State of Washington Contracts & Procurement Division Department of Enterprise Services P.O. Box 41411 Olympia, WA 98504-1411	Contract No.:	02526
Jane A. Kosanovich 5637 Sunrise Beach Road NW Olympia, WA 98502	Amendment No.:	1
	Effective Date:	October 28, 2026

FIRST AMENDMENT

TO

CONTRACT NO. 02526

SIGN LANGUAGE INTERPRETER SERVICES

This First Amendment ("Amendment") to Contract No. 02526 is made and entered into by and between the State of Washington acting by and through the Department of Enterprise Services, a Washington State governmental agency ("Enterprise Services") and Jane A. Kosanovich, a Sole Proprietorship ("Contractor") and is dated as of October 28, 2026.

R E C I T A L S

A. Enterprise Services and Contractor (collectively the "Parties") entered into that certain Contract No. 02526 dated effective as of April 21, 2026 ("Contract").

B. The Parties desire to amend the Contract to add *Exhibit D – HIPAA Compliance and Data Protection Agreement* to the Contract.

C. The Parties further desire to amend *Exhibit A – Included Goods/Services* of the Contract to remove Section 5.B.

D. The amendment set forth herein is within the scope of the Contract.

A G R E E M E N T

NOW THEREFORE, in consideration of the mutual covenants and agreements set forth herein, the Parties hereby agree to amend the Contract, as previously amended, as follows:

1. COMPLIANCE WITH HIPAA. *Exhibit D – HIPAA Compliance and Data Protection Agreement*, provided below, is incorporated into the Contract.

2. CONTRACTOR EXPECTATIONS. The following language is removed from all applicable sections in the Contract.

5.B. Contractor may be required to agree to additional privacy protections to provide services to Purchaser. For example, successful Contractors that wish to provide services to Purchasers that are covered entities under HIPAA may be required to execute service level agreements (SLAs), Memorandum of Understanding (MOU), Business Associate Agreements (BAAs), etc.

3. NO CHANGE OTHER THAN AMENDMENT. Except as amended herein, the Contract is unaffected and remains in full force and effect.

4. INTEGRATED AGREEMENT; MODIFICATION. This Amendment constitutes the entire agreement and understanding of the Parties with respect to the subject matter and supersedes all prior negotiations and representations. In the event of any conflict between this Amendment and the Contract or any earlier amendment, this Amendment shall control and govern. This Amendment may not be modified except in writing signed by the Parties.

5. AUTHORITY. Each party to this Amendment, and each individual signing on behalf of each party, hereby represents and warrants to the other that it has full power and authority to enter into this Amendment and that its execution, delivery, and performance of this Amendment has been fully authorized and approved, and that no further approvals or consents are required to bind such party.

6. ELECTRONIC SIGNATURES. An electronic signature or electronic record of this Amendment or any other ancillary agreement shall be deemed to have the same legal effect as delivery of an original executed copy of this Amendment or such other ancillary agreement for all purposes.

7. COUNTERPARTS. This Amendment may be executed in one or more counterparts, each of which shall be deemed an original, and all of which counterparts together shall constitute the same instrument which may be sufficiently evidenced by one counterpart. Execution of this Amendment at different times and places by the parties shall not affect the validity thereof so long as all the parties hereto execute a counterpart of this Amendment.

EXECUTED AND EFFECTIVE as of the day and date first above written.

JANE A. KOSANOVICH,
A SOLE PROPRIETORSHIP

By: Jane A. Kosanovich
Jane A. Kosanovich (Oct 26, 2026 03:25:28 PDT)
Name: Jane A. Kosanovich
Title: ASL Interpreter
Date: 10/26/2026

STATE OF WASHINGTON
DEPARTMENT OF ENTERPRISE SERVICES

By: _____
Name: Tim Foitzik
Title: Procurement Supervisor
Date: 10/23/2026

EXHIBIT D

HIPAA COMPLIANCE AND DATA PROTECTION AGREEMENT

1. **Purpose.** The purpose of this Exhibit is to establish a Business Associate relationship between the Contractor and applicable Purchasers and to set forth the Parties' understanding with regard to the Business Associate's Use and Disclosure of Protected Health Information (defined below) in accordance with the business associate agreement requirements of the Health Insurance Portability and Accountability Act of 1996. Contractor shall comply with HIPAA and all provisions of this agreement for all appointments covered by HIPAA, unless otherwise specified by the Purchaser. Purchasers may indicate an appointment is covered by HIPAA by indicating so in Purchaser's request for services made through the ODHH Request system, or via other means specified by the Purchaser.

