

<b>AMENDMENT OF SOLICITATION / MODIFICATION OF CONTRACT</b>			1. Contract Number CW85535	Page of Pages 1   25		
2. Amendment/Modification Number  M0002	3. Effective Date  See 16c.	4. Requisition/Purchase Request No.  RK149279	5. Solicitation Caption Fraud Case Management and Data Analytics System Subscription			
6. Issued by: Office of Contracting and Procurement Information Technology Group 441 4 <sup>th</sup> Street, NW, Suite 330S Washington, DC 20001		Code <input type="checkbox"/>	7. Administered by (If other than line 6) D.C. Department of Human Services 64 New York Ave NE Washington, DC 20002			
8. Name and Address of Contractor (No. street, city, county, state, and zip code)  Pondera Solutions, LLC 80 Blue Ravine Road, Suite 250 Folsom, CA 95630		9A. Amendment of Solicitation No.				
		9B. Dated (See Item 11)				
		X	10A. Modification of Contract/Order No. CW85535			
			10B. Dated (See Item 13) 10/06/2020			
11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS						
<input type="checkbox"/> The above numbered solicitation is amended as set forth in item 14. The hour and date specified for receipt of Offers <input type="checkbox"/> is extended. <input type="checkbox"/> is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15 and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) BY separate letter or fax which includes a reference to the solicitation and amendment number. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such may be made by letter or fax, provided each letter or telegram refers to the solicitation and this amendment, and is received prior to the opening hour and date specified.						
12. Accounting and Appropriation Data (If Required)						
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS; IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14						
A. This change order is issued pursuant to (Specify Authority): The changes set forth in Item 14 are made in the contract/order no. in item 10A.						
B. The above numbered contract/order is modified to reflect the administrative changes (such as changes in paying office, appropriation data etc.) set forth in item 14, pursuant to the authority of 27 DCMR, Chapter 36, Section 3601.2.						
X C. This supplemental agreement is entered into pursuant to authority of: 27 DCMR 3601.2 (c) Bilateral Contract Modification and agreement between the parties.						
D. Other (Specify type of modification and authority) 27 DCMR Chapter 20, Section 2008 Exercise of Option						
<b>E. IMPORTANT:</b> Contractor <input type="checkbox"/> is not <input checked="" type="checkbox"/> is required to sign this document and return <u>1</u> copy to the issuing office.						
14. Description of Amendment/Modification (Organized by UCF Section headings, including solicitation/contract subject matter where feasible.)  Contract CW85535 is hereby modified to include the following list of attachments to incorporated into the contract by reference:  1. Attachment J.5. HIPPA Business Associate Compliance Clauses. 2. Attachment J.6. Addendum to Business Associate Compliance Agreement Clause for the Department of Human Services Fraud Case Management and Data Analytics System.  All other terms and conditions remain unchanged.						
Except as provided herein, all terms and conditions of the document is referenced in Item 9A or 10A remain unchanged and in full force and effect.						
15A. Name and Title of Signer (Type or print)  Sharie A. Kirsch, Sr. Vice President		16A. Name of Contracting Officer Brenda Allen				
15B. Name of Contractor Pondera Solutions, LLC <i>Sharie A. Kirsch</i> (Signature of person authorized to sign)	15C. Date Signed 06/23/21	16B. District of Columbia <i>Brenda Allen</i> (Signature of Contracting Officer)		16C. Date Signed 6/23/2021		

<b>AMENDMENT OF SOLICITATION / MODIFICATION OF CONTRACT</b>	1. Contract Number	Page of Pages	
	CW85535-M0002	2	25

**CONTRACT SUMMARY**

<b>Contract Period</b>	<b>Type of Modification</b>	<b>Period of Performance</b>	<b>Price</b>
Base Year	Contract Award	October 6, 2020 through October 5, 2021	\$295,000.00
Base Year: M0001	Administrative Change of Contracting Officer	January 25, 2021	\$0.00
Base Year: M0002	Bilateral Contract Modification: Incorporation of HIPPA Business Associate Compliance and BAA Agreements	April 14, 2021	\$0.00
<b>Contract Total Value</b>			<b>\$295,000.00</b>

## HIPAA BUSINESS ASSOCIATE COMPLIANCE AGREEMENT CLAUSE

For the purpose of this Business Associate Agreement (“BAA”) clause, D.C. **Department of Human Services (DHS), Office of Program Review, Monitoring and Investigation (OPRMI)**, a covered component within the District of Columbia’s (“District”) Hybrid Entity will be referred to as a “Covered Entity” as that term is defined by the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”) and associated regulations promulgated at 45 C.F.R. §§ 160, 162 and 164 as amended (the “HIPAA Regulations”) and **Pondera Solutions, LLC**, as a recipient of Protected Health Information (“PHI”) or electronic PHI from **DHS OPRMI** is a “Business Associate” as that term is defined by HIPAA.

Terms used, but not otherwise defined, in this BAA shall have the same meaning as those terms in the HIPAA Regulations.

### 1. Definitions

- a. *Business Associate* means a person or entity, who, on behalf of the District or of an Organized Health Care Arrangement (as defined in this section) in which the Covered Entity participates, but other than in the capacity of a member of the Workforce of the District government or Organized Health Care Arrangement, creates, receives, maintains, or transmits PHI for a function or activity for the District, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R § 3.20, billing, benefit management, practice management, and repricing; or provides, other than in the capacity of a member of the Workforce of such Covered Entity, legal, actuarial, accounting, consulting, Data Aggregation (as defined in 45 C.F.R § 164.501), management, administrative, accreditation, or financial services to or for the District, or to or for an Organized Health Care Arrangement in which the District participates, where the provision of the service involves the disclosure of PHI from the District or arrangement, or from another Business Associate of the District or arrangement, to the person. A Covered Entity may be a Business Associate of another Covered Entity.

A Business Associate includes, (i) a Health Information Organization, e-prescribing gateway, or other person that provides data transmission services with respect to PHI to a Covered Entity and that requires access on a routine basis to such PHI; (ii) a person that offers a personal health record to one or more individuals on behalf of the District; (iii) a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate.

A *Business Associate* does not include: (i) a health care provider, with respect to disclosures by a Covered Entity to the health care provider concerning the treatment of the individual; (ii) a plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or health maintenance organization, HMO, with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 C.F.R § 164.504(f) apply and are met; (iii) a government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law; (iv) a Covered Entity participating in an Organized Health Care Arrangement that performs a function, activity or service included in the definition of a Business Associate above for or on behalf of such Organized Health Care Arrangement.

