DATA SECURITY & REPORTING REQUIREMENTS

The terms of this Exhibit apply to all Contractors that access Washington Health Benefit Exchange's (WAHBE) systems, network, Data and/or documentation, whether housed or managed on behalf of, or in the performance of services, for WAHBE.

WAHBE's duty is to protect the confidentiality, integrity, and security of WAHBE Data, as defined in this Exhibit. To execute these responsibilities, this Exhibit sets forth the requirements for Contractors who access, obtain, repackage, and/or distribute WAHBE Data. These requirements are in addition to WAHBE policies, standards, and other contractual terms and conditions. Contractor must receive advance written approval from WAHBE for any variance from these requirements.

Contractors with access to WAHBE Data must comply with applicable governing laws and standards including Center for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-e) v2.2 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Contractors with access to Federal Tax Information (FTI) Data must comply with applicable governing laws and standards including IRS Publication 1075.

WAHBE reserves the right to update or modify these requirements as necessary to protect individuals of the State of Washington and Data entrusted to WAHBE. If WAHBE updates or modifies these requirements, Contractor must conform its systems, applications, processes, or procedures to comply with the update or modification within a reasonable time period, as 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 Data.

    b. Advanced Encryption Standard (AES) means a symmetric encryption algorithm.

    c. FIPS means Federal Information Processing Standard. It is a National Institute of Standards and Technology (NIST) approved encryption mechanism.

    d. Contractor means that firm, provider, organization, individual or other entity performing Deliverables under this Contract, including all employees of the Contractor.

    e. Data, or WAHBE Data, means any information with a confidential or sensitive nature that is hosted, processed, or developed by or on behalf of WAHBE (e.g., software code, configuration files, Personal Identifiable Information (PII), FTI, or security-related documentation).

    f. Data at Rest means data that is stored on a physical or logical device and is not being accessed.

    f. FTI means Federal Tax Information. It is prohibited from general use and disclosure under Title 26 of the United States Code.

    g. Hardened Password means a string of at least fifteen (15) characters including one (1) upper case, one (1) lower case, one (1) number, one (1) special character (i.e., non-alphanumeric characters) and do not allow previous 24 consecutive passwords.

    h. PII means Personally Identifiable Information, any Data that could potentially identify a specific individual or can be used to distinguish one person from another collected by or on behalf of WAHBE or applicants for insurance affordability programs as defined in 45 CFR 155.260.

i. Security Incident means a warning that there may be or has been a threat to information or computer or physical security including, but not limited to unauthorized access; Data or security breach; service attacks; malicious code; and unauthorized disclosure or misuse of WAHBE Data.

j. Security Breach means any unauthorized access or improper disclosure that has been verified to have affected WAHBE Data.

k. Subcontractor means one who is not in the employment of the Contractor and who is performing all or part of those services under this Contract or under a separate contract with the Contractor. The terms "Subcontractor" and "Subcontractors" means Subcontractor(s) in any tier.

l. Transmitting means the transferring of Data electronically, such as via email.

m. Transporting: the physical transferring of Data that has been stored.

n. 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 must 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 must be conducted and documented for all Contractor's employees or Sub-Contractors that have access to WAHBE Data. Training must include, at minimum:

      i. Social Engineering/Phishing
      ii. Internet Hygiene
      iii. Insider Threats
      iv. Password creation and use
      v. Malware
      vi. Applicable Regulatory requirements
      vii. Incident Reporting
      viii. Company Policies
      ix. Advanced training for IT Professionals
      x. Personally Identifiable Information (PII)
      xi. Handling and protecting the WAHBE application Data including sensitive Data
      xii. Proper disposal of Data storage media

d. Contractor must maintain all annual awareness training documentation for six (6) years and must produce documentation for WAHBE inspection, within 5 business days of request.

3. Use and Disclosure: Contractor acknowledges that in performing the services it will have access to, or be directly or indirectly exposed to, WAHBE Data. Contractor must use such information solely for performing the services. Contractor must take all reasonable measures to protect WAHBE Data from disclosure, including measures at least as strict as those measures Contractor would use to protect its own confidential information. Contractor must not disclose WAHBE Data 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 this Exhibit.

