SCANNING & DIGITIZATION SERVICES

NON-MANDATORY FOR STATE AGENCIES

NON-MANDATORY FOR POLITICAL SUBDIVISIONS

Vendor: **Valley Business Machines (VBM)**
Master Agreement #: **2024-0200-0079**
Term: **September 18, 2023 – September 30, 2025**
Renewals Remaining: **Two (2) additional one-year renewal option through 2029**
IRIS: **MA # 240000053**

Contract Summary: This non-mandatory contract is issued in accordance with Invitation to Bid (ITB) #2024-0200-0079 to provide to provide document scanning and digitization services with indexing capabilities as specified in the solicitation document for the Anchorage area. The contract shall be on an as-needed basis for all state agencies, political subdivisions, federally recognized tribes, and other entities authorized to use statewide contracts in the State of Alaska.

CONTRACT PRICING

Anchorage		
Services Description	**Unit**	**Cost**
Scanning Black and White	Per Page	$ 0.07
Scanning Color	Per Page	$ 0.07
PDF w/ OCR	Per Page	$ 0.09
PDF w/o OCR	Per Page	$ 0.07
PDF w/ ICR	Per Page	$ 0.10
PDF w/o ICR	Per Page	$ 0.07
Media File (i.e. DVD)	Per File	$ 5.00
Document Preparation	Hour	$ 20.00
Manual Indexing	Per Hour	$ 36.00
Storage Cost	30 Days	$ 2.00
Pick up/Delivery	Hour	$ 25.00
Document Destruction	Per lb.	$ 0.50

Note: Storage costs only start applying 10 days after the ordering end user has been notified the boxes can be picked up after scanning.

Submitting Orders: To arrange for paper documents to be scanned, please contact Lee Riley, at (907) 376-5077 or 907-631-4514 or Lee@vbmalaska.com, or Katie Lindsey at Katie@vbmalaska.com.

CONTRACT DETAILS

1. **AGENCY PREPARATION**
   - Using agencies must insure that all boxes are taped shut before sending them to the contractor to be scanned.
   - All boxes must have a box list with identification names and numbers listed per box.
   - Using agencies are responsible for prepping documents for scanning.
     - Remove all paperclips, staples, binders, etc.
     - Any document smaller than 5.5”x8.5” must be taped to a must be taped to a larger piece of paper, or photocopied to an 8.5 x 11" paper and inserted.

   NOTE: Documents not prepared correctly may result in preparation charges by the contractor at the price submitted on bid schedule.

2. **AGENCY DOCUMENT SHIPPING/ DROP OFF**
   - **Agency Drop-off**
     - Agencies can have their boxes picked up by the contractor at the price specified on bid schedule. Agencies will have the option to drop boxes off to awarded contractor to have documents scanned.
     - Once the job is complete agencies may request documents to be mailed back to them or will be able to pick up the documents if they desire.
   - **Shipping and Delivery**
     - An agency may ship documents to the contractor if desired. Agencies are responsible for shipping costs to the contractor.
     - Once documents are digitized the contractor will ship them back to the agency via the shipping method requested by the agency. Shipping costs must be billed to the agency as a pass-through charge and identified as a separate line item on the invoice.
     - If the agency wants the documents delivered by the contractor, it will be at the price specified on the bid schedule. If the agency is located out of the delivery area of the contractor, the contractor shall ship the documents as specified above.

Contractor Requirements:

3. **SCANNING REQUIREMENTS:**
   - All services provided under this contract by the contractor shall be performed in the State of Alaska, within 75 miles of the respective cities identified in the ITB (Anchorage bidders would not be able to perform services for Juneau, and vice versa for example).
   - There will be no agency on-site scanning.
   - All pages will be scanned in the same order as presented.
   - Scanned images shall be placed on a DVD, CD, thumb drive, external hard drive, or other appropriate approved media for delivery to the agency.
   - The contractor must follow naming conventions that the state identifies on their box or indexing list. This will be established before documents are scanned, the naming convention will be specified by the using agency.
   - The scanning services must include the capability to scan single-sided and double-sided documents. Paper sizes including but not limited to, 5.5”x8.5” 8.5”x11” 8.5”x14” 5”x8” 11”x17”.

