AMENDMENT OF SOLICITATION / MODIFICATION OF CONTRACT	1. Contract Number	Page of Pages	
	CFOPD-20-C-022B	1	1

2. Amendment/Modification Number	3. Effective Date	4. Requisition/Purchase Request No.	5. Solicitation Caption
Modification 7	Upon Contracting Officer's Signature		Medical Audit Services

6. Issued by: Code	7. Administered by (If other than line 6)
Office of the Chief Financial Officer Office of Contracts 1100 4th Street, S.W. Suite E620 Washington, D.C. 20024 202-442-7012 - main	

Myers and Stauffer, LC 10200 Grand Central Avenue, Suite 200 Owings Mills, MD 21117-4183 Mark Korpela, CFE - Principal 800-505-1698 (p) 410-627-0225 (c) mkorpela@mslc.com	9A. Amendment of Solicitation
	9B. Dated
X	10A. Modification of Contractor/Order No. CFOPD-20-C-022B
	10B. Dated (See Item 13) July 17, 2020

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in item 14. The hour and date specified for receipt of Offers ☐ is extended. ☐ 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 makes reference 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

X	A. This change order is issued pursuant to (Specify Authority): 27 DCMR Section 3601.2(c)and Section I.8 Changes of the Contract. 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.
	C. This supplemental agreement is entered into pursuant to authority of:
	D. Other (Specify type of modification and authority) Option Year Extension

E. IMPORTANT: **Contractor** ☐ is not ☒ is required to sign this document and return 1 copy to the issuing office.

14. Description of Amendment/Modification:

The District intends to achieve the following with Modification 7:

1. Revise Section J Attachment to add Attachment J.4, District of Columbia Business Associate Agreement.

All other terms and conditions shall 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)	16A. Name of Contracting Officer
Mark Korpela, Principal	

15B. Contractor	15C. Date Signed	16B. District of Columbia	16C. Date Signed
Mark Korpela (Signature of person authorized to sign)	02/02/2024	Drakus Wiggins (Signature of Contracting Officer)	02/02/2024

DICTRICT OF COLUMBIA
BUSINESS ASSOCIATE AGREEMENT

This agreement shall apply to all contracts where the contractor transmits, creates, accesses, receives, or maintains health information on individuals who are served by the District of Columbia and is a Business Associate as that term is defined by the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), and associated regulations promulgated at 45 CFR Parts 160, 162, and 164, as amended (HIPAA Regulations).

(a) **Definitions**

(1) "Business Associate" means a person or entity, who, on behalf of the District or of an Organized Health Care Arrangement (as defined in this clause) 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.

(2) "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 clause, 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.

(3) "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.

(6) "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.

(7) "Designated Record Set" means a group of records maintained by or for a Covered Entity that are:

(A) The medical records and billing records about individuals maintained by or for a covered health care provider;

(B) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(C) Records used, in whole or in part, by or for the Covered Entity to make decisions about individuals.

(6) "Health Care" means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(A) 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

(B) Sale or dispensing of a drug, device, equipment, or other item in accordance with the prescription.

(7) "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.

(8) "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.

(9) "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 clause.

(10) "Individual" means 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).

(11) "Individually Identifiable Health Information" means 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.

(12) "National Provider Identifier (NPI)" means the Standard Unique Health Identifier for Healthcare Providers as defined at 42 C.F.R. § 162.406.

(13) "Organized Health Care Arrangement" means (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.

(14) "Personal Representative" means 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).

(15) "Privacy and Security Official" means 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.

(16) "Privacy Officer" means 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.

(17) "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. parts 160 and 164, subparts A and E, as it may be amended.

(18) "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.

(19) "Record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity.

(20) "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.

(21) "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.

(22) "Security Officer" means the person designated by the Security Official or one of the District'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 laws. 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.

(23) "Security Rule" means the Standards for Security of Individually Identifiable Health Information at 45 C.F.R. parts 160, 162 and 164, subpart C.

(24) "Unsecured PHI" means 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, enacted at part of the American Recovery and Reinvestment Act of 2009 (Pub.L 111-5, 123 Stat 115), approved February 17, 2009.

(25) "Workforce" means 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.

(b) **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:

(1) Business Associate agrees not to use or disclose PHI or ePHI (other than as permitted or required by this clause or as Required by Law.

(2) 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 (Pub.L 111-5, 123 Stat 115) approved February 17, 2009 (ARRA), to maintain the security of the PHI and to prevent use or disclosure of such PHI other than as provided for by this clause. Business Associate acknowledges that, pursuant § 13401, Business Associate must comply with the Security Rule and privacy provisions detailed in this clause.

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 clause 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:

(R) Required (A) Addressable

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 Healthcare 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)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
		Isolating Healthcare Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
		Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
		Response and Reporting (R)
		Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
		(R)
		Written Contract or Other Arrangement (R)

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)

(1) The Business Associate agrees to name a Privacy or Security Officer who is accountable for developing, maintaining, implementing, overseeing the compliance of, and enforcing compliance with this clause, the Security Rule and other applicable federal and District privacy laws within the Business Associate's business. The Business Associate reports violations and conditions to the District-wide Privacy and Security Official or the Agency Privacy Officer of the covered component within the District's Hybrid Entity.