- b. *Covered Entity* means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by 45 C.F.R. §§ 160 and 164. With respect to this BAA, *Covered Entity* shall also include the designated Health Care Components of the District government's Hybrid Entity or a District agency following HIPAA's implementing regulations and best practices.
- c. *Covered Functions* means those functions of a Covered Entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.
- d. *Data Aggregation* means, with respect to PHI created or received by a Business Associate in its capacity as the Business Associate of a Covered Entity, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in its capacity as a Business Associate of another Covered Entity, to permit data analyses that relate to the health care operations of the respective Covered Entities.
- e. *Designated Record Set* means a group of records maintained by or for a Covered Entity that are:
  - i. The medical records and billing records about individuals maintained by or for a covered health care provider,
  - ii. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
  - iii. Records used, in whole or in part, by or for the Covered Entity to make decisions about individuals.
- f. *Health Care* means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:
  - i. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
  - ii. Sale or dispensing of a drug, device, equipment, or other item in accordance with the prescription.
- g. *Health Care Components* means a component or a combination of components of a Hybrid Entity designated by a Hybrid Entity in accordance with 45 CFR § 164.105(a)(2)(iii)(D). *Health Care Components* must include non-Covered Functions that provide services to the Covered Functions for the purpose of facilitating the sharing of PHI with such functions of the Hybrid Entity without Business Associate agreements or individual authorizations.
- h. *Health Care Operations* shall include (1) conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 C.F.R. § 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (2) reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification,

licensing, or credentialing activities; (3) except as prohibited under 45 C.F.R. § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 C.F.R. § 164.514(g) are met, if applicable; (4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (6) business management and general administrative activities of the entity, including, but not limited to: (i) management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer; (iii) resolution of internal grievances; (iv) The sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and (v) consistent with the applicable requirements of 45 C.F.R. § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the Covered Entity..

- i. *Hybrid Entity* means a single legal entity that is a Covered Entity and whose business activities include both covered and non-Covered Functions, and that designates Health Care Components, in accordance with 45 C.F.R. § 164.105(a)(2)(iii)(C). A *Hybrid Entity* is required to designate Health Care Components, any other components of the entity that provide services to the Covered Functions for the purpose of facilitating the sharing of PHI with such functions of the Hybrid Entity without Business Associate agreements or individual authorizations. The District is a Hybrid Covered Entity. Hybrid Entities are required to designate and include functions, services and activities within its own organization, which would meet the definition of Business Associate and irrespective of whether performed by employees of the Hybrid Entity, as part of its Health Care Components for compliance with the Security Rule and privacy requirements under this BAA.
- j. *Individual* shall mean the person who is the subject of PHI in accordance with 45 C.F.R. § 160.103. The term *individual* shall also include the individual's personal representative in accordance with 45 C.F.R. § 164.502(g).
- k. *Individually Identifiable Health Information* shall mean information that is a subset of health information, including demographic information collected from an individual and,
  - i. Is created or received by a health care provider, health plan, employer, or health care clearinghouse,
  - ii. Relates to the past, present, or future physical or mental health or condition of an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - iii. That identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- l. *National Provider Identifier (NPI)* shall mean the Standard Unique Health Identifier for Healthcare Providers as defined at 42 C.F.R. § 162.406.

- m. *Organized Health Care Arrangement* shall mean (1) a clinically integrated care setting in which individuals typically receive health care from more than one health care provider; (2) an organized system of health care in which more than one Covered Entity participates and in which the participating Covered Entities: (i) hold themselves out to the public as participating in a joint arrangement; and (ii) participate in joint activities that include at least one of the following: (a) utilization review, in which health care decisions by participating Covered Entities are reviewed by other participating Covered Entities or by a third party on their behalf; (b) quality assessment and improvement activities, in which treatment provided by participating Covered Entities is assessed by other participating Covered Entities or by a third party on their behalf; or (c) payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating Covered Entities through the joint arrangement and if PHI created or received by a Covered Entity is reviewed by other participating Covered Entities or by a third party on their behalf for the purpose of administering the sharing of financial risk in accordance with 42 C.F.R. § 160.103.
- n. *Personal Representative*: shall mean a person authorized, under District or other applicable law, to act on behalf of the subject of PHI in accordance with 42 C.F.R. § 164.502(g).
- o. *Privacy and Security Official*: shall mean the person or persons designated by the District, a Hybrid Entity, who is/are responsible for developing, maintaining, implementing, and enforcing the District-wide Privacy Policies and Procedures, and for overseeing full compliance with HIPAA Regulations, and other applicable federal and state privacy laws.
- p. *Privacy Officer* shall mean the person designated by the District's Privacy and Security Official or one of the District's covered components within its Hybrid Entity, who is responsible for overseeing compliance with a Covered Agency's Privacy Policies and Procedures, the HIPAA Regulations, and other applicable federal and state privacy laws. Also referred to as the agency Privacy Officer, the individual shall follow the guidance of the District's Privacy and Security Official and shall be responsive to and report to the District's Privacy and Security Official on matters pertaining to HIPAA compliance.
- q. *Privacy Rule* shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. parts 160 and 164, subparts A and E.
- r. *Protected Health Information ("PHI")* means individually identifiable health information, including electronic information ("ePHI"), that is created or received by the Business Associate from or on behalf of the Covered Entity, or agency following HIPAA best practices, which is:
- i. Transmitted by, created, or maintained in electronic media; or
  - ii. Transmitted or maintained in any other form or medium.
  - iii. PHI or ePHI does not include individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g; (ii) In records described at 20 U.S.C. § 1232(g)(a)(4)(B)(iv); (iii) In employment records held by a Covered Entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years.
- s. *Record* shall mean any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity.

- t. *Required By Law* means a mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits pursuant to 45 C.F.R. § 164.103.
- u. *Secretary* means the person serving as Secretary of the United States Department of Health and Human Services (HHS) or any other officer or employee of HHS to whom the authority involved has been delegated.
- v. *Security Officer* means the person designated by the Security Official or one of the District of Columbia's designated Health Care Components, who is responsible for overseeing compliance with the Covered Agency's Privacy Policies and Procedures, the Security Rules, and other applicable federal and state privacy law(s). The Covered Agency's security officer shall follow the guidance of the District's Security Official, as well as the Associate Security Official within the Office of the Chief Technology Officer and shall be responsive to the same on matters pertaining to HIPAA compliance.
- w. *Security Rule* shall mean the Standards for Security of Individually Identifiable Health Information at 45 C.F.R. parts 160, 162 and 164, subpart C.
- x. Unsecured PHI shall mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the U.S. Department of Health and Human Services Secretary in the guidance issue under § 13402(h)(2) of the Health Information Technology Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA)(Pub.L 111-5, 123 Stat 115), approved February 17, 2009.
- y. *Workforce* shall mean employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of such Covered Entity, whether or not they are paid by the Covered Entity or Business Associate.