- Documents may contain handwritten and/or printed text and/or graphics. Graphics may include, but not be limited to, drawings, plans, photographs, icons, graphs, charts and signatures. Each scanned image should reflect the color properties of the original document. Contractor must offer color, grayscale, and bitonal scanning.
- Upon request the contractor shall perform Document Preparation as necessary to scan all files at the price submitted on the bid schedule. This includes but is not limited to removing all staples, paperclips, repair all torn documents, straighten all folded plans and mount any irregular size memorandum on standard 5.5”x8.5” 8.5”x11” 8.5”x14” 5”x8” 11”x17” paper.
- Documents are stored in multiple formats, including loose pages, sewn-in bindings, stapled and 3-ring binders. Document preparation may require separation of documents from their binding prior to scanning.
- The condition of most documents are reasonably good; however, some older documents shall require special handling.

4. DOCUMENT SECURITY REQUIREMENTS:

- Contractor will handle confidential information according to State of Alaska laws and regulations. I.E. documents and digitized information will be kept in a locked area, and documents will be held out of public view.
- No unauthorized personnel will have access to the state files while under contractor jurisdiction.
- Contractor will notify the state when the scanned electronic files are completed and will be returned to the state with an estimated time of arrival.
- Contractor will need to confirm the state has received the scanned electronic files and the state must confirm, in writing (email), the hard copy files can be destroyed or shipped back to the agency.
- Contractor’s employees handling state documents must pass a criminal background check and follow the FBI Security Policy for CJIS organizations.
- Must handle HIPAA/personnel files in secure and HIPAA compliant manner.

5. INDEXING REQUIREMENTS:

- Optical Character Recognition (OCR) must be available for all document types.
- Intelligent Character Recognition (ICR) must be available for all document types.
- The contractor must be able to perform:
  - Accurate indexing or attribution of metadata to each file and record scanned;
  - Ability to correct OCR/ICR read errors.
  - Manual Keying.
  - Double-Blind Keying.
  - Edit checks to ensure that index field formats, values, etc. are correct.
  - Barcode Recognition.
  - Auto-Indexing Capabilities.

6. QUALITY REQUIREMENTS:

- A quality control process shall be in place to ensure that scanned images are complete and accurate. The contractor will perform a 100% frame by frame inspection and rescan any documents where:
  - There is substantial loss of detail when compared to the original.
  - The tonal values are uneven.
  - The contrast is too low or too high.
  - There are skewed or misaligned images.
- All data must be preserved in a form identical to, or functionally equal to, the original record.

- Upon request documents shall rotate to provide maximum readability (e.g., letters shall be in proper orientation when document is displayed without rotation.).

- Scanned documents must be viewable in PDF or TIF format at a minimum of 400-600 dpi, including greyscale or color scanning. Other format types may be requested. *Standard formats for permanent records (best practice for non-permanent) are PDF, PDF/A, TIFF, JPEG2000, PNG. 400 dpi minimum if OCR is required, 600 dpi minimum for photos, maps, plats.*

7. DOCUMENT SHIPPING AND DROP-OFF/PICK-UP

- **Contractor Pick-up/drop-off**
  - Contractor will pick-up boxes containing documents to be scanned at the price listed per box on the bid schedule.
    - In the event an agencies documents are on a retention schedule, the contractor may need to drop off the scanned documents along with the media files back to the agency, at the price listed on the bid schedule.
- **Shipping**
  - Media files and documents can be dropped off or mailed back to using agency as a passthrough cost.

8. DOCUMENT DESTRUCTION

- After the documents are scanned and digitized the contractor will destroy the documents within 30 days of the agency's request and supply written notification of such by email (to be provided by the agency) when this occurs.
- Contractors will be held to the cost of destruction submitted on bid schedule.
- If the agency would like to have their documents sent back to them, the contractor will do so. Please note shipping charges will be the responsibility of the agency (to be billed as a pass through if not arranged directly by the agency).
- When documents are requested to be destroyed, all documents containing personal and confidential information must be shredded, burned, pulverized, or otherwise rendered unreadable in such a manner that the information is not recoverable.