2. **Definitions**. The words and phrases listed below, as used in this Agreement, shall each have the following definitions:

   a. "Agreement" or "Contract" means the entire written agreement between Enterprise Services and the Contractor, including any Exhibits, documents, or materials incorporated by reference. The parties may execute this contract in multiple counterparts, each of which is deemed an original and all of which constitute only one agreement. E-mail or Facsimile transmission of a signed copy of this contract shall be the same as delivery of an original. This Agreement incorporates by reference all Business Associate provisions required by the U.S. Department of Health and Human Services, Office for Civil Rights. Any ambiguity in this Agreement shall be interpreted to permit compliance with HIPAA, as defined below.

   b. "Authorized User(s)" means an individual or individuals with an authorized business requirement to access Purchaser's Confidential Information.

   c. "Breach" means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the Protected Health Information, with the exclusions and exceptions listed in 45 CFR 164.402.

   d. "Business Associate," as used in this Agreement, means the "Contractor" and generally has the same meaning as the term "business associate" at 45 CFR 160.103. Any reference to Business Associate in this Contract includes Business Associate's owners, directors, partners, employees, agents, officers, Subcontractors, third party contractors, volunteers, or directors. A Business Associate shall perform all Contract duties, activities and tasks in compliance with HIPAA, as defined below. For purposes of any permitted Subcontract, "Contractor" includes any Subcontractor and its owners, members, officers, directors, partners, employees, and/or agents.

   e. "CFR" means the code of federal regulations. All references in this Contract to CFR titles,

parts, subparts, or sections shall include any successor, amended, or replacement regulation or interim Office of Management and Budget (OMB) circular.

f. "Confidential Information" or "Data" means information that is exempt from disclosure to the public or other unauthorized persons under RCW 42.56 or other federal or state laws. Confidential Information includes, but is not limited to, "PHI" and "Personal Information," defined below.

g. "Covered Entity" means an entity as defined at 45 CFR 160.103, in its conduct of covered functions by its health care components.

h. "Designated Record Set" means a group of records maintained by or for a Covered Entity, that is: the medical and billing records about Individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or Used in whole or part by or for the Covered Entity to make decisions about Individuals.

i. "Electronic Protected Health Information (ePHI)" means Protected Health Information, defined below, that is transmitted by electronic media or maintained in any medium described in the definition of electronic media at 45 CFR 160.103.

j. "Encrypt" means to encode Confidential Information into a format that can only be read by those possessing a "key"; a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 128 bits.

k. "Hardened Password" means a string of at least eight characters containing at least one alphabetic character, at least one number and at least one special character such as an asterisk, ampersand or exclamation point.

l. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, as amended by the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 ("HITECH"), and all applicable implementing regulations, including, without limitation, the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule"), Notification in the Case of Breach of Unsecured Protected Health Information ("Breach Notification Rule"), and the Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule") found at Title 45, Parts 160 and 164 of the Code of Federal Regulations, dealing with the security, confidentiality, integrity and availability of protected health or health-related information, as well as breach notifications (all such laws and regulations shall be collectively referred to herein as "HIPAA").

m. "Individual(s)" means the person(s) who is the subject of PHI and includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

n. "Minimum Necessary" means the least amount of PHI necessary to accomplish the purpose for which the PHI is needed.

o. "Personal Information" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education,

business, use or receipt of governmental services or other activities, addresses, telephone numbers, Social Security Numbers, driver license numbers, other identifying numbers, any financial identifiers, or as included in RCW 42.56.230.

p. "Physically Secure" means that access is restricted through physical means to authorized individuals only.

q. "Program Agreement" means an agreement between the Contractor and the Purchaser containing special terms and conditions, including a statement of work to be performed by the Contractor and payment to be made by the Purchaser.

r. "Protected Health Information (PHI)" means individually identifiable health information (including ePHI) created, received, maintained or transmitted by a Business Associate on behalf of a health care component of the Covered Entity that relates to the provision of health care to an Individual; the past, present, or future physical or mental health or condition of an Individual; or the past, present, or future payment for provision of health care to an Individual. PHI includes demographic information that identifies the Individual or about which there is reasonable basis to believe can be used to identify the Individual. PHI does not include Information regarding a person who has been deceased for more than 50 years; employment records held by Covered Entity in its role as employer; or Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g and student records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

s. "RCW" means the Revised Code of Washington. All references in this Contract to RCW chapters or sections shall include any successor, amended, or replacement statute.