## 2. Obligations and Activities of Business Associate

Business Associate agrees to comply with applicable federal and District confidentiality and security laws, including, but not limited to the Privacy Rule and Security Rule and the following:

- a. Business Associate agrees not to use or disclose PHI or ePHI (other than as permitted or required by this BAA or as Required by Law).
- b. Business Associate agrees to use appropriate safeguards and comply with administrative, physical, and technical safeguards requirements described at 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316 as required by § 13401 of the Health Information Technology Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009 ("ARRA")(Pub.L 111-5, 123 Stat 115) approved February 17, 2009, to maintain the security of the PHI and to prevent use or disclosure of such PHI other than as provided for by this BAA.

Business Associate acknowledges that, pursuant § 13401, Business Associate must comply with the Security Rule and privacy provisions detailed in this BAA.

The additional requirements of § 13401 of HITECH that relate to security and apply to a Covered Entity shall also apply to Business Associate and shall be incorporated into an agreement between the Business Associate and the Covered Entity. Business Associate shall be directly liable for any violations of this BAA or HIPAA Regulations. A summary of HIPAA Security Standards for the Protection of ePHI, found at Appendix A to Subpart C or 45 C.F.R. Part 164 is as follows:

### Administrative Safeguards

Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)



Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)

### Physical Safeguards

Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

### Technical Safeguards (see § 164.312)

Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)

Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

- c. The Business Associate agrees to name a Privacy and/or Security Officer who is accountable for developing, maintaining, implementing, overseeing the compliance of, and enforcing compliance with this BAA, the Security Rule and other applicable federal and state privacy law within the Business Associate’s business. The Business Associate reports violations and conditions to the District-wide Privacy and Security Official and/or the Agency Privacy Officer of the covered component within the District’s Hybrid Entity.
- d. The Business Associate agrees to establish procedures for mitigating, and to mitigate to the extent practicable, any deleterious effects that are known to the Business Associate of a use or disclosure of PHI by the Business Associate in violation of the requirements of this BAA.
- e. The Business Associate agrees to report to Covered Entity, in writing, any use or disclosure of the PHI not permitted or required by this BAA or other incident or condition arising out the Security Rule, including breaches of unsecured PHI as required at 45 C.F.R § 164.410, to the District-wide Privacy and Security Official or agency Privacy Officer within ten (10) business days from the time the Business Associate becomes aware of such unauthorized use or disclosure. However, if the Business Associate is an agent of the District (i.e., performing delegated essential governmental functions), the Business Associate must report the incident or condition immediately. Upon the determination of an actual data breach, and in consultation with the District’s Privacy and Security Official, the Business Associate will handle breach notifications to individuals, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), and potentially the media, on behalf of the District.
- f. The Business Associate agrees to ensure that any Workforce member or any agent, including a subcontractor, agrees to the same restrictions and conditions that apply through this BAA with respect to PHI received from the Business Associate, PHI created by the Business Associate, or PHI received by the Business Associate on behalf of the Covered Entity.
- g. In accordance with 45 C.F.R §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information

- h. Initially, within ten (10) business days following the commencement of this Contract, or within ten (10) business days of a new or updated agreement with a subcontractor, the Business Associate agrees to provide the District a list of all subcontractors who meet the definition of a Business Associate. Additionally, Business Associate agrees to ensure its subcontractors understanding of liability and monitor, where applicable, compliance with the Security Rule and applicable privacy provisions in this BAA.
- i. The Business Associate agrees to provide access within five (5) business days, at the request of the Covered Entity or an Individual, **at a mutually agreed upon location, during normal business hours, and in a format** as directed by the District Privacy Official or agency Privacy Officer, or as otherwise mandated by the Privacy Rule or applicable District laws, rules and regulations, to PHI in a Designated Record Set, to the Covered Entity or an Individual, to facilitate the District's compliance with the requirements under 45 C.F.R. §164.524.
- j. The Business Associate agrees to make any amendment(s) within five (5) business days to the PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 **in a format** consistent with agreed upon data layout previously provided to the BA or as directed by the District Privacy Official or agency Privacy Officer in order to facilitate the District's compliance with the requirements under 45 C.F.R. §164.526.
- k. The Business Associate agrees to use the standard practices of the Covered Entity to verify the identification and authority of an Individual who requests the PHI in a Designated Record Set of a recipient of services from or through the Covered Entity.
- l. The Business Associate agrees to record authorizations and log such disclosures of PHI and information related to such disclosures as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and applicable District laws, rules and regulations.
- m. The Business Associate agrees to provide to the Covered Entity or an Individual, within ten business days of a request **at a mutually agreed upon location, during normal business hours, and in a format designated** by the District's Privacy and Security Official or agency Privacy Officer and the duly authorized Business Associate Workforce member, information collected in accordance with Paragraph (i) of this Section above, to permit the Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528, and applicable District laws, rules and regulations.
- n. The Business Associate agrees to make internal practices, books, and records, including policies and procedures, and PHI, relating to the use and disclosure of PHI received from the Business Associate, or created, or received by the Business Associate on behalf of the Covered Entity, available to the Covered Entity, or to the Secretary, within ten business days of their request and **at a mutually agreed upon location, during normal business hours, and in a format designated** by the District Privacy and Security Official or agency Privacy Officer and the duly authorized Business Associate Workforce member, or in a time and manner designated by the Secretary, for purposes of the Secretary in determining compliance of the Covered Entity with the Privacy Rule.
- o. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R Part 164, the Business Associate agrees to comply with the

requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).