9. PROCESS:

1. Authorizing Staff: Each Participating agency will appoint a member of their staff to be the point of contact and will be responsible for notifying the contractors of any concerns, re-scheduling pickups, document retrieval needs, etc.
2. Preparation: Agencies must keep their documents in standard archive boxes, sized 15 x 12 x 10, 24 x 12 x 10, or 24 x 15 x 10 and must be taped shut. These boxes will either be mailed or dropped off to the contractor. Agencies must create document lists, showing what documents are in each box, these lists will be provided to the contractor to insure boxes remain in same order they arrived in.
3. Quote: Once an agency has an order ready, they will notify the contractor via email or telephone of the number of boxes and documents to be scanned. The contractor will then give the agency a quote based directly on the contract rates. If the agency's document count is not accurate or the agency does not provide the actual number of documents, the quote will be an estimate only. Once scanning is complete, the contractor shall send the agency a final quote based on the actual number of documents scanned at contract rates.
4. Shipping: If contractor is located in a different city, the ordering agency will be responsible for arranging and paying for shipping costs to and from the contractor.

5. Scanning: Once the contractor has received the documents, they will scan them into the desired form and will then notify the agency once the job is complete.
6. Destruction: Once all scanning is complete the contractor will destroy the documents if destruction is approved by the agency. File destruction must meet conditions for confidential destruction as commonly defined in AS 45.48.500 Disposal of Records.
7. Documents needing to be returned for storage: Once all documents are scanned and electronic files are ready, the contractor will send them back to the using agency or will call using agency for them to be picked up. Shipments to the ordering agency will be arranged by the contractor using the shipping method requested by the agency and shall be billed to the agency as a passthrough cost. Such costs must be identified on invoices as a separate line item.

Additional general requirements:

- SECURITY AND BACKGROUND CHECK REQUIREMENTS
  Employees that have access to documents, or document images must pass a nationwide seven-year criminal history background check. The vendor shall not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to one year is an authorized penalty. The vendor shall promote and maintain an awareness of the importance of securing the state's information among the vendor's employees and agents.
  The vendor will be responsible for any costs associated with obtaining criminal history reports. Copies shall be made available to the state within 30 days upon request.

- CONVERSION OF PAPER FORMATS TO DIGITIZED IMAGES WITH ASSOCIATED METADATA AND INCLUDING DELIVERY OF THE IMAGED RECORDS.

1. Accurate Electronic Records: The primary objective in the image conversion service process is to capture the most accurate and complete facsimile of the source documents as possible and accurately and completely capture, either automatically or manually, the required index or metadata. Vendor will be required to have on file, documented policies, assigned responsibilities, and formal procedures of the management for their processing of electronic records.

2. Image Scanning: The objective of image scanning is to capture the most accurate and complete digitized facsimile of the document as possible. Vendor will meet the following requirements: Periodic testing of the scanner's proper functioning which includes a standard scan target page for checking the image quality of bi-tonal scanners;
   - Cursory operator review of individual images as they are being scanned;
   - Single and duplex scanning;
   - Elimination of blank pages;

3. Document Preparation: Vendor will supply agencies with bar-coded batch separator sheets and document separator sheets. Agencies will use them with preparing their documents for imaging. State staff will be responsible for preparation of all documents sent for imaging.
   Indexing: Vendor must be able to perform the following:
   - Accurate indexing or attribution of metadata to each file and document scanned;

- Ability to correct OCR/ICR read errors;
- Manual Keying;
- Double-Blind Keying;
- Edit checks to ensure that index field formats, values, etc. are correct;
- Barcode Recognition;
- Auto-Indexing Capabilities;

4. Records Destruction: Pursuant to the personal information protection act (PIPA, HB 65) all electronic media devices containing personal information must be shredded, burned, pulverized, or otherwise rendered unreadable in such a manner that the media is not recoverable.