(2) 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 clause.

(3) The Business Associate agrees to report to Covered Entity, in writing, any use or disclosure of the PHI not permitted or required by this clause 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 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 HSS, Office for Civil Rights, and potentially the media, on behalf of the District.

(4) 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 clause 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.

(5) 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.

(6) Within 10 business days following the award of the contract, or within 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 clause.

(7) The Business Associate agrees to provide access within 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.

(8) The Business Associate agrees to make any amendments within 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 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.

(9) 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. The Business Associate agrees to comply with the applicable portions of the ordering agency's Identity and Procedure Verification Policy.

(10) 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.

(11) The Business Associate agrees to provide to the Covered Entity or an Individual, within 5 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 (b)10, 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.

(12) 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 5 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.

(13) 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 obligations.

(14) As deemed necessary by the District, the Business Associate agrees to the monitoring and auditing of items listed in paragraph (b) of this clause, as well as data systems storing or transmitting PHI, to verify compliance.

(15) 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.

(16) 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 clause.

(17) If the Business Associate has not submitted the District's Business Associate Questionnaire prior to contract award, the Business Associate shall file a completed Questionnaire with the Agency Privacy Officer/Liaison or the Contract Administrator within 30 days after contract award. Business Associate shall complete and submit the Questionnaire to the Agency Privacy Officer/Liaison or the Contract Administrator on or before October 1st of each year of this contract. At the discretion of the Agency Privacy Officer/Liaison, Business Associates with limited access to PHI may be granted a written waiver of the requirement to file a Questionnaire. contract.

(c) **Permitted Uses and Disclosures by the Business Associate.**

(1) Except as otherwise limited in this clause, 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.

(2) Except as otherwise limited in this clause, 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.

(3) Except as otherwise limited in this clause, 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.

(4) Except as otherwise limited in this clause, 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).

(5) Business Associate may use PHI to report violations of this clause or the HIPAA Regulations to the appropriate federal and District of Columbia authorities, consistent with 45 C.F.R. § 164.502(j)(1)-(2).

(d) **Additional Obligations of the Business Associate.**

(1) 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 the written report to the Privacy Officer no later than 30 business days after the award of the contract. 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 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 agency responsible for receiving and processing requests for PHI; and

(viii) Supporting documents if the recipient/personal representative has access to the Report/File.

(2) 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) 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) Reporting 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) Making all policies and procedures, and documents relating to security, available to the Secretary for the purposes of determining the Covered Entity's compliance with HIPAA.

(iv) If 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.

(v) Business Associate agrees not to electronically transmit or permit access to PHI unless such transmission or access is authorized by this clause 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 clause, "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 the Agency Privacy Officer/Liaison or the Contract Administrator with the key or keys to decrypt such information and will otherwise assure the Covered Entity that such PHI is accessible upon reasonable request.

(vi) 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 the Agency Privacy Officer/Liaison or the Contract Administrator that all such software complies with all applicable standards and specifications required by the HIPAA Regulations and shall inform the Agency Privacy Officer/Liaison or the Contract Administrator of any software standards or specifications not compliant with the HIPAA Regulations.

(vii) At the request of the Covered Entity, the Business Associate agrees to amend this clause to comply with all HIPAA mandates.

(e) **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.

(f) **Obligations of the Covered Entity.**

(1) 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.

(2) 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.

(3) 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.

(4) The 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.

(g) **Representations and Warranties.**

The Business Associate represents and warrants:

(1) That 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 under this clause; and

(2) That all of its employees, agents, subcontractors, representatives and members of its Workforce, whose services may be used to fulfill obligations under this clause are or shall be appropriately informed of the terms of this clause 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 clause.

(h) **Term and Termination.**

(1) The requirements of this clause 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

(2) Except as provided in paragraph (h)3 below, upon termination or expiration of the contract, the Business Associate shall return in a mutually agreed upon format or confidentially destroy all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity within 5 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.

(3) 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 clause to such PHI and limit further uses maintains such PHI. Additionally, the Business Associate shall:

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

(ii) Return to Covered Entity, or, if agreed to by Covered Entity, destroy, the remaining PHI that the Business Associate still maintains in any form;

(iii) 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;

(iii) 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 in paragraph 49(c) hereof; and

(iv) Return to Covered Entity, or, if agreed to by Covered Entity, destroy, the PHI 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.

(4) Except for provisions Required by Law as defined herein, no provision of this clause shall be deemed waived unless in expressed in writing and signed by duly authorized representatives of the Covered Entity and Business Associate. 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.

(5) Any ambiguity in this clause shall be resolved to permit compliance with applicable federal and District laws, rules, and regulations, 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.