- p. As deemed necessary by the District, the Business Associate agrees to the monitoring and auditing of items listed in paragraph 2 of this BAA, as well as data systems storing or transmitting PHI, to verify compliance.
- q. The Business Associate may aggregate PHI in its possession with the PHI of other Covered Entities that Business Associate has in its possession through its capacity as a Business Associate to other Covered Entities provided that the purpose of the Data Aggregation is to provide the Covered Entity with data analyses to the Health Care Operations of the Covered Entity. Under no circumstances may the Business Associate disclose PHI of one Covered Entity to another Covered Entity absent the explicit written authorization and consent of the Privacy Officer/Liaison or a duly authorized Workforce member of the Covered Entity.
- r. Business Associate may de-identify any and all PHI provided that the de-identification conforms to the requirements of 45 C.F.R. § 164.514(a)-(b) and any associated HHS guidance. Pursuant to 45 C.F.R. § 164.502(d)(2), de-identified information does not constitute PHI and is not subject to the terms of this BAA.
- s. If the Business Associate has not submitted the District's Business Associate Questionnaire prior to contract award, the Business Associate shall file the Questionnaire with the Agency Privacy Officer/Liaison or the Agency Contract Administrator within thirty calendar days after contract award. Business Associate shall file and submit an updated Questionnaire to the Agency Privacy Officer/Liaison or the Agency Contract Administrator on or before October 1<sup>st</sup> of each contract year. At the discretion of the Agency Privacy Officer/Liaison, Business Associates with limited access to PHI may be granted a written waiver to file a letter attesting to their HIPAA compliance on or before October 1<sup>st</sup> of each contract year. A copy of the Business Associate Questionnaire can be located at [www.ocp.dc.gov/OCP Solicitations /Required Solicitation Documents](http://www.ocp.dc.gov/OCP/Solicitations/RequiredSolicitationDocuments).

### 3. Permitted Uses and Disclosures by the Business Associate

- a. Except as otherwise limited in this BAA, the Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, the Covered Entity as specified in the Contract, provided that such use or disclosure would not violate Subpart E of 45 C.F.R Part 164 if the same activity were performed by the Covered Entity or would not violate the minimum necessary policies and procedures of the Covered Entity.
- b. Except as otherwise limited in this BAA, the 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.
- c. Except as otherwise limited in this BAA, the Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that the disclosures are Required By Law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used, or further disclosed, only as Required By Law, or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it has knowledge that the confidentiality of the information has been breached.

- d. Except as otherwise limited in this BAA, the Business Associate may use PHI to provide Data Aggregation services to the Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).
- e. Business Associate may use PHI to report violations of this BAA or the HIPAA Regulations to the appropriate federal and District of Columbia authorities, consistent with 45 C.F.R. § 164.502(j)(1)-(2).

4. Additional Obligations of the Business Associate

- a. Business Associate shall submit a written report to the Covered Entity that identifies the files and reports that constitute the Designated Record Set of the Covered Entity. Business Associate shall submit said written report to the Privacy Officer no later than thirty (30) business days after the commencement of this BAA. In the event that Business Associate utilizes new files or reports which constitute the Designated Record Set, Business Associate shall notify the Covered Entity of said event within thirty (30) days of the commencement of the file's or report's usage. The Designated Record Set file shall include, but not be limited to the identity of the following:
  - i. Name of the Business Associate of the Covered Entity,
  - ii. Title of the Report/File,
  - iii. Confirmation that the Report/File contains PHI(Yes or No),
  - iv. Description of the basic content of the Report/File,
  - v. Format of the Report/File (Electronic or Paper),
  - vi. Physical location of Report/File,
  - vii. Name and telephone number of current member(s) of the Workforce of the Covered Entity or other District Government agency responsible for receiving and processing requests for PHI; and
  - viii. Supporting documents if the recipient/personal representative has access to the Report/File.
- b. Business Associate must provide assurances to the Covered Entity that it will continue to employ sufficient administrative, technical, and physical safeguards, as described under the Security Rule, to protect and secure (the Covered Entity's) ePHI entrusted to it. These safeguards include:
  - i. The Business Associate agrees to administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that the Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity.
  - ii. The Business Associate agrees to report to the Covered Entity any security incident of which it becomes aware, including any attempts to access ePHI, whether those attempts were successful or not.
  - iii. This BAA may be terminated if the Covered Entity determines that the Business Associate has materially breached the agreement.

- iv. The Business Associate agrees to make all policies and procedures, and documents relating to security, available to the Secretary of HHS for the purposes of determining the Covered Entity's compliance with HIPAA.
  - v. This BAA continues in force for as long as the Business Associate retains any access to the Covered Entity's ePHI.
  - vi. With respect to the subset of PHI known as electronic PHI (ePHI) as defined by HIPAA Security Standards at 45 C.F.R. §§ 160 and 164, subparts A and C (the "Security Rule"), if in performing the Services, Business Associate, its employees, agents, subcontractors and any other individual permitted by Business Associate will have access to any computer system, network, file, data or software owned by or licensed to Provider that contains ePHI, or if Business Associate otherwise creates, maintains, or transmits ePHI on Provider's behalf, Business Associate shall take reasonable security measures necessary to protect the security of all such computer systems, networks, files, data and software. With respect to the security of ePHI, Business Associate shall: (a) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the Provider; (b) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; and (c) Report to the Provider any security incident of which it becomes aware.
  - vii. Business Associate agrees not to electronically transmit or permit access to PHI unless such transmission or access is authorized by this BAA and further agrees that it shall only transmit or permit such access if such information is secured in a manner that is consistent with applicable law, including the Security Rule. For purposes of this BAA "encrypted" shall mean the reversible conversion of readable information into unreadable, protected form so that only a recipient who has the appropriate "key" can convert the information back into original readable form. If the Covered Entity stores, uses or maintains PHI in encrypted form, or in any other secured form acceptable under the security regulations, Covered Entity shall promptly, at request, provide with the key or keys to decrypt such information and will otherwise assure that such PHI is accessible by upon reasonable request.
  - viii. In the event Business Associate performs functions or activities involving the use or disclosure of PHI on behalf of Covered Entity that involve the installation or maintenance of any software (as it functions alone or in combination with any hardware or other software), Business Associate shall ensure that all such software complies with all applicable standards and specifications required by the HIPAA Regulations and shall inform of any software standards or specifications not compliant with the HIPAA Regulations.
- c. At the request of the Covered Entity, the Business Associate agrees to amend this BAA to comply with all HIPAA mandates.

## 5. Sanctions

Business Associate agrees that its Workforce members, agents, and subcontractors who violate the provisions of HIPAA or other applicable federal or District privacy law will be subject to

discipline in accordance with Business Associate's internal Personnel Policy and applicable collective bargaining agreements. Business Associate agrees to impose sanctions consistent with Business Associate's personnel policies and procedures and applicable collective bargaining agreements with respect to persons employed by it. Members of the Business Associate Workforce who are not employed by Business Associate are subject to the policies and applicable sanctions for violation of this BAA. In the event Business Associate imposes sanctions against any member of its Workforce, agents and subcontractors for violation of the provisions of HIPAA or other applicable federal or District privacy laws, the Business Associate shall inform the District Privacy Official or the agency Privacy Officer/Liaison of the imposition of sanctions.