- **SECURITY AND BACKGROUND CHECK REQUIREMENTS**
  Employees that have access to documents, or document images must pass a nationwide seven-year criminal history background check. The vendor shall not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to one year is an authorized penalty. The vendor shall promote and maintain an awareness of the importance of securing the state's information among the vendor's employees and agents.

  The vendor will be responsible for any costs associated with obtaining criminal history reports. Copies shall be made available to the state within 30 days upon request.

- **Nondisclosure and Confidentiality:** Bidder agrees that all confidential information shall be used only for purposes of providing the deliverables and performing the services specified herein and shall not disseminate or allow dissemination of confidential information except as provided for in this section. The Bidder shall hold as confidential and will use reasonable care (including both facility physical security and electronic security) to prevent unauthorized access by, storage, disclosure, publication, dissemination to and/or use by third parties of, the confidential information. "Reasonable care" means compliance by the Bidder with all applicable federal and state law, including the Social Security Act and HIPAA. The Bidder must promptly notify the state in writing if it becomes aware of any storage, disclosure, loss, unauthorized access to or use of the confidential information.

- ***Confidential information***, As used herein, is defined as any data, files, software, information or materials (whether prepared by the state or its agents or advisors) in oral, electronic, tangible or intangible form and however stored, compiled or memorialized that is classified confidential as defined by State of Alaska classification and categorization guidelines (i) provided by the state to the Bidder or a Bidder agent or otherwise made available to the Bidder or a Bidder agent in connection with this contract, or (ii) acquired, obtained or learned by the Bidder or a Bidder agent in the performance of this contract. Examples of confidential information include, but are not limited to: technology infrastructure, architecture, financial data, trade secrets, equipment specifications, user lists, passwords, research data, and technology data (infrastructure, architecture, operating systems, security tools, IP addresses, etc.).

- **Criminal Justice Information Systems (CJIS) Compliance:** Bidder must follow CJIS security policy. Located at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center. If you require a hardcopy contact the Procurement Officer of record.

- **Business Associate Agreement:**

A. Covered Entity (CE) wishes to disclose certain information to Business Associate (BA), some of which may constitute Protected Health Information ("PHI");

B. It is the goal of CE and BA to protect the privacy and provide for the security of PHI owned by CE that is disclosed to BA or accessed, received, stored, maintained, modified or retained by BA in compliance with HIPAA (42 U.S.C. 1320d – 3120d-8) and its implementing regulations at 45 C.F.R. 160 and 45 C.F.R. 164 (the "Privacy and Security Rule"), the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5) (the "HITECH Act"), and with other applicable laws;

C. The purpose and goal of the HIPAA Business Associate Agreement ("BAA") is to satisfy certain standards and requirements of HIPAA, HITECH Act, and the Privacy and Security Rule, including but not limited to 45 C.F.R. 164.502(e) and 45 C.F.R. 164.504(e), as may be amended from time to time;

D. CE may operate a drug and alcohol treatment program that must comply with the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law and regulations, 42 U.S.C. 290dd-2 and 42 C.F.R. Part 2 (collectively "Part 2"); and

E. BA may be a Qualified Service Organization ("QSO") under Part 2 and therefore must agree to certain mandatory provisions regarding the use and disclosure of substance abuse treatment information.

Therefore, in consideration of mutual promises below and the exchange of information pursuant to the BAA, CE and BA agree as follows:

1. Definitions.

   a. General: As used in this BAA, the terms "Protected Health Information," "Health Care Operations," and other capitalized terms have the same meaning given to those terms by HIPAA, the HITECH Act and the Privacy and Security Rule. In the event of any conflict between the mandatory provisions of HIPAA, the HITECH Act or the Privacy and Security Rule, and the provisions of this BAA, HIPAA, the HITECH Act or the Privacy and Security Rule shall control. Where the provisions of this BAA differ from those mandated by HIPAA, the HITECH Act or the Privacy and Security Rule but are nonetheless permitted by HIPAA, the HITECH Act or the Privacy and Security Rule, the provisions of the BAA shall control.

   b. Specific:

      1) Business Associate: "Business Associate" or "BA" shall generally have the same meaning as the term "business associate" at 45 C.F.R. 160.103.