t. "Regulation" means any federal, state, or local regulation, rule, or ordinance.

u. "Secured Area" means an area to which only authorized representatives of the entity possessing the Confidential Information have access. Secured Areas may include buildings, rooms or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.

v. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

w. "Subcontract" means any separate agreement or contract between the Contractor and an individual or entity ("Subcontractor") to perform all or a portion of the duties and obligations that the Contractor is obligated to perform pursuant to this Contract. The term "Subcontractor" includes a Business Associate that creates, receives, maintains, or transmits Protected Health Information on behalf of another Business Associate.

x. "Tracking" means a record keeping system that identifies when the sender begins delivery of Confidential Information to the authorized and intended recipient, and when the sender receives confirmation of delivery from the authorized and intended recipient of Confidential Information.

y. "Trusted Systems" include only the following methods of physical delivery: (1) hand-delivery

by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (2) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and (4) the Washington State Campus mail system. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.

z. "Unique User ID" means 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.

aa. "Use" includes the sharing, employment, application, utilization, examination, or analysis, of PHI within an entity that maintains such information.

bb. "WAC" means the Washington Administrative Code. All references in this Contract to WAC chapters or sections shall include any successor, amended, or replacement regulation.

3. Confidentiality.

a. The Business Associate shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Agreement for any purpose that is not directly connected with Business Associate's performance of the services contemplated hereunder, except:

(1) as provided by law; or,

(2) in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information.

b. The Business Associate shall protect and maintain all Confidential Information gained by reason of this Contract against unauthorized use, access, disclosure, modification or loss. This duty requires the Business Associate to employ reasonable security measures, as detailed below.

4. Use and Disclosure of PHI. Business Associate is limited to the following permitted and required uses or disclosures of PHI:

a. Duty to Protect PHI. Business Associate shall protect PHI from, and shall use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to EPHI, to prevent the unauthorized Use or disclosure of PHI other than as provided for in this Contract or as required by law, for as long as the PHI is within its possession and control, even after the termination or expiration of this Contract.

b. Minimum Necessary Standard. Business Associate shall apply the HIPAA Minimum Necessary standard to any Use or disclosure of PHI necessary to achieve the purposes of this Contract. See 45 CFR 164.514 (d)(2) through (d)(5).

c. Disclosure as Part of the Provision of Services. Business Associate shall only Use or disclose PHI as necessary to perform the services specified in this Contract or as required by law, and shall not Use or disclose such PHI in any manner that would violate Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information) if done by Covered Entity, except for the specific uses and disclosures set forth below.

d. Use for Proper Management and Administration. Business Associate may Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

e. Disclosure for Proper Management and Administration. Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.

f. Impermissible Use or Disclosure of PHI. Business Associate shall report to the Purchaser in writing all Uses or disclosures of PHI not provided for by this Contract within one (1) business day of becoming aware of the unauthorized Use or disclosure of PHI, including Breaches of unsecured PHI as required at 45 CFR 164.410 (Notification by a Business Associate), as well as any security incident of which it becomes aware. Upon request by the Purchaser, Business Associate shall mitigate, to the extent practicable, any harmful effect resulting from the impermissible Use or disclosure. The parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity that attempted but unsuccessful security incidents, such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, regularly occur and that no further notice will be made by Business Associate so long as no such incident results in unauthorized access, use or disclosure of PHI.

g. De-identification of PHI.

   (1) Creation and Use of De-identified Data. In the event Business Associate wishes to de-identify PHI, it must first submit its proposed plan for accomplishing the conversion to the Purchaser for the Purchaser's approval, which shall not be unreasonably withheld provided such conversion meets the requirements of 45 CFR 164.514. Business Associate may use de-identified PHI only as directed or otherwise agreed to by the Purchaser.