6. Obligations of the Covered Entity

- a. The Covered Entity shall notify the Business Associate of any limitation(s) in its Notice of Privacy Practices of the Covered Entity in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect the use or disclosure of PHI by the Business Associate.
- b. The Covered Entity shall notify the Business Associate of any changes in, or revocation of, permission by the Individual to the use or disclosure of PHI, to the extent that such changes may affect the use or disclosure of PHI by the Business Associate.
- c. The Covered Entity shall notify the Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect the use or disclosure of PHI by the Business Associate.

7. Permissible Requests by Covered Entity

Covered Entity shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule and Subpart E of 45 C.F.R Part 164 if done by the Covered Entity.

8. Representations and Warranties.

The Business Associate represents and warrants to the Covered Entity:

- a. That it is duly organized, validly existing, and in good standing under the laws of the jurisdiction in which it is organized or licensed, it has the full power to execute this BAA and it, its employees, agents, subcontractors, representatives and members of its Workforce are licensed and in good standing with the applicable agency, board, or governing body to perform its obligations hereunder, and that the performance by it of its obligations under this BAA has been duly authorized by all necessary corporate or other actions and will not violate any provision of any license, corporate charter or bylaws;
- b. That it, its employees, agents, subcontractors, representatives and members of its Workforce are in good standing with the District, that it, its employees, agents, subcontractors, representatives and members of its Workforce will submit a letter of good standing from the District, and that it, its employees, agents, subcontractors, representatives and members of its Workforce have not been de-barred from being employed as a contractor by the federal government or District;
- c. That neither the execution of this BAA, nor its performance hereunder, will directly or indirectly violate or interfere with the terms of another agreement to which it is a party, or give any

governmental entity the right to suspend, terminate, or modify any of its governmental authorizations or assets required for its performance hereunder. The Business Associate represents and warrants to the Covered Entity that it will not enter into any agreement the execution or performance of which would violate or interfere with this BAA,

- d. That it is not currently the subject of a voluntary or involuntary petition in bankruptcy, does not currently contemplate filing any such voluntary petition, and is not aware of any claim for the filing of an involuntary petition,
- e. That all of its employees, agents, subcontractors, representatives and members of its Workforce, whose services may be used to fulfill obligations under this BAA are or shall be appropriately informed of the terms of this BAA and are under legal obligation to the Business Associate, by contract or otherwise, sufficient to enable the Business Associate to fully comply with all provisions of this BAA. Modifications or limitations that the Covered Entity has agreed to adhere to with regards to the use and disclosure of PHI of any individual that materially affects or limits the uses and disclosures that are otherwise permitted under the Privacy Rule will be communicated to the Business Associate, in writing, and in a timely fashion;
- f. That it will reasonably cooperate with the Covered Entity in the performance of the mutual obligations under this Agreement,
- g. That neither the Business Associate, nor its shareholders, members, directors, officers, agents, subcontractors, employees or members of its Workforce have been excluded or served a notice of exclusion or have been served with a notice of proposed exclusion, or have committed any acts which are cause for exclusion, from participation in, or had any sanctions, or civil or criminal penalties imposed under, any federal or District healthcare program, including but not limited to Medicare or Medicaid, or have been convicted, under federal or District law (including without limitation following a plea of *nolo contendere* or no contest or participation in a first offender deferred adjudication or other arrangement whereby a judgment of conviction has been withheld), of a criminal offense related to (a) the neglect or abuse of a patient, (b) the delivery of an item or service, including the performance of management or administrative services related to the delivery of an item or service, under a federal or District healthcare program, (c) fraud, theft, embezzlement, breach of fiduciary responsibility, or other financial misconduct in connection with the delivery of a healthcare item or service or with respect to any act or omission in any program operated by or financed in whole or in part by any federal, state, or local government agency (d) the unlawful, manufacture, distribution, prescription or dispensing of a controlled substance, or (e) interference with or obstruction of any investigation into any criminal offense described in (a) through (d) above. The Business Associate further agrees to notify the Covered Entity immediately after the Business Associate becomes aware that any of the foregoing representations and warranties may be inaccurate or may become incorrect

9. Term and Termination

- a. *Term.* The requirements of this BAA shall be effective as of the date of the contract award, and shall terminate when all of the PHI provided by the Covered Entity to the Business Associate, or created or received by the Business Associate on behalf of the Covered Entity, is confidentially destroyed or returned to the Covered Entity within five (5) business days of its request. The PHI shall be returned in a format mutually agreed upon by and between the Privacy Official and/or Privacy Officer or their designee and the appropriate and duly authorized Workforce member of the Business Associate.; If it is infeasible to return or confidentially destroy the PHI, protections



shall be extended to such information, in accordance with the termination provisions in this Section and communicated to the Privacy Official or Privacy Officer or their designee. The requirement to return PHI to the District at the end of the contract term or if the contract is terminated applies irrespective of whether the Business Associate is also a Covered Entity under HIPAA. Where a Business Associate is also a Covered Entity, PHI provided by the District, or created or received by the Business Associate on behalf of the District, a duplicate of the record may be acceptable if mutually agreed.

b. *Termination for Cause.* Upon the Covered Entity's knowledge of a material breach of this BAA by the Business Associate, the Covered Entity shall either:

- i. Provide an opportunity for the Business Associate to cure the breach within a period of ten (10) days (or such longer period as the District may authorize in writing) after receipt of notice from the Contracting Officer specifying such failure or end the violation and terminate the Contract if the Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity; or
- ii. Immediately terminate the Contract if the Business Associate breaches a material term of this BAA and a cure is not possible.

If neither termination nor cure is feasible, the Covered Entity shall report the violation to the Secretary of HHS.

c. *Effect of Termination.*

- i. Except as provided in paragraph (ii) of this section, upon termination of the Contract, for any reason, the Business Associate shall **confidentially destroy** all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity within thirty business days of termination. This provision shall apply to PHI that is in the possession of ALL subcontractors, agents, or Workforce members of the Business Associate. The Business Associate shall retain no copies of PHI in any form.
- ii. In the event that the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide written notification to the Covered Entity of the conditions that make the return or confidential destruction infeasible. Upon determination by the agency Privacy Officer/Liaison that the return or confidential destruction of the PHI is infeasible, the Business Associate shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI for so long as the Business Associate maintains such PHI. Additionally, the 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 Covered Entity [or, if agreed to by Covered Entity, destroy] the remaining PHI that the Business Associate still maintains in any form,
  - (3) Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to ePHI to prevent use or disclosure of the PHI, other than as provided for in this section, for as long as Business Associate retains the PHI,

- (4) Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at [Insert section number related to paragraph (under “Permitted Uses and Disclosures By The Business Associate”)] which applied prior to termination; and
- (5) Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

The obligations outlined in Section 2. Obligations and Activities of Business Associate shall survive the termination of this Contract.