4. Protection of WAHBE Systems and Data:

   a. In all events where Contractor has access to WAHBE Data, Contractor must meet all standards and requirements including, but not limited to industry security standards, use of computer firewalls, strong user authentication, encrypted transmissions, secure coding practice, 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 must be validated to ensure no destructive computer programming such as viruses and malware exists. Common controls such as secure coding techniques, data encryption, principle of least privilege, input- and output-validation must be maintained to ensure the integrity of the Data.

   c. Contractor must implement security baselines on all systems and applications that meet applicable industry and federal guidelines. Minimum security baselines are available at https://www.cisecurity.org/ or https:/www.nist.gov or https://owasp.org/. Documentation must be submitted to WAHBE upon request.

   d. Contractor must maintain following security documentation at a minimum to ensure adherence to security standards and proactive management of vulnerabilities. These must be made available to WAHBE within 5 business days of request.

      i. Security policies and procedures that defined organization's approach to information security, including standards for access control, data integrity, incident response, etc.
      ii. System security plan outlining the security controls and measures in place to protect systems and data.

   e. Contractor must 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 must 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 may conduct periodic vulnerability scans of any network or site maintained by Contractor that houses WAHBE Data. Contractor must take all reasonable steps to facilitate such scans and must promptly remediate any systems vulnerable of exposing WAHBE Data.

f. Contractor must notify WAHBE of a change in responsibilities where access is no longer necessary for employees or contractors. Inactive WAHBE system and accounts must be disabled within 60 days of inactivity or when no longer necessary to perform daily tasks.

g. Contractor must segregate or otherwise distinguish WAHBE Data from non-WAHBE Data to ensure proper return or destruction when WAHBE determines the Data is no longer needed.

h. Contractor must store WAHBE Data on media (e.g., hard disk, optical disc, tape, etc.) which will exclude non-WAHBE Data.

i. Contractor must store WAHBE Data in a logical container on electronic media, such as a partition or folder dedicated to WAHBE Data.

j. Contractor must store WAHBE Data within a Database that is distinguishable from non-WAHBE Data by the value of a specific field or fields within Database records.

k. Contractor must encrypt all WAHBE Data at rest. The mechanism used to encrypt the Data must be latest FIPS 140 validated encryption method and operate using latest FIPS 140 validated encryption module.

l. If Contractor cannot 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.

m. Physical Storage. When storing WAHBE Data the Contractor must perform the following:

    i. Access to Data stored on local workstation hard disks 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. Previous 24 consecutive passwords cannot be reused when using a hardened password. The Data on the drive must be encrypted and only accessible to authenticated user(s) with a need-to- know. Data must 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 must 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 must be documented and provided to the WAHBE Contract Manager and WAHBE Security upon request. Hard drives that have contained sensitive Data must be wiped with a method that will render the deleted information irretrievable (See Section 7 Data Disposal).

    iii. Network server storage. Access to the Data must be restricted to Authorized User(s) using 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 must 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 must 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 7. 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 must not be transported out of a secure area. WAHBE Data provided on removable media, such as optical discs or USB drives, which will be used in local workstation optical disc drives or USB connections must be encrypted with latest Federal Information Processing Standard (FIPS) 140 validated encryption method. 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 must 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 WAHBE Data must be under the physical control of Contractor staff with authorization to access the Data.

vii. WAHBE Data must not be stored on portable devices or media unless specifically authorized in the Contract. Portable media includes any Data storage that can be detached or removed from a computer and transported. If so authorized, the Data must be given the following protections:

1. Data at rest and in transit must be encrypted using an industry standard algorithm, latest FIPS 140 validated encryption method.