      2) Covered Entity: "Covered Entity" or "CE" shall have the same meaning as the term "covered entity" at 45 C.F.R. 160.103.

      3) Privacy and Security Rule: "Privacy and Security Rule" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.

2. Permitted Uses and Disclosures by Business Associate.

   a. BA may only use or disclose PHI for the following purposes:

   b. BA may use or disclose PHI as required by law.

c. BA agrees to make uses and disclosures and requests for PHI consistent with CE's minimum necessary policies and procedures.

d. BA may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by CE, except for the specific uses and disclosures set out below.

e. BA may disclose PHI for the proper management and administration of BA or to carry out the legal responsibilities of BA, provided the disclosures are required by law, or BA 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 notified BA of any instances of which it is aware in which the confidentiality of the information has been breached.

f. BA may provide data aggregation services related to the health care operations of CE.

3. Obligations of Business Associate.

a. Permitted uses and disclosures: BA may only use and disclose PHI owned by the CE that it creates, receives, maintains, or transmits if the use or disclosure is in compliance with each applicable requirement of 45 C.F.R. 164.504(e) of the Privacy Rule or this BAA. The additional requirements of Subtitle D of the HITECH Act contained in Public Law 111-5 that relate to privacy and that are made applicable with respect to Covered Entities shall also be applicable to BA and are incorporated into this BAA.

To the extent that BA discloses CE's PHI to a subcontractor, BA must obtain, prior to making any such disclosure: (1) reasonable assurances from the subcontractor that it will agree to the same restrictions, conditions, and requirements that apply to the BA with respect to such information; and (2) an agreement from the subcontractor to notify BA of any Breach of confidentiality, or security incident, within two business days of when it becomes aware of such Breach or incident.

b. Safeguards: 45 C.F.R. 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies, procedures and documentation requirements) shall apply to BA in the same manner that such sections apply to CE, and shall be implemented in accordance with HIPAA, the HITECH Act, and the Privacy and Security Rule. The additional requirements of Title XIII of the HITECH Act contained in Public Law 111-5 that relate to security and that are made applicable to Covered Entities shall also apply to BA and are incorporated into this BAA.

Unless CE agrees in writing that this requirement is infeasible with respect to certain data, BA shall secure all paper and electronic PHI by encryption or destruction such that the PHI is rendered unusable, unreadable or indecipherable to unauthorized individuals; or secure paper, film and electronic PHI in a manner that is consistent with guidance issued by the Secretary of the United States Department of Health and Human Services specifying the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals, including the use of standards developed under Section 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by Section 13101 of the HITECH Act contained in Public Law 111-5.

BA shall not use personally owned devices to create, receive, maintain or transmit PHI. Devices the BA uses to create, receive, maintain or transmit CE's electronic PHI shall be owned and managed by BA or CE.

BA shall patch its operating system and all applications within two weeks of the release of any patch. BA shall keep its antivirus and antimalware installed and active. BA shall limit its use of administrative accounts for IT operations only.

c. Reporting Unauthorized Disclosures and Breaches: During the term of this BAA, BA shall notify CE within 24 hours of discovering a Breach of security; intrusion; or unauthorized acquisition, access, use or disclosure of CE's PHI in violation of any applicable federal or state law, including security incidents. BA shall identify for the CE the individuals whose unsecured PHI has been, or is reasonably believed to have been, breached so that CE can comply with any notification requirements if necessary. BA shall also indicate whether the PHI subject to the Breach; intrusion; or unauthorized acquisition, access, use or disclosure was encrypted or destroyed at the time. BA shall take prompt corrective action to cure any deficiencies that result in Breaches of security; intrusion; or unauthorized acquisition, access, use, and disclosure. BA shall fulfill all breach notice requirements unless CE notifies BA that CE will take over the notice requirements. BA shall reimburse CE for all costs incurred by CE that are associated with any mitigation, investigation and notice of Breach CE undertakes or provides under HIPAA, HITECH Act, and the Privacy and Security Rule as a result of a Breach of CE's PHI caused by BA or BA's subcontractor or agent.

