WAHBE must approve in advance, in writing, any variance from these security requirements

WAHBE reserves the right to update or modify these security requirements as necessary to protect the citizens of Washington and data entrusted to WAHBE. If WAHBE updates or modifies these Security Requirements, Contractor shall conform its systems, applications, processes or procedures to comply with the update or modification within a reasonable time period, with regard to all relevant security and legal concerns, as may be determined at the discretion of WAHBE.

1. Definitions:
    a. Authorized User(s) means an individual or individuals with an authorized business requirement to access WAHBE Confidential Information.
    b. Advanced Encryption Standard (AES) means a symmetric encryption algorithm.
    c. Hardened Password means a string of at least eight (8) characters including one (1) upper case, one (1) lower case, one (1) number and one (1) special character (i.e., non-alphanumeric characters).
    d. Security Incident means a warning that there may be or has been a threat to information or computer security including, but not limited to: unauthorized access; data or security breach; service attacks; malicious code; and unauthorized disclosure or misuse of confidential information.
    e. Transmitting: the transferring of data electronically, such as via email.
    f. Transporting: the physical transferring of data that has been stored.
    g. Unique User ID: a string of characters that identifies a specific user and which, in conjunction with a password, passphrase, or other mechanism, authenticates a user to an information system.

2. Contractors connected to WAHBE network or stewards of WAHBE data shall protect data by using the appropriate administrative, physical and technical safeguards:
    a. To prevent the use or disclosure of data other than as permitted or required by the terms and conditions of this exhibit, and
    b. To reasonably and appropriately protect the confidentiality, integrity, and availability of data the Contractor creates, receives, maintains, or transmits on behalf of WAHBE for as long as the data is within its possession and control, even after the termination or expiration of this Contract.
    c. Annual Awareness Training shall be conducted and documented for all Contractor's employees or Sub-Contractors that have access to WAHBE data that includes at minimum:
        i. Social Engineering/Phishing
        ii. Internet Hygiene
        iii. Insider Threats

iv. Password creation and use
v. Malware
vi. Regulatory requirements
vii. Incident Reporting
viii. Company Policies
ix. Advanced training for IT Professionals

3. Use and Disclosure: Contractor acknowledges that in performing the services it will have access to, or be directly or indirectly exposed to, client confidential information. Contractor shall use such information solely for performing the services. Contractor shall take all reasonable measures to protect all client information from disclosure, including measures at least as strict as those measures Contractor would use to protect its own confidential information. Contractor shall not disclose client information to any parties other than those with a need to know to perform the services on behalf of WAHBE and only to the extent such employees or Subcontractors are bound by the term executed and acknowledged by WAHBE.

4. The terms of this Exhibit shall apply to Contractor and any Subcontractors who use systems, network, data and/or documentation that is housed or managed by Contractors on behalf of, or in the performance of services, for WAHBE. For purposes of this Exhibit, they shall be collectively referred to as "Exchange Data".

5. Compliance with Applicable Law: WAHBE is governed by Washington State Regulations, IRS pub 1075, CMS minimum standards, US Privacy Act, and Washington Records Release Act. Contractor irrevocably consents to the jurisdiction and venue of any state or federal regulations and agrees to comply.

6. Protection of WAHBE Systems and data:

    a. In all events where Contractor has access to WAHBE data, Contractor shall meet all standards and requirements including, but not limited to: industry security standards, use of computer firewalls, strong user authentication, encrypted transmissions, anti-malware programs, regular and timely software patch updates, and controlled access to the physical location of computer hardware. This includes, without limitation, Contractor's transmission or storage of electronic files or electronic data.

    b. Application integrity shall be validated to ensure destructive computer programming such as harmful computer instructions, viruses, Trojan horses and other harmful code is mitigated; and integrity of data is maintained.

    c. Contractor shall implement security baselines on all systems and applications that meet industry and federal standards. Documentation must be submitted upon request. Security baselines can be found at https://www.cisecurity.org/ or https:/www.nist.gov.