   (2) Re-identification Prohibited. Unless otherwise agreed upon by the parties, in the event that the Purchaser provides Business Associate with de-identified PHI, Business Associate shall not be given access to, nor shall Business Associate attempt to develop on its own, any keys or codes that can be used to re-identify the data.

h. Failure to Cure. If the Purchaser learns of a pattern or practice of the Business Associate that constitutes a violation of the Business Associate's obligations under the terms of this

Contract and reasonable steps by the Purchaser do not end the violation, the Purchaser shall terminate this Contract in accordance with Section 20, Termination for Default. In addition, If Business Associate learns of a pattern or practice of its Subcontractors that constitutes a violation of the Business Associate's obligations under the terms of their contract and reasonable steps by the Business Associate do not end the violation, Business Associate shall terminate the Subcontract, if feasible.

i. Consent to Audit. Business Associate shall give reasonable access to PHI, its internal practices, records, books, documents, electronic data or all other business information received from, or created or received by Business Associate on behalf of the Purchaser, to the Secretary of DHHS and/or to the Purchaser for use in determining compliance with HIPAA privacy requirements.

j. Obligations of Business Associate Upon Expiration or Termination. Upon expiration or termination of this Contract for any reason, with respect to PHI received from the Purchaser, or created, maintained, or received by Business Associate, or any Subcontractors, on behalf of the Purchaser, Business Associate shall:

(1) Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

(2) Return to the Purchaser or destroy the remaining PHI that the Business Associate or any Subcontractors still maintain in any form;

(3) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to Electronic Protected Health Information to prevent Use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate or any Subcontractors retain the PHI;

(4) Not Use or disclose the PHI retained by Business Associate or any Subcontractors other than for the purposes for which such PHI was retained and subject to the same conditions set out in the "Use and Disclosure of PHI" section of this Contract which applied prior to termination; and

(5) Return to the Purchaser or destroy the PHI retained by Business Associate, or any Subcontractors, when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

k. Survival. The obligations of the Business Associate under this section shall survive the termination or expiration of this Contract.

5. Individual Rights.

a. Accounting of Disclosures.

(1) Business Associate shall document all disclosures, except those disclosures that are exempt under 45 CFR 164.528, of PHI and information related to such disclosures.

(2) Within ten (10) business days of a request from the Purchaser, Business Associate shall make available to the Purchaser the information in Business Associate's possession that is necessary for the Purchaser to respond in a timely manner to a request for an accounting of disclosures of PHI by the Business Associate. See 45 CFR 164.504(e)(2)(ii)(G) and 164.528(b)(1).

(3) At the request of the Purchaser or in response to a request made directly to the Business Associate by an Individual, Business Associate shall respond, in a timely manner and in accordance with HIPAA and the HIPAA Rules, to requests by Individuals for an accounting of disclosures of PHI.

(4) Business Associate record keeping procedures shall be sufficient to respond to a request for an accounting under this section for the six (6) years prior to the date on which the accounting was requested.

b. Access.

(1) Business Associate shall make available PHI that it holds that is part of a Designated Record Set when requested by the Purchaser as necessary to satisfy the Purchaser's obligations under 45 CFR 164.524 (Access of Individuals to Protected Health Information).

(2) If the request for access to PHI in a designated record set is made by the Individual to the Business Associate, the Business Associate will refer the individual to the Purchaser. If the Purchaser asks the Business Associate to respond to a request, the Business Associate shall comply with requirements in 45 CFR 164.524 (Access of Individuals to Protected Health Information) on form, time and manner of access. When the request is made by the Purchaser, the Business Associate shall provide the records to the Purchaser within ten (10) business days.

c. Amendment.

(1) If the Purchaser amends, in whole or in part, a record or PHI contained in an Individual's Designated Record Set and the Purchaser has previously provided the PHI or record that is the subject of the amendment to Business Associate, then the Purchaser will inform Business Associate of the amendment pursuant to 45 CFR 164.526(c)(3) (Amendment of Protected Health Information).

(2) Business Associate shall make any amendments to PHI in a Designated Record Set as directed by the Purchaser or as necessary to satisfy the Purchaser's obligations under 45 CFR 164.526 (Amendment of Protected Health Information).

6. Data Transport. When transporting the Purchaser Confidential Information electronically, including via email, the Data will be protected by:

a. Transporting the Data within the (State Governmental Network) SGN or Contractor's internal network, or;

b. Encrypting any Data that will be in transit outside the SGN or Contractor's internal network.

This includes transit over the public Internet.