## 10. Miscellaneous

- a. *Regulatory References.* A reference in this BAA to a section in the Privacy Rule means the section as in effect or as amended.
- b. *Amendment.* A Covered Entity and Business Associate (“the Parties”) agree to take such action as is necessary to amend this BAA from time to time as is necessary for the Covered Entity to comply with the requirements of the Privacy Rule and HIPAA Regulations. Except for provisions Required By Law as defined herein, no provision hereof shall be deemed waived unless in expressed in writing and signed by duly authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any other right or remedy under this BAA.
- c. *Survival.* The respective rights and obligations of the Business Associate under Section 9. Term and Termination of this HIPAA Compliance BAA and Sections 9 and 20 of the Standard Contract Provisions for use with the District of Columbia Government Supply and Services Contracts shall survive termination of the Contract.
- d. *Interpretation.* Any ambiguity in this BAA shall be resolved to permit compliance with applicable federal and District laws, rules and regulations, and the HIPAA Rules, and any requirements, rulings, interpretations, procedures, or other actions related thereto that are promulgated, issued or taken by or on behalf of the Secretary; provided that applicable federal and District laws, rules and regulations shall supersede the Privacy Rule if, and to the extent that they impose additional requirements, have requirements that are more stringent than or provide greater protection of patient privacy or the security or safeguarding of PHI than those of the HIPAA Regulations.

The terms of this BAA amend and supplement the terms of the Contract. In the event of a conflict between the terms of the BAA and the terms of the Contract, the terms of this BAA shall control; provided, however, that this BAA shall not supersede any other federal or District law or regulation governing the legal relationship of the Parties, or the confidentiality of records or information, except to the extent that the Privacy Rule preempts those laws or regulations. In the event of any conflict between the provisions of the Contract (as amended by this BAA) and the Privacy Rule, the Privacy Rule shall control.

- e. *No Third-Party Beneficiaries.* The Covered Entity and the Business Associate are the only parties to this BAA and are the only parties entitled to enforce its terms. Except for the rights of Individuals, as defined herein, to have access to and amend their PHI, and to an accounting of the uses and disclosures thereof, in accordance with paragraphs (2)(f), (g) and (j) of this BAA, nothing

in the BAA gives, is intended to give, or shall be construed to give or provide any benefit or right, whether directly, indirectly, or otherwise, to third persons.

- f. *Compliance with Applicable Law.* The Business Associate shall comply with all federal and District laws, regulations, executive orders, and ordinances, as they may be amended from time to time during the term of this BAA and the Contract; to the extent they are applicable to this BAA and the Contract.
- g. *Governing Law and Forum Selection.* This Contract shall be construed broadly to implement and comply with the requirements relating to the Privacy Rule, and other applicable laws and regulations. All other aspects of this Contract shall be governed under the laws of the District. The Covered Entity and the Business Associate agree that all disputes which cannot be amicably resolved by the Covered Entity and the Business Associate regarding this BAA shall be litigated before the District of Columbia Contract Appeals Board, the District of Columbia Court of Appeals, or the United States District Court for the District of Columbia having jurisdiction, as the case may be. The Covered Entity and the Business Associate expressly waive any and all rights to initiate litigation, arbitration, mediation, negotiations and/or similar proceedings outside the physical boundaries of the District of Columbia and expressly consent to the jurisdiction of the above tribunals.
- h. *Indemnification.* The Business Associate shall indemnify, hold harmless and defend the Covered Entity from and against any and all claims, losses, liabilities, costs, and other expenses incurred as a result or arising directly or indirectly out of or in connection with (a) any misrepresentation, breach of warranty or non-fulfillment of any undertaking of the Business Associate under this BAA; and (b) any claims, demands, awards, judgments, actions and proceedings made by any person or organization, arising out of or in any way connected with the performance of the Business Associate under this BAA.
- i. *Injunctive Relief.* Notwithstanding any rights or remedies under this BAA or provided by law, the Covered Entity retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of PHI by the Business Associate, its Workforce, any of its subcontractors, agents, or any third party who has received PHI from the Business Associate.
- j. *Assistance in litigation or administrative proceedings.* The Business Associate shall make itself and any agents, affiliates, subsidiaries, subcontractors or its Workforce assisting the Business Associate in the fulfillment of its obligations under this HIPAA Compliance BAA and the Contract, available to the Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Covered Entity, its directors, officers or employees based upon claimed violation of HIPAA, the Privacy Rule or other laws relating to security and privacy, except where the Business Associate or its agents, affiliates, subsidiaries, subcontractors or its Workforce are a named adverse party.
- k. *Notices.* Any notices between the Parties or notices to be given under this BAA shall be given in writing and delivered by personal courier delivery or overnight courier delivery, or by certified mail with return receipt requested, to the Business Associate or to the Covered Entity, to the addresses given for each Party below or to the address either Party hereafter gives to the other Party. Any notice, being addressed and mailed in the foregoing manner, shall be deemed given five (5) business days after mailing. Any notice delivered by personal courier delivery or overnight courier delivery shall be deemed given upon notice upon receipt.