   If the unauthorized acquisition, access, use or disclosure of CE's PHI involves only Secured PHI, BA shall notify CE within 10 days of discovering the Breach but is not required to notify CE of the names of the individuals affected.

d. BA is not an agent of CE.

e. BA's Agents: If BA uses a subcontractor or agent to provide services under this BAA, and the subcontractor or agent creates, receives, maintains, or transmits CE's PHI, the subcontractor or agent shall sign an agreement with BA containing substantially the same provisions as this BAA and further identifying CE as a third-party beneficiary with rights of enforcement and indemnification from the subcontractor or agent in the event of any violation of the subcontractor or agent agreement. BA shall mitigate the effects of any violation of that agreement.

f. Availability of Information to CE: Within 15 days after the date of a written request by CE, BA shall provide any information necessary to fulfill CE's obligations to provide access to PHI under HIPAA, the HITECH Act, or the Privacy and Security Rule.

g. Accountability of Disclosures: If BA is required by HIPAA, the HITECH Act, or the Privacy or Security Rule to document a disclosure of PHI, BA shall make that documentation. If CE is required to document a disclosure of PHI made by BA, BA shall assist CE in documenting disclosures of PHI made by BA so that CE may respond to a request for an accounting in accordance with HIPAA, the HITECH Act, and the Privacy and Security Rule. Accounting records shall include the date of the disclosure, the name and if known, the address of the recipient of the PHI, the name of the individual who is subject of the PHI, a brief description of the PHI disclosed and the purpose of the disclosure. Within 15 days of a written request by CE, BA shall make the accounting record available to CE.

h. Amendment of PHI: Within 30 days of a written request by CE or an individual, BA shall amend PHI maintained, transmitted, created or received by BA on behalf of CE as directed by CE or the individual when required by HIPAA, the HITECH Act or the Privacy and Security Rule, or take other measures as necessary to satisfy CE's obligations under 45 C.F.R. 164.526.

i. Internal Practices: BA shall make its internal practices, books and records relating to the use and disclosure of CE's PHI available to CE and all appropriate federal agencies to determine CE's and BA's compliance with HIPAA, the HITECH Act and the Privacy and Security Rule.

j. Risk Assessment: BA shall biennially conduct a thorough assessment of the potential risks to and vulnerabilities of the confidentiality, integrity, and availability of CE's PHI that BA receives, stores, transmits, or has access to. BA shall provide CE, upon request, with a written report detailing the results of the risk assessment within 5 days.

k. To the extent BA is to carry out one or more of CE's obligations under Subpart E of 45 C.F.R. Part 164, BA must comply with the requirements of that Subpart that apply to CE in the performance of such obligations.

l. Audits, Inspection and Enforcement: CE may, after providing reasonable notice to the BA, conduct an inspection of the facilities, systems, books, logs and records of BA that relate to BA's use of CE's PHI, including inspecting logs showing the creation, modification, viewing, and deleting of PHI at BA's level. Failure by CE to inspect does not waive any rights of the CE or relieve BA of its responsibility to comply with this BAA. CE's failure to detect or failure to require remediation does not constitute acceptance of any practice or waive any rights of CE to enforce this BAA.

Notwithstanding BA's obligation to report under paragraph 3.c of this BAA, BA shall provide a monthly report to CE detailing the unauthorized, or reasonable belief of unauthorized, acquisition, access, use, or disclosure of CE's PHI, including any unauthorized creation, modification, or destruction of PHI and unauthorized login attempts. BA shall include privileged and nonprivileged accounts in its audit and report, indicating the unique individual using the privileged account. BA shall also indicate whether CE's PHI subject to unauthorized activity was encrypted or destroyed at the time of the unauthorized activity.