7. **Protection of Data.** The Business Associate agrees to store Data on one or more of the following media and protect the Data as described:

   a. Hard disk drives. Data stored on local workstation hard disks. Access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

   b. Network server disks. Data stored on hard disks mounted on network servers and made available through shared folders. Access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User 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 smart cards. Data on disks mounted to such servers must be located 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.

      For the Purchaser Confidential Information stored on these disks, 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 Disposition may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

   c. Optical discs (CDs or DVDs) in local workstation optical disc drives. Data provided by the Purchaser on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secured Area. When not in use for the contracted purpose, such discs 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 the Purchaser Data on optical discs must be located 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.

   d. Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers. Data provided by the Purchaser on optical discs which will be attached to network servers and which will not be transported out of a Secured Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User 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 smart cards. Data on discs attached to such servers must be located 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.

   e. Paper documents. Any paper records must be protected by storing the records in a Secured Area which is only accessible to authorized personnel. 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 persons have access.

f. Remote Access. Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by the Purchaser staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor staff. Contractor will notify the Purchaser staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Contract.

g. Data storage on portable devices or media.

(1) Except where otherwise specified herein, the Purchaser Data shall not be stored by the Business Associate on portable devices or media unless specifically authorized within the terms and conditions of the Contract. If so authorized, the Data shall be given the following protections:

(a) Encrypt the Data with a key length of at least 128 bits

(b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.

(c) 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 20 minutes.

(d) Physically Secure the portable device(s) and/or media by:

i. Keeping them in locked storage when not in use,

ii. Using check-in/check-out procedures when they are shared, and

iii. Taking frequent inventories.

(2) When being transported outside of a Secured Area, portable devices and media with the Purchaser Confidential Information must be under the physical control of Contractor staff with authorization to access the Data.

(3) Portable devices include, but are not limited to; smart phones, tablets, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook/netbook computers if those computers may be transported outside of a Secured Area.

(4) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape), or flash media (e.g. CompactFlash, SD, MMC).

h. Data stored for backup purposes.

(1) the Purchaser Data may be stored on portable media as part of a Business Associate's existing, documented backup process for business continuity or disaster recovery purposes. Such storage is authorized until such time as that media would be reused

during the course of normal backup operations. If backup media is retired while the Purchaser Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements in Section 9.

(2) the Purchaser Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a Business Associate's existing, documented backup process for business continuity or disaster recovery purposes. Such media will be protected as otherwise described in this Agreement. If this media is retired while the Purchaser Confidential Information still exists upon it, the data will be destroyed at that time in accordance with the disposition requirements in Section 9. Data Disposition.

8. Data Segregation.

a. The Purchaser Data must be segregated or otherwise distinguishable from non-Purchaser data. This is to ensure that when no longer needed by the Business Associate, all the Purchaser Data can be identified for return or destruction. It also aids in determining whether the Purchaser Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.

b. The Purchaser Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-Purchaser Data;

c. The Purchaser Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to the Purchaser Data;

d. The Purchaser Data will be stored in a database which will contain no non-Purchaser data; or

e. The Purchaser Data will be stored within a database and will be distinguishable from non-Purchaser data by the value of a specific field or fields within database records.

f. When stored as physical paper documents, the Purchaser Data will be physically segregated from non-Purchaser data in a drawer, folder, or other container.

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

9. Data Disposition. When the contracted work has been completed or when no longer needed, except as noted in Section 7. Protection of Data b. Network server disks above, Data shall be returned to the Purchaser or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or

Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling 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, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a course abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding

10. Breach Notification.

a. In the event of a Breach of unsecured PHI or disclosure that compromises the privacy or security of PHI obtained from the Purchaser or involving the Purchaser clients, Business Associate will take all measures required by state or federal law.

b. Business Associate will notify the Purchaser within one (1) business day by telephone and in writing of any acquisition, access, Use or disclosure of PHI not allowed by the provisions of this Agreement or not authorized by HIPAA or required by law of which it becomes aware which potentially compromises the security or privacy of the Protected Health Information as defined in 45 CFR 164.402 (Definitions).