If to the Business Associate, to

If to the Covered Entity, to

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Attention: \_\_\_\_\_

Attention: \_\_\_\_\_

Fax: \_\_\_\_\_

Fax: \_\_\_\_\_

- l. *Headings.* Headings are for convenience only and form no part of this BAA and shall not affect its interpretation.
- m. *Counterparts; Facsimiles.* This BAA may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.
- n. *Successors and Assigns.* The provisions of this BAA shall be binding upon and shall inure to the benefit of the Parties hereto and their respective successors and permitted assigns, if any.
- o. *Severance.* In the event that any provision of this BAA is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this BAA will remain in full force and effect. In addition, in the event a Party believes in good faith that any provision of this BAA fails to comply with the then-current requirements of the Privacy Rule, such party shall notify the other Party in writing, in the manner set forth in Section 10. Miscellaneous, Paragraph k. Notices. Within ten (10) business days from receipt of notice, the Parties shall address in good faith such concern and amend the terms of this BAA, if necessary, to bring the contested provision(s) into compliance.
- p. *Independent Contractor.* The Business Associate will function as an independent contractor and shall not be considered an employee of the Covered Entity for any purpose. Nothing in this BAA shall be interpreted as authorizing the Business Associate Workforce, its subcontractor(s) or its agent(s) or employee(s) to act as an agent or representative for or on behalf of the Covered Entity.
- q. *Entire Agreement.* This BAA, as may be amended from time to time pursuant to Section 10. Miscellaneous, Paragraph b. Amendment, which incorporates by reference specific procedures from the District of Columbia Department of Health Privacy Policy Operations Manual, constitutes the entire agreement and understanding between the Parties and supersedes all prior oral and written agreements and understandings between them with respect to applicable District and federal laws, rules and regulations, HIPAA and the Privacy Rule, and any rules, regulations, requirements, rulings, interpretations, procedures, or other actions related thereto that are promulgated, issued or taken by or on behalf of the Secretary of HHS.

Attachments:

Exhibit J.5 Identity and Procedure Verification

**Addendum to Business Associate Compliance Agreement Clause for Contract CW85535  
Fraud Case Management System for DHS**

**Background**

The parties to this Addendum, The District of Columbia (“District”) Department of Human Services (“DHS”), a governmental entity, and Pondera Solutions (“Pondera”), a corporate entity, entered into a procurement contract on October 5, 2020. The Contract is identified as CW85535.

In its agreement with DHS, Pondera agreed to design an information technology system (“System”) to assist DHS’ Office of Program Review, Monitoring and Investigation (“OPRMI”). The System will be an integrated, user friendly solution to enhance public assistance fraud detection and reporting capabilities for DHS and support compliance with all Federal and District laws, regulations, and policies. The System will provide subscription-based Software-as-a-Service (SaaS) access to the benefits fraud case management and data analytics system.

In designing and implementing this System, Pondera will require access to sensitive and confidential data contained both in electronic and non-electronic format. This data contains both Protected Health Information (“PHI”) and Personally Identifying Information (“PII”) from data protected by Federal and District law. The OPRMI confidential data includes information from the District’s Medicaid, Supplemental Nutrition Assistance Program (“SNAP”) and Temporary Assistance for Needy Families (“TANF”) programs.

Pondera has signed the District’s HIPAA BUSINESS ASSOCIATE COMPLIANCE ADDENDUM CLAUSE (“BAA”) attached to this Addendum, which is incorporated into this Addendum by reference. This BAA provides for the handling of all PHI in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

**B. Applicable Laws:**

The applicable confidentiality laws include:

[SNAP - 7 C.F.R. § 272.1 \(Lexis Advance through March 8, 2021 issue of the Federal Register, with the exception of the amendments appearing at 86 FR 13191 and 86 FR 13200\)](#)

[Medicaid – 42 U.S.C.S. § 1396a Sec. 1902 \(LexisNexis, Lexis Advance through Public Law 116-313, approved January 5, 2021, with gaps of Public Law 116-260 and Public Law 116-283\)](#)

[42 C.F.R. § 431.302 \(Lexis Advance through March 8, 2021 issue of the Federal Register, with the exception of the amendments appearing at 86 FR 13191 and 86 FR 13200\)](#)

[42 C.F.R. § 431.306 \(Lexis Advance through March 8, 2021 issue of the Federal Register, with the exception of the amendments appearing at 86 FR 13191 and 86 FR 13200\)](#)

Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 CFR [Part 160](#) and Subparts A and E of [Part 164](#). All references to the “HIPAA Security and Privacy Rule” are deemed to include all amendments to such rule in the HITECH Act, and the HIPAA Final Omnibus Rule of 2013, and any regulations, and any other adopted amendments or regulations.

TANF - 42 U.S.C. § 602(a)(1)(A)(iv). [42 U.S.C.S. § 602 \(LexisNexis, Lexis Advance through Public Law 116-313, approved January 5, 2021, with gaps of Public Law 116-260 and Public Law 116-283\)](#)

DC Public Benefit Confidentiality – D.C. Code §4-209.04 - [D.C. Code § 4-209.04](#) (2021).

## C. Definitions

- 1.1 The term “Confidential Information” means any data or information proprietary to DHS and not generally known to the public, whether in tangible or intangible form, in whatever medium provided, whether unmodified or modified by Pondera or its agents or representatives (as defined herein), whenever and however disclosed, including, but not limited to: SNAP Data, Medicaid Data, TANF Data, PHI, or PII (which are defined herein).
- 1.2 The term “Electronic Protected Health Information” means Protected Health Information transmitted by Electronic Media (as defined in the HIPAA Security and Privacy Rule) or maintained in Electronic Media.
- 1.3 The term “Medicaid Data” means any information relating to the PII of recipients of the District and Federal benefit program known as the Medicaid Assistance Program for low-income individuals and is embodied in 42 U.S.C. § 1396 *et seq.*
- 1.4 The term “Protected Health Information (“PHI”)” means individually identifiable health information including, without limitation, all information, data, documentation, and materials, including without limitation, demographic, medical and financial information, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can identify the individual. “Protected Health Information” includes without limitation “Electronic Protected Health Information” as defined below.
- 1.5 The term “Personally Identifiable Information (PII)” is any data that could be used to identify a particular person. Examples include a full name and Social Security Number.
- 1.6 The term “Record” means any item, collection, or grouping of information about an individual maintained by DHS, including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying assigned to the individual, such as a finger or voice print or a photograph.
- 1.7 The term “SNAP Data” means any information relating to the identity of recipients of the federal benefit program (formerly known as Food Stamps) that assists low-income individuals with a means of obtaining food and embodied in 7 U.S.C. Chapter 51.
- 1.8 The term “TANF Data” means all information relating to the identity of recipients of the federal and District benefit program known as Temporary Assistance for Needy Families program which assists low-income individuals and is embodied in The Social Security Act, Title IV (Part A of Title IV)

## D. Disclosure of Confidential Information

Occasionally, DHS may disclose Confidential Information to Pondera. Pondera will: (a) limit disclosure of any Confidential Information to its directors, officers, employees, agents or representatives (collectively "Representatives") who need to know such Confidential Information in connection with the current or contemplated business relationship between the parties to which this Addendum relates, and only for that purpose; (b) advise its Representatives of the proprietary nature of the Confidential Information and of the obligations in this Addendum, require such Representatives to be bound by written confidentiality restrictions no less stringent than those contained herein, and assume full liability for acts or omissions by its Representatives inconsistent with its obligations under this Addendum; (c) keep all Confidential Information strictly confidential by using a reasonable care, but not less than care used by it in safeguarding its own confidential information; and (d) not disclose any Confidential Information received by it to any third parties (except as otherwise provided for herein).