    d. Contractor shall conduct periodic reviews, at minimum of annually, of any system storing WAHBE data or supporting systems to evaluate the security risks of such systems. Reviews shall be conducted in accordance with the US Department of Commerce National Institute of Standards and Technology (NIST) Technical Guide to Information Security Testing and Assessment (Special Publication (SP) 800-115). In addition, WAHBE shall conduct periodic vulnerability scans of any network or site maintained by Contractor that houses WAHBE data. Contractor shall take all reasonable steps to facilitate such scans and shall promptly remediate any systems vulnerable of exposing WAHBE data. Contractor shall report all security incidents to the WAHBE Contract Manager as soon as possible, but no later than one business day after discovery.

e. Inactive accounts shall be disabled by HBE within 60 days of inactivity or when no longer necessary to perform daily tasks. The vendor shall notify HBE of a change in responsibilities where access is no longer necessary for employees or contractors.

f. Physical Storage. When storing WAHBE data the Contractor shall perform the following:

i. Hard disk drives. Data stored on local workstation hard disks. Access to the data will be restricted to Authorized User(s) by requiring login to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provides equal or greater security, such as biometrics or smart cards. The data on the drive shall be encrypted and only accessible to authenticated user(s) with a need to know. Data shall be secured on the disk in such a way that other user(s) that do not need access to the data will not have the ability to access it.

ii. Workstations with sensitive data stored on them shall be tracked and their movements documented until the sensitive data is removed from the workstation. When the data is removed the date of its removal and method of its removal shall be documented and provided to the WAHBE Contract Manager. Hard drives that have contained sensitive data shall be wiped with a method that will render the deleted information irretrievable (See Section 9 Data Disposal).

iii. Network server storage. Access to the data shall be restricted to Authorized User(s) through the use of access control lists which will grant access only after the Authorized User(s) has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or physical token. Data on disks mounted to such servers shall be in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism. Access shall be reviewed at minimum annually.

iv. For WAHBE data stored on network storage: Deleting unneeded data is sufficient as long as the disks remain in a secured area and otherwise meet the requirements listed in the above paragraph. Destruction of the data as outlined in Section 9. Data Disposal may be deferred until the disks are retired, replaced, or otherwise taken out of the secured area.

v. Removable Media, including Optical discs (CDs or DVDs) in local workstation optical disc drives shall not be transported out of a secure area. Sensitive or Confidential Data provided by WAHBE on removable media, such as optical discs or USB drives, which will be used in local workstation optical disc drives or USB connections shall be encrypted with two hundred sixty-five (256) bit AES encryption or better. When not in use for the Contracted purpose, such devices must be locked in a drawer, cabinet or other container to which only authorized users have the key, combination or mechanism required to access the contents of the container. Workstations which access WAHBE data on optical discs shall be in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

vi. When being transported outside of a secure area, portable devices and media with confidential WAHBE data must be under the physical control of Contractor staff with authorization to access the data.

vii. WAHBE data shall not be stored on portable devices or media unless specifically authorized within the Special Terms and Conditions of the Contract. Portable media includes any data storage that can be detached or removed from a computer and transported. If so authorized, the data shall be given the following protections:

1. Encrypt the data with a key length of at least two hundred fifty-six (256) bit AES using an industry standard algorithm.
2. Control access to devices with a Unique User ID and hardened password or stronger authentication method such as physical token or biometrics.
3. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is twenty (20) minutes.
4. Physically protect the portable device(s) and/or media by:
    a. Keeping them in locked storage when not in use
    b. Using check-in/check-out procedures when they are shared, and
    c. Taking frequent inventories

viii. Paper documents. All paper records shall be protected by storing the records in a secure area which is only accessible to Authorized User(s). When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only Authorized User(s) have access.