BA shall provide a yearly report to CE that lists the names of all individuals with technical or physical access to CE's PHI and the scope of that access.

m. Restrictions and Confidential Communications: Within 10 business days of notice by CE of a restriction upon use or disclosure or request for confidential communications pursuant to 45 C.F.R.164.522, BA shall restrict the use or disclosure of an individual's PHI. BA may not respond directly to an individual's request to restrict the use or disclosure of PHI or to send all communication of PHI to an alternate address. BA shall refer such requests to the CE so that the CE can coordinate and prepare a timely response to the requesting individual and provide direction to the BA.

n. Indemnification: BA shall indemnify and hold harmless CE for any civil or criminal monetary penalty or fine imposed on CE for acts or omissions in violation of HIPAA, the HITECH Act, or the Privacy or Security Rule that are committed by BA, a member of its workforce, its agent, or its subcontractor.

4. Obligations of CE. CE will be responsible for using legally appropriate safeguards to maintain and ensure the confidentiality, privacy and security of PHI transmitted to BA under the BAA until the PHI is received by BA. CE will not request BA to use or disclose PHI in any manner that would not be permissible under HIPAA, the HITECH Act or the Privacy and Security Rule if done by CE.

5. Termination.

a. Breach: A breach of a material term of the BAA by BA that is not cured within a reasonable period of time will provide grounds for the immediate termination of the contract.

b. Reasonable Steps to Cure: In accordance with 45 C.F.R. 164.504(e)(1)(ii), CE and BA agree that, if it knows of a pattern of activity or practice of the other party that constitutes a material breach or violation of the other party's obligation under the BAA, the nonbreaching party will take reasonable steps to get the breaching party to cure the breach or end the violation and, if the steps taken are

unsuccessful, terminate the BAA if feasible, and if not feasible, report the problem to the Secretary of the U.S. Department of Health and Human Services.

c. Effect of Termination: Upon termination of the contract, BA will, at the direction of the CE, either return or destroy all PHI received from CE or created, maintained, or transmitted on CE's behalf by BA in any form. Unless otherwise directed, BA is prohibited from retaining any copies of PHI received from CE or created, maintained, or transmitted by BA on behalf of CE. If destruction or return of PHI is not feasible, BA must continue to extend the protections of this BAA to PHI and limit the further use and disclosure of the PHI. The obligations in this BAA shall continue until all of the PHI provided by CE to BA is either destroyed or returned to CE.

6. Amendment. The parties acknowledge that state and federal laws relating to electronic data security and privacy are evolving, and that the parties may be required to further amend this BAA to ensure compliance with applicable changes in law. Upon receipt of a notification from CE that an applicable change in law affecting this BAA has occurred, BA will promptly agree to enter into negotiations with CE to amend this BAA to ensure compliance with changes in law.

7. Ownership of PHI. For purposes of this BAA, CE owns the data that contains the PHI it transmits to BA or that BA receives, creates, maintains or transmits on behalf of CE.

8. Litigation Assistance. Except when it would constitute a direct conflict of interest for BA, BA will make itself available to assist CE in any administrative or judicial proceeding by testifying as witness as to an alleged violation of HIPAA, the HITECH Act, the Privacy or Security Rule, or other law relating to security or privacy.

9. Regulatory References. Any reference in this BAA to federal or state law means the section that is in effect or as amended.

10. Interpretation. This BAA shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy and Security Rule and applicable state and federal laws. The parties agree that any ambiguity in BAA will be resolved in favor of a meaning that permits the CE to comply with and be consistent with HIPAA, the HITECH Act, and the Privacy and Security Rule. The parties further agree that where this BAA conflicts with a contemporaneously executed confidentiality agreement between the parties, this BAA controls.

11. No Private Right of Action Created. This BAA does not create any right of action or benefits for individuals whose PHI is disclosed in violation of HIPAA, the HITECH Act, the Privacy and Security Rule or other law relating to security or privacy.

12. Privacy and Security Point of Contact. All communications occurring because of this BAA shall be sent to HSS-Security@alaska.gov in addition to the CE.

In witness thereof, the parties hereto have duly executed this BAA as of the effective date of the executed contract.

For any additional information, please contact:
Joshua Hartman
Contracting Officer
Joshua.Hartman@alaska.gov