c. Business Associate will notify the Purchaser Contact shown on the cover page of this Contract within one (1) business day by telephone or e-mail of any potential Breach of security or privacy of PHI by the Business Associate or its Subcontractors or agents. Business Associate will follow telephone or e-mail notification with a faxed or other written explanation of the Breach, to include the following: date and time of the Breach, date Breach was discovered, location and nature of the PHI, type of Breach, origination and destination of PHI, Business Associate unit and personnel associated with the Breach, detailed description of the Breach, anticipated mitigation steps, and the name, address, telephone number, fax number, and e-mail of the individual who is responsible as the primary point of contact. Business Associate will address communications to the Purchaser Contact. Business Associate will coordinate and cooperate with the Purchaser to provide a copy of its investigation and other information requested by the Purchaser, including advance copies of any notifications required for the Purchaser review before disseminating

and verification of the dates notifications were sent.

d. If the Purchaser determines that Business Associate or its Subcontractor(s) or agent(s) is responsible for a Breach of unsecured PHI:

(1) requiring notification of Individuals under 45 CFR 164.404 (Notification to Individuals), Business Associate bears the responsibility and costs for notifying the affected Individuals and receiving and responding to those Individuals' questions or requests for additional information;

(2) requiring notification of the media under 45 CFR 164.406 (Notification to the media), Business Associate bears the responsibility and costs for notifying the media and receiving and responding to media questions or requests for additional information;

(3) requiring notification of the U.S. Department of Health and Human Services Secretary under 45 CFR 164.408 (Notification to the Secretary), Business Associate bears the responsibility and costs for notifying the Secretary and receiving and responding to the Secretary's questions or requests for additional information; and

(4) the Purchaser will take appropriate remedial measures up to termination of this Contract.

11. Subcontracts and other Third Party Agreements. In accordance with 45 CFR 164.502(e)(1)(ii), 164.504(e)(1)(i), and 164.308(b)(2), Business Associate shall ensure that any agents, Subcontractors, independent contractors or other third parties that create, receive, maintain, or transmit PHI on Business Associate's behalf, enter into a written contract that contains the same terms, restrictions, requirements, and conditions as the HIPAA compliance provisions in this Contract with respect to such PHI. The same provisions must also be included in any contracts by a Business Associate's Subcontractor with its own business associates as required by 45 CFR 164.314(a)(2)(b) and 164.504(e)(5).

12. Obligations. To the extent the Business Associate is to carry out one or more of the Purchaser's obligation(s) under 45 CFR, Part 164, Subpart E (Privacy of Individually Identifiable Health Information), Business Associate shall comply with all requirements that would apply to the Purchaser in the performance of such obligation(s).

13. Liability. Within ten (10) business days, Business Associate must notify the Purchaser of any complaint, enforcement or compliance action initiated by the Office for Civil Rights based on an allegation of violation of the HIPAA Rules and must inform the Purchaser of the outcome of that action. Business Associate bears all responsibility for any penalties, fines or sanctions imposed against the Business Associate for violations of the HIPAA Rules and for any imposed against its Subcontractors or agents for which it is found liable.

14. Inspection. The Contractor shall, at no cost, provide the Purchaser and the Office of the State Auditor with reasonable access to Contractor's place of business, Contractor's records, and the Purchaser client records, wherever located. These inspection rights are intended to allow the Purchaser and the Office of the State Auditor to monitor, audit, and evaluate the Contractor's performance and compliance with applicable laws, regulations, and these Contract terms. These inspection rights shall survive for six (6) years following this Contract's termination or

expiration.

15. **Termination for Default**. Enterprise Services may immediately terminate this Contract for default, in whole or in part, by written notice to the Contractor if the Purchaser has a reasonable basis to believe that the Contractor has:

    a. Failed to meet or maintain any requirement for contracting with the Purchaser;

    b. Failed to protect the health or safety of any Purchaser client; or

    c. Violated any applicable law or regulation.

16. **Subrecipients**.

    a. General. If the Business Associate is a subrecipient of federal awards as defined by 2 CFR, Part 200 and this Agreement, the Business Associate shall:

        (1) Maintain records that identify, in its accounts, all federal awards received and expended and the federal programs under which they were received, by Assistance Listing Number (ALN) and title, award number and year, name of the federal agency, and name of the pass-through entity;

        (2) Maintain internal controls that provide reasonable assurance that the Business Associate is managing federal awards in compliance with laws, regulations, and provisions of contracts or grant agreements that could have a material effect on each of its federal programs;

        (3) Prepare appropriate financial statements, including a schedule of expenditures of federal awards;

        (4) Incorporate 2 CFR, Part 200, Subpart F audit requirements into all agreements between the Business Associate and its Subcontractors who are subrecipients;