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 fifteen (15) 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 must 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.

n. Remote and Network Access. When accessing WAHBE Data remotely the Contractor must comply with the following:

i. WAHBE Data accessed and used interactively over the internet must meet minimum standards including updated anti-malware, current security patches, and local firewall. Access to the website wahealthplanfinder.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 Contractor administrator and any privileged user passwords must change every 60 days, and other

Contractor user passwords once every 90 days; except where augmented by other technical control such as SSH keys, and/or complex ephemeral token. Previous 24 consecutive passwords cannot be reused. The passwords must not allow User ids, first Name or the last name of the user.

ii. Contractor must have established and documented access termination procedures for existing Authorized User(s) with access to WAHBE Data. These procedures must be provided to WAHBE staff upon request. Contractor must 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 must be managed by the Contractor and permissions granted on a need basis only when access to WAHBE Data is present.

iv. Data Transmission - When transmitting WAHBE Data electronically, including via email, the Data must be protected by:

1. Using encrypted connections to transmit the Data within or outside the network by utilizing standardized protocols such as Transport Layer Security (TLS) or encrypted Virtual Private Network (VPN). These standardized protocols must meet the latest version per applicable industry and federal guidelines.

2. Using latest FIPS 140 validated encryption method to transmit any Data within or outside the network.

5. Contractor must have the ability to detect or monitor potential data breach or unauthorized access or transfer of WAHBE data using a Data Loss Prevention (DLP) solution.

6. Contractor must audit and maintain audit logs for all the systems processing, storing, and transmitting WAHBE Data. Audit logs must be available to WAHBE upon request when investigating a potential security incident. Otherwise, audit logs must be made available to WAHBE within 5 business days.

7. Data Disposal: When the Contracted work has been completed, Data retention requirements have been met, or when WAHBE determines Data is no longer needed, Data must 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:	**Must 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 or removable media.
Paper documents containing WAHBE Data	Shredded, pulping or incineration and recycled onsite or through a Contracted firm provided the Contract with the recycler assures that the confidentiality of Data will be protected and is destroyed according to specification. Destroy paper using crosscut shredders that produce particles that are 1mmx5mm (0.04 in x 0,2in.) in size or

Data stored on:	Must be destroyed by:
	smaller, or pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32in. (2.4 mm) security screen.
Optical discs (e.g., CDs or DVDs)	Incineration, shredding, or cutting/breaking into small pieces
Magnetic tape	Degaussing, incinerating or crosscut shredding
Cloud	Deleting*, Data/media sanitization, or cryptographic erasure

* Deleting unnecessary Data is sufficient if the disks remain in a secured area and otherwise meet the requirements listed in Section 4, above. Destruction of the Data as outlined in this section of this Exhibit may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

8. Contractor must notify WAHBE Security at securityincidents@wahbexchange.org for any change in their system that impacts the way they receive, process, store, access, protect and/or transmit WAHBE data. Contractor must provide change notification and a security impact analysis. Data shared with Subcontractors: If WAHBE Data provided under this Contract is to be shared with a Subcontractor; the Contract with the Subcontractor must include all the Data security provisions in this Contract and any amendments, attachments, or exhibits to this Contract.

9. Contractor must maintain incident response plan which should include procedures and protocols for promptly responding to and mitigating security incidents and breaches. Contractor must regularly review and update the incident response plan to ensure its effectiveness and alignment with current security threats and best practices.

10. Notice of Unauthorized Disclosure or Security Breach.

    a. Contractor must immediately notify WAHBE Security, securityincidents@wahbexchange.org within one (1) hour of discovery of:

        i. Unauthorized disclosure or use of any WAHBE Data.

        ii. Any breaches of security that compromise the WAHBE Data or Contractor's ability to safeguard WAHBE Data.

        iii. 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.

    b. Notifications must include at minimum, both a telephone call and email to the WAHBE Contract Manager and an email to WAHBE Security at securityincidents@wahbexchange.org.

    c. Contractor must establish and document a policy to address the compromise or potential compromise of Data that complies with NIST 800-61 Incident Response Guide. Contractor must provide WAHBE with such policy upon request.

Authorized Contractor Signature	Full Name and Title (Printed or Typed)
Date	Title