#### **E. Use of Confidential Information**

Pondera agrees to use the Confidential Information solely in connection with the current or contemplated business relationship between the parties and not for any purpose other than as authorized by this Addendum without the prior written consent of an authorized representative of the DHS. No other right or license, whether expressed or implied, in the Confidential Information is granted to Pondera. Title to the Confidential Information will remain solely with DHS. All use of Confidential Information by Pondera shall benefit DHS and any modifications and improvements thereof by Pondera shall be the sole property of DHS.

#### **F. Compelled Disclosure of Confidential Information**

If Pondera is compelled by Law to disclose any Confidential Information it shall provide DHS with prompt written notice so DHS may seek a protective order or other remedy and/or waive compliance with this Addendum, cooperate with DHS to obtain a protective order or other remedy, and if the parties cannot obtain a protective order, other remedy, or otherwise fail to quash the legal process requiring disclosure, Pondera will disclose the requested Data only to the extent to satisfy the request.

#### **G. Security of Data**

Pondera will not attempt to identify individuals' records by any method. Datasets containing Confidential Information shall be encrypted. All reasonable precautions shall be taken to secure Confidential Information from individuals who do not specifically have authorized access. Confidential Information shall be kept on a password-protected file server in a secure environment. Confidential Information will be kept in a separate directory on the server also password-protected and will be accessible only by Pondera staff members specifically authorized to receive access as provided in this Addendum.

#### **H. Term**

This Addendum shall remain in effect for a two-year term. Notwithstanding the foregoing, Pondera's duty to hold in confidence Confidential Information disclosed during term shall remain in effect indefinitely.

#### **I. Remedies**

Both parties acknowledge that the Confidential Information to be disclosed is of a sensitive nature, and that the unauthorized dissemination of the Confidential Information violate both District and federal law.

The damages to DHS that would result from the unauthorized dissemination of the Confidential Information would be impossible to calculate. Therefore, both parties agree that DHS shall be entitled to injunctive relief preventing the dissemination of any Confidential Information in violation of the terms hereof. Such injunctive relief shall be besides any other remedies available, whether at law or in equity. DHS may recover its costs and fees, including reasonable attorneys' fees, incurred in obtaining any such relief. Further, if litigation occurs relating to this Addendum, the prevailing party may recover its reasonable attorney's fees and expenses.

## **J. Return of Confidential Information**

Pondera shall, within thirty calendar days, return and redeliver to DHS all tangible material embodying any Confidential Information provided and all notes, summaries, memoranda, drawings, manuals, records, excerpts or derivative information deriving therefrom, and all other documents or materials ("Notes") (and all copies of the foregoing, including "copies" that have been converted to computerized media in image, data, word processing, or other types of files either manually or by image capture) based on or including any Confidential Information, in whatever form of storage or retrieval, upon the earlier of (i) the completion or termination of the dealings between the parties contemplated; (ii) the termination of this Addendum; or (iii) when the DHS may so request; provided however that Pondera may retain such of its documents as is necessary to enable it to comply with its reasonable document retention policies. Pondera, with the written consent of the DHS may (or with Notes, at Pondera's option) immediately destroy the foregoing embodying Confidential Information (or the reasonably nonrecoverable data erasure of computerized data) and, upon request, certify in writing such destruction by an authorized officer of Pondera supervising the destruction).

## **K. Notice of Breach**

Pondera shall notify the DHS promptly upon discovery of, or suspicion of, (1) any unauthorized use or disclosure of Confidential Information by Pondera or its Representatives; or (2) any actions by Pondera or its Representatives inconsistent with their respective obligations under this Addendum, Pondera shall cooperate with any efforts of DHS to help DHS regain possession of Confidential Information and prevent its further unauthorized use.

## **L. Miscellaneous**

- 1.1 This Addendum constitutes the entire understanding between the parties and supersedes any prior or contemporaneous understandings and Addendums, whether oral or written, between the parties, regarding the subject hereof. This Addendum can be modified only by a written amendment signed by the party against whom enforcement of such modification is sought.
- 1.2 The validity, construction and performance of this Addendum shall be governed and construed under the laws of the District of Columbia applicable to contracts made and to be performed within such state, without giving effect to any conflict of laws provisions thereof. The Federal and state courts in the District of Columbia shall have sole and exclusive jurisdiction over any disputes arising under, or connected with or related to, the terms of this Addendum and Pondera: (i) consents to personal jurisdiction; and (ii) waives the right to raise *forum non conveniens* or any similar objection.
- 1.3 Any failure by either party to enforce the other party's strict performance of any provision of this Addendum will not constitute a waiver of its right to enforce such provision or any other provision of this Addendum.



- 1.4** Although the restrictions in this Addendum are considered by the parties to be reasonable to protect the Confidential Information, if any such restriction is found by a court of competent jurisdiction to be unenforceable, such provision will be modified, rewritten or interpreted to include as much of its nature and scope as will render it enforceable. If it cannot be so modified, rewritten or interpreted to be enforceable, it will not be given effect, and the remainder of the Addendum will be enforced as if such provision was not included.
- 1.5** Any notices or communications required or permitted to be given may be delivered by hand, deposited with a nationally recognized overnight carrier, electronic-mail, or mailed by certified mail, return receipt requested, postage prepaid, in each case, to the address of the other party first stated above (or such other addressee as furnished by a party under this paragraph). All such notices or communications shall be deemed to have been given and received (a) with personal delivery or electronic-mail, on the date of such delivery, (b) with delivery by a nationally recognized overnight carrier, on the third business day following dispatch and (c) with mailing, on the seventh business day following such mailing.
- 1.6** This Addendum is personal, and neither party may directly or indirectly assign or transfer it by law or otherwise without the prior written consent of the other party, which consent will not be unreasonably withheld. All obligations in this Addendum shall extend to and be binding upon the parties to this Addendum and their respective successors, assigns and designees.
- 1.7** Paragraph headings used in this Addendum are for reference only and shall not be used or relied upon in interpreting this Addendum.

**IN WITNESS WHEREOF**, the parties have executed this Addendum as of the date first above written.

**D.C. Department of Human Services**

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

**Pondera Solutions, LLC**

By: Sharie A. Kirsch

Name: Sharie A. Kirsch

Title: Sr. Vice President