g. Remote and Network Access. When accessing WAHBE data remotely the Contractor shall:

i. WAHBE data accessed and used interactively over the internet shall meet minimum standards including updated anti-malware, current security patches, and local firewall. Access to the website washingtonhealthplanfinder.org or other services managed by WAHBE will be controlled by WAHBE staff who will issue authentication credentials (e.g. a Unique User ID and hardened password) to Authorized User(s). The administrator and any privileged user password must change every 60 days and other user password once every 90 days. Previous 6 consecutive passwords cannot be reused. The passwords must not allow User ids, first Name or the last name of the user.

ii. Contractor shall have established and documented access termination procedures for existing Authorized User(s) with access to WAHBE data. These procedures shall be provided to WAHBE staff upon request. Contractor shall notify WAHBE staff immediately whenever an Authorized User(s) in possession of such credentials is terminated or otherwise leaves the employment of the Contractor, and whenever an Authorized User(s) duties change such that the Authorized User(s) no longer requires access to perform work for this Contract.

iii. Access via remote terminal/workstation over the internet shall be managed by the Contractor and permissions granted on a need basis only when access to WAHBE data is present.

iv. Data Transmitting. When transmitting WAHBE data electronically, including via email, the data shall be protected by:

1. Transmitting the data within the WAHBE network or Contractor's internal network, or;

2. Encrypting any data that will be transmitted outside the WAHBE network or Contractor internal network with two hundred fifty-six (256) bit AES encryption or better. This includes transit over the public Internet.

7. Contractor shall maintain audit logs for all systems containing WAHBE data.

8. Data Segregation:

    a. WAHBE data shall be segregated or otherwise distinguished from non-WAHBE data to ensure proper return or destruction when no longer needed.

        i. WAHBE data shall be stored on media (e.g. hard disk, optical disc, tape, etc.) which will exclude non-WAHBE data. Or,

        ii. WAHBE data shall be stored in a logical container on electronic media, such as a partition or folder dedicated to WAHBE data. Or,

        iii. WAHBE data shall be stored in a database which will exclude non- WAHBE data. Or,

        iv. WAHBE data shall be stored within a database and will be distinguishable from non-WAHBE data by the value of a specific field or fields within database records. Or,

        v. When it is not feasible or practical to segregate WAHBE data from non- WAHBE data, then both the WAHBE data and the non-WAHBE data with which it is commingled must be protected as described in this exhibit.

9. Data Disposal: When the Contracted work has been completed or when no longer needed, data shall be returned to WAHBE or destroyed. Media on which WAHBE data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	Shall be destroyed by:
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks)	Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or confidential data	Shredded and recycled through a Contracted firm provided the Contract with the recycler assures that the confidentiality of data will be protected
Paper documents containing confidential information requiring special handling (e.g. protected health information)	On-site shredding by a method that renders the data unreadable, crosscut shredding, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or cutting/breaking into small pieces
Magnetic tape	Degaussing, incinerating or crosscut shredding

10. Data shared with Subcontractors: If WAHBE data provided under this Contract is to be shared with a Subcontractor; the Contract with the Subcontractor shall include all the data security provisions in this Contract and any amendments, attachments, or exhibits to this Contract.

11. Notice of Unauthorized Disclosure or Security Breach. Contractor shall immediately notify WAHBE of:

    a. Unauthorized disclosure or use of any WAHBE Data;

    b. Any breaches of security that may compromise the WAHBE data or Contractor's ability to safeguard WAHBE data;

c. Notifications shall include at minimum, both a telephone call and email to the WAHBE Contract Manager and an email to WAHBE Security at security@wahbexchange.org.

d. Contractor shall establish and document a policy to deal with the compromise or potential compromise of data that complies with NIST 800-61 Incident Response Guide. Contractor shall provide WAHBE with such policy upon request.

e. A breach of security or other circumstance which causes, may have caused, or allowed access to WAHBE information by unauthorized persons or systems, whether intentional, fraudulent, or accidental, must be reported to WAHBE as soon as possible and no later than one (1) business day after discovery.