        (5) Comply with the applicable requirements of and any future amendments to either 2 CFR, Part 200, and any successor or replacement regulation or OMB Circular; and

        (6) Comply with the Omnibus Crime Control and Safe streets Act of 1968, Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, Title II of the Americans with Disabilities Act of 1990, Title IX of the Education Amendments of 1972, The Age Discrimination Act of 1975, and The Department of Justice Non-Discrimination Regulations, 28 C.F.R. Part 42, Subparts C.D.E. and G, and 28 C.F.R. Part 35 and 39.

    b. Single Audit Act Compliance. If the Business Associate is a subrecipient and expends $750,000 or more in federal awards from any and/or all sources in any fiscal year, the Business Associate shall procure and pay for a single audit or a program-specific audit for that fiscal year. Upon completion of each audit, the Business Associate shall:

        (1) Submit to the Purchaser contact person the data collection form and reporting

package specified in 2 CFR Part 200, Subpart F, reports required by the program-specific audit guide (if applicable), and a copy of any management letters issued by the auditor;

(2) Follow-up and develop corrective action for all audit findings; in accordance with 2 CFR Part 200, Subpart F; prepare a "Summary Schedule of Prior Audit Findings" reporting the status of all audit findings included in the prior audit's schedule of findings and questioned costs.

c. Overpayments. If it is determined by the Purchaser, or during the course of a required audit, that the Business Associate has been paid unallowable costs under this or any Program Agreement, the Purchaser may require the Business Associate to reimburse the Purchaser in accordance with 2 CFR, Part 200.

17. Savings Clause and Termination.

In the event the federal or state laws are amended so that fulfillment of this Contract is not feasible or no longer necessary, both the Department and the Business Associate shall be discharged from further obligation created under the terms of this Contract, and Business Associate shall return or destroy all PHI received from the Department upon termination of the agreement, as provided above. If an existing or subsequent Business Associate Agreement is entered into by the Department and the Business Associate which supersedes this Contract, then this Contract is terminated in regard to superseded terms and conditions. The remainder of the provisions of this Contract intended to survive shall survive such termination if not superseded.

18. Automatic Amendment. Upon the effective date of any amendment to HIPAA, this Agreement shall automatically amend so that the obligations imposed on Business Associate remain in compliance with such regulations.

19. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with HIPAA.

20. Conflicts. Any provision of the Program Agreement, any Exhibit, or any other underlying agreement that is directly contradictory to one or more terms of this Agreement ("Contradictory Term") shall be superseded by the terms of this Agreement only to the extent of the contradiction, as necessary for the parties' compliance with HIPAA and to the extent that it is reasonably impossible to comply with both the Contradictory Term and the terms of this Agreement.

02526 Amendment 1 - Jane A Kosanovich

Final Audit Report 2026-10-26

Created:	2026-10-21
By:	Haley Robertson (haley.robertson@des.wa.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAXGKOwdczm9NuuUEYNv0fhyF0RV3iQOQd

"02526 Amendment 1 - Jane A Kosanovich" History

Document created by Haley Robertson (haley.robertson@des.wa.gov)
2026-10-21 - 10:25:55 PM GMT

Document emailed to Tim Foitzik (Tim.Foitzik@des.wa.gov) for signature
2026-10-21 - 10:26:00 PM GMT

Email viewed by Tim Foitzik (Tim.Foitzik@des.wa.gov)
2026-10-21 - 10:58:12 PM GMT

Email viewed by Tim Foitzik (Tim.Foitzik@des.wa.gov)
2026-10-23 - 10:30:50 PM GMT

Document e-signed by Tim Foitzik (Tim.Foitzik@des.wa.gov)
Signature Date: 2026-10-23 - 10:43:05 PM GMT - Time Source: server - Signature Appearance Selected: IMAGE

Document emailed to Jane A. Kosanovich (janeterps@gmail.com) for signature
2026-10-23 - 10:43:07 PM GMT

Email viewed by Jane A. Kosanovich (janeterps@gmail.com)
2026-10-26 - 10:22:59 AM GMT

Document e-signed by Jane A. Kosanovich (janeterps@gmail.com)
Signature Date: 2026-10-26 - 10:25:28 AM GMT - Time Source: server - Signature Appearance Selected: TYPE

Agreement completed.
2026-10-26 - 10:25:28 